International Journal of Law, Social Science and Humanities (IJLSH)

Volume 2, Issue 3, November 2025
E-ISSN: 3063-7554
https://doi.org/10.70193/ijlsh.v2i3.260

Standardizing Smart Contracts for Regulatory Compliance in Cross-Border Payments

Samiur Rahman[1*]

[1] Department of Law, University of Newcastle Upon Tyne, United Kingdom

Submitted: 07 August 2025 *Revised: 18 September 2025* *Published: 09 November 2025*

Abstract:

Smart contracts auto-executing digital agreements built on DLT (Distributed Ledger Technology), an emerging technology of blockchain are revolutionizing cross-border payments by enhancing efficiency and automation. However, their widespread adoption is hindered by a fragmented regulatory landscape and legal uncertainties across jurisdictions. Therefore, to promote the urgency of regulatory governance of smart contract, this research advocates for the techno-legal standardization of smart contracts to ensure regulatory compliance in international financial transactions. It investigates how smart contracts can be designed to meet diverse legal requirements while maintaining technical adaptability, scalability, and interoperability. Drawing on interdisciplinary literature and qualitative methods including expert interviews, surveys, and case studies the study aims to develop a framework that balances innovation with legal certainty. Key challenges addressed include jurisdictional fragmentation, enforcement mechanisms, integration with legacy systems like SWIFT, and compliance with KYC/AML regulations. The research also examines emerging solutions such as decentralized identity frameworks, trusted oracles, and hybrid on-chain/off-chain models. By bridging the gap between law, technology, and finance, this study offers actionable insights for policymakers, financial institutions, blockchain developers, and international businesses. Ultimately, it contributes to the development of a standardized smart contract ecosystem that supports secure, efficient, and legally compliant cross-border payments.

Keywords: Smart Contracts; Blockchain; Regulatory Compliance; Cross-Border Payments

INTRODUCTION

Emerging technologies are driving inclusive growth and transforming global industries, with blockchain standing out as a revolutionary force in reshaping financial transactions (Mhlanga, 2023). As a decentralized and distributed ledger system, blockchain offers numerous advantages by democratizing financial services and improving accessibility, particularly in developing nations (Daley, 2024). A key innovation within this ecosystem is the smart contract self executing agreements with terms directly written into code, which can significantly enhance the efficiency of cross-border payments (Lajoie-O'Malley et al., 2020).However, despite its potential, the adoption of smart contracts faces significant regulatory challenges (Liao & Caramichael, 2022).

The regulatory landscape surrounding smart contracts remains fragmented and complex, particularly in cross-border financial transactions (Javaid et al., 2022). Existing contract laws, designed for traditional legal agreements, struggle to adequately address the unique nature of smart contracts (Jerry I.H Hsiao, 2017). Key legal issues such as enforcement, jurisdiction, dispute resolution, and compliance with varying national regulations pose considerable challenges (Harsono & Suprapti, 2024). Without a standardized framework, the risk of regulatory fragmentation grows, leading to uncertainty for businesses and financial institutions looking to implement smart contracts in cross-border payments.

*Corresponding Author : Samiur Rahman, Department of Law, University of Newcastle Upon Tyne, United Kingdom, ORCID iD: 0000-0001-9263-4745, E-mail: S.Rahman12@newcastle.ac.uk

In recent years, the fintech industry has seen rapid growth, driven by technologies such as blockchain, artificial intelligence, and big data analytics (Panisi, 2017). Fintech startups have capitalized on the efficiency and automation potential of smart contracts to disrupt traditional banking models. Smart contracts play a pivotal role in DeFi (Decentralized Finance) applications, enabling peer-to-peer lending, borrowing, and payments without the need for intermediaries like banks (Sousa Batista & Associados, Sociedade de Advogados & Gomes, 2018).

However, this evolution also brings new risks, including operational risks and the absence of clear governance frameworks to manage these transactions. The intersection of fintech and smart contracts is reshaping the global financial landscape, but for widespread adoption, industry players must navigate the intricate regulatory environment.

In addition to regulatory hurdles, smart contracts also raise concerns regarding security, scalability, and interoperability (Çağlayan Aksoy, 2022). The immutability of blockchain technology ensures transparency and fraud reduction, but these benefits come with vulnerabilities, particularly in financial applications. Moreover, the lack of interoperability between different blockchain platforms limits the seamless execution of smart contracts across borders. Scalability issues are also evident in complex applications like Smart Legal Energy Contracts (SLECs), where the increasing number of participants complicates contract execution.

Despite these challenges, smart contracts have the potential to transform the financial industry by reducing transaction costs, improving market efficiency, and automating agreement enforcement. Therefore, this research seeks to explore the standardization of smart contracts from a regulatory compliance perspective, focusing on cross-border payments and as a key research question that is: How can smart contracts be standardized to ensure regulatory compliance and facilitate efficient cross-border payments, considering the diverse regulatory landscapes and the evolving nature of both smart contracts and regulations? Hence, the primary aim of this research is to develop a framework for standardizing smart contracts to ensure regulatory compliance in cross-border payments, addressing both the legal and technological challenges and opportunities associated with their adoption. However, the widespread adoption of smart contract hinges on industrial adoption as construction sector nowadays are reluctant to adopt smart contract into their operational infrastrsctures. Research indicates that MENA (Middle East and North Aftrican) regions are unwilling to adopt smart contract due to infancy of the technology (Gouda Mohamed et al., 2025)

By examining both legal and technical challenges, this research aims to propose a framework for the "techno-legal" standardization of smart contracts, ensuring their smooth integration into global financial systems while addressing the regulatory complexities that currently impede their widespread adoption. Therefore, this research is both timely and innovative, providing substantial benefits to both academic circles and industry stakeholders. It presents a progressive solution to a critical challenge within the rapidly changing realm of international finance and blockchain technology.

METHODS

This research has employed a doctrinal method of research focusing on expounding literature review of recent studies on smart contracts to investigate the current regulatory and technical landscape of smart contract. This method is chosen to gain deep inter-disciplinary understandings of the exisiting research on smart contract standardization. Therefore, locating a complex interplay between technological, legal, and economic factors that underscore the essence of developing a standardized smart contract to be used convenietenly for cross-border trading. The primary sources analysed were authoritative journals, books and reputable websites and primary sources include legislative analysis of United States relating to smart contract. The collected data was analyzed using critial evaluation to reach a solution for the primary research question of this research paper.

RESULTS

Smart contracts have immense potentials for automating financial transactions. However, widespread adoption depends on overcoming technical and regulatory challenges. Therefore, this research finds

key areas where regulatory oversight could be solidified for a uniform standardized techno-legal smart contract suitable for global adaptation in the face of DeFi and blockchain proliferation. Contemporary need is to balance computer codes with legal language, ensuring contracts remain enforceable as laws evolve such as creating hybrid smart contract models that integrates both legal clauses within code preserving both technical superiority and legal authenticity. Unification process through UNIDROIT could be ventured for maximizing global compliance through multi or bilateral co-operation.

Legal standardization of smart contract would require developing legislation underpinning the essence of decentralized technologies and would compliment existing decentralized technologies e.g "blockchain" to be regulated under the supervision of government while sandboxing this within regulatory goverenance innovation is achieveable. Digital Finance Co-operatiove Research Centrer (DFCRC), an Australian Government's initiative to digitalize and standardize digital assets could be replicated in other countries for greater regulatory recognition of decentralized technololologies such as smart contracts.

However, implementation of smart contract now faces jurisdictional fragmentation which complicates cross-border adoption. Possible solution is designing programmable legal clauses within the smart contract code and advocate for global adoption by following supranational and bilaterial adoption. Moreover, compliance mechanisms such as KYC (Know Your Customer) and AML (Anti-Money Laundering) checks should be auto programmed within smart contract codes for enhancing legal compliance and integrity. In the meantime, for achieving technical granularity integration of decentralized technology such as zero knowledge proofs could enhance privacy and security compliance.

Technicalities of making smart contract interoperable remains a hurdle due to platform heterogeneity and uncertainties of oracle solutions that may hinder widespread adoption. However, this can be resolved by adopting cross-chain protocols and decentralized oracle networks. In the context of banking reforms for digital assets, legacy financial systems like SWIFT should adopt CBDC (Central Bank Digital Currencies) or Blockchain based swift protocols for facilitating blockchain based digital currencies and boost smart contract's prospects for cross border commerce (Digital Finance CRC, n.d.).

Scalability and privacy concerns especially sensitive transactions could be achieved through formal verification tools regulated by goverenment. Finally, the dispute resolution issues in smart contracts underscores the need for integrated ODR (Online Dispute Resolution) models that will allow parties of contractual dispute to settle claim digitally without court's intervention.

Future research should focus on developing sustainable standardization frameworks focusing on 'techno-legal" approach balancing both technical robustness and legal credibility enhancing interoperability, scalability, privacy across platforms resulting in legal recognition of smart contracts in international trade therefore, opening possibilities for seamless integration with legacy banking systems.

DISCUSSION

This discussion explores how the standardization of smart contracts can ensure regulatory compliance and improve the efficiency of cross-border payments, all within the context of diverse and evolving regulatory landscapes. While previous studies have highlighted the feasibility of using blockchain-based smart contracts in international transactions, less attention has been given to the technological risks and legal challenges that may arise with broader adoption. This research seeks to fill that gap by examining potential strategies for standardizing smart contracts and overcoming regulatory barriers in the cross-border payments sector.

The literature reviewed in this discussion section consists primarily of scholarly articles, focusing on both legal and technical aspects of smart contracts. This review is organized into four sections. The first section discusses standardization in terms of technical granularity and regulatory compliance, exploring how smart contracts can be made flexible enough to adapt to changing regulations while maintaining legal validity.

The second section examines the legal and regulatory uncertainties that surround smart contracts, particularly in cross-border contexts. The third section focuses on the integration and interoperability of smart contracts with existing financial systems. Finally, the review concludes with an analysis of how standardization can optimize smart contracts for efficient cross-border payments, addressing key challenges such as scalability, integration, interoperability, trust and regulatory compliance.

Smart Contract Standardization: Granularity and Regulatory Considerations

Blockchain powered smart contracts hold great potential for transforming cross-border payments. However, to realize this potential, standardized frameworks are necessary. This section explores the ideal level of standardization and how it can be adapted to meet both evolving regulatory requirements and technological complexity.

Some authors propose a reference model for standardizing Smart Legal Energy Contracts (SLEC), primarily focusing on the energy sector (Cali et al., 2022). While specific to energy, their model offers valuable insights that could be applied to cross-border payments. The model emphasizes interoperability by using a language-agnostic approach, which involves creating device, syntactic, and semantic layers that allow different systems to communicate effectively.

Similarly, (Hunn & Accord Project, UK, 2019) advocates for standardization through stateful computation, which allows smart contracts to track their execution history and generate new states as agreements evolve on the blockchain. Hunn also introduces a Hybrid On-Chain/Off-Chain model, which utilizes the security of blockchain for executing contracts while keeping sensitive data off-chain. This approach addresses privacy concerns while still ensuring the security of transactions. Additionally, Hunn highlights the importance of combining human-readable legal text with machine-readable code, enabling smart contracts to meet both technical and legal requirements for compliance.

Despite these advancements, several challenges remain in achieving full regulatory compliance. For instance, the rigidity of blockchain code makes it difficult to adapt smart contracts to the complex and often flexible nature of commercial agreements. Moreover, the decentralized nature of blockchain introduces technical uncertainties that can complicate legal compliance, especially in cross-border settings. These issues highlight the need for further research to ensure that smart contracts can integrate smoothly with existing legal systems.

The authors also emphasize the importance of developing compliance mechanisms that allow smart legal contracts to integrate seamlessly with current legal frameworks. While smart contracts offer a promising solution for secure and efficient cross-border payments, widespread adoption will depend on finding the right balance between standardization and flexibility. Processes such as ensuring determinism and consistency in data encoding/decoding can build trust and foster interoperability across systems. However, this raises a critical question: how granular should standardization be to support both innovation and regulatory compliance?

In the same note, other researchers explore this question, arguing that achieving the right level of granularity in smart contracts requires a balance between standardization and flexibility (Aleinieh & Zoboli, 2021). Legal standardization, particularly incorporating specific regulatory requirements, is crucial to achieving this balance. The research further examines how smart contracts can maintain technical precision while complementing existing regulatory practices. For this to happen, standardization must be adaptable to contemporary contract laws, but various regulatory hurdles must be addressed prior to this.

However, one researcher underscore the importance of legal compliance (Mashhour et al., 2023). They point out that while converting contract law into code offers benefits like automation and reduced ambiguity, there are still challenges related to adapting to changing legal landscapes and navigating regulatory fragmentation across jurisdictions.

To overcome these hurdles, standardization of smart contracts must be technically refined to support cross-border transactions. These standards must be granular enough to incorporate legal and regulatory compliance while still fostering innovation and efficiency in international transactions.

Legal and Regulatory Uncertainty

The emerging legal landscape around smart contracts presents significant challenges to their widespread adoption. The absence of a unified regulatory framework, coupled with the complexities of cross-border transactions, creates uncertainty for both businesses and consumers. These legal ambiguities, along with the technical intricacies of smart contracts, have fostered a risk-averse environment that hinders their full potential.

Some authors realize that implementation of smart contracts faces numerous legal challenges. They argue that stakeholders must understand these legal implications, jurisdictional issues, and compliance with existing laws to ensure the enforceability of smart contracts (Vasiu and Vasiu, 2023). The authors also stress the importance of addressing security risks. They suggest that future research should focus on integrating smart contracts with legal frameworks to resolve jurisdictional discrepancies.

To reduce legal uncertainties, standardized legal definitions of key terms are crucial. This could lead to the development of a universal framework that encompasses various legal interpretations. Moreover, tackling security vulnerabilities such as through vulnerability assessments, Oracle security, and technical standardizations will be essential in building trust among stakeholders and promoting broader acceptance of smart contracts across jurisdictions.

While Vasiu and Vasiu focus on conceptual legal solutions, (Levi and Lipton, 2018) explore the enforceability of smart contracts specifically in the United States. They highlight the absence of federal contract law, which means that state-level legislative actions play a key role in legitimizing smart contracts. For instance, laws like the Uniform Electronic Transactions Act (UETA) gave validity to blockchain based smart contracts (National Conference of Commissioner on Uniform State Laws, 1999). And Federal Electronic Signatures in Global and National Commerce Act (E-Sign) recognize the validity of contracts formed through electronic agents or computer programs (Electronic Signatures in Global and National Commerce Act, 2000). States such as Nevada and Arizona have even amended UETA laws to include smart contracts under contract law.

In the U.S., smart contracts must comply with the common law principles of offer, acceptance, and consideration to ensure legal enforceability. Levi and Lipton suggest that one approach could be the creation of code-only smart contracts, which would contain only executable code without the need for traditional text-based contracts. However, this approach raises challenges, particularly for non-technical parties who may struggle to enforce these contracts without the help of trusted experts.

Another challenge arises with the use of Oracles external data sources that smart contracts rely on. Ensuring the integrity of off-chain data provided by Oracles remains difficult, which further complicates enforceability of smart contracts in different jurisdictions. Although, U.S. has already taken steps to legitimize smart contracts, other states still couldn’t legitimize nor determine the legitimacy of smart contracts through statutory enactments due to jurisdictional and technological issues. This reveals a critical gap known as jurisdictional fragmentations associated with smart contracts.

On the other hand, to fully realize the potential of smart contracts, both technical standardization and legal compliance must be addressed (Vasiu and Vasiu, 2023). They point out that existing regulations lack substantive analysis of smart contracts, leading to contradictions regarding their enforceability. Additionally, there are unresolved questions about whether smart contracts comply with traditional contract law principles.

The immutability of smart contracts also creates conflict with the European Union’s General Data Protection Regulation (GDPR), particularly the "right to be forgotten." Sensitive aspects of smart contracts cannot be deleted upon request, contradicting GDPR’s privacy policies (General Data Protection Regulation (GDPR), 2016). The authors suggest the use of zero knowledge proof cryptographic techniques to address this issue, although these solutions are technically complex to adopt industrially.

Despite these concerns, several U.S. states have enacted legislation Arizona HB 2417 (Weninger & House of Representatives, 2017). And Nevada SB 398 also legitimized smart contract (Nevada State Legislature, 2017). Moreover, Vermont H.868 that legitimizes blockchain transactions and smart contracts (Vermont General Assembly, n.d.). These laws aim to ensure the enforceability of smart contracts and address compliance issues through clear regulations.

One author highlights the need for conflict-of-laws principles, similar to the Rome I Regulation, to manage jurisdictional complexities in smart contracts (Andriyanov, 2020). However, he acknowledges that this is a temporary solution and calls for more comprehensive legal frameworks. In the ASEAN+6 regions, (Goh, 2022) also stresses the need for legislative policy development to regulate smart contracts effectively, suggesting that the UNIDROIT or (International Institute for the Unification of Private) Law guidelines could play a key role in reducing legal uncertainties (UNIDROIT, n.d.). Hybrid contract models are proposed as another way to mitigate these uncertainties.

The study also advocates for supranational regulations to minimize the risks related to jurisdictional discrepancies and the enforceability of smart contracts. However, further research and validation are needed to determine the effectiveness of these supranational rules and hybrid approaches in achieving standardization.

Highlight the potential of Online Dispute Resolution (ODR) as a complementary mechanism for enforcing smart contracts. While smart contracts offer advantages such as immutability, automation, and transparency, they are not immune to disputes. Integrating ODR could provide an efficient and cost-effective way to resolve these disputes, particularly in cross-border contexts. However, the lack of standardized frameworks complicates the enforcement of ODR decisions, especially across jurisdictions (Goldenfein and Leiter, 2018).

Further explores how blockchain technology could enhance ODR, particularly in e-commerce, where disputes are common but often low in value. As the legal framework around smart contracts is still developing, ODR may offer a viable solution for resolving contractual issues (Koulu , 2016).

In conclusion, addressing the legal and regulatory uncertainties surrounding smart contracts particularly in cross-border transactions requires the development of statutory rules and conflict oflaws principles to manage jurisdictional and enforcement discrepancies. Additionally, incorporating proactive and reactive measures within smart contract platforms, such as ODR mechanisms and distributed jurisdiction, could help mitigate these challenges. Further research is needed to assess the effectiveness of these approaches.

Interoperability and Integration with Existing Systems

Interoperability and integration are critical challenges that need to be addressed to resolve the incompatibility of smart contracts with existing payment systems. However, the uncertain nature of blockchain technology can introduce additional complexities. One scholar proposes a conceptual multi-chain framework designed to enhance interoperability and integration in blockchain-based Letter of Credit (L/C) transactions within B2B e-commerce platforms (Li ,2021). This standardized model consists of three layers: the blockchain infrastructure layer, the application layer, and the application services layer. The framework aims to establish a three-tier architecture (account chain, transaction chain, and IoT chain) to improve transaction efficiency and ensure regulatory compliance.

Building on this, (Khorasani et al., 2024) introduced the “Automated Gateways” framework, which enhances smart contract interoperability across different blockchain platforms. While promising, this framework still requires further research to assess its compatibility with existing legacy payment systems. Automated Gateways integrates interoperability directly into the blockchain’s core, aligning with web3 principles of decentralization and transparency in cross-chain transactions. The framework also includes a communication management module, which operates independently and uses the gRPC protocol to ensure transparency across different networks. However, its current application is limited to permissioned blockchains, and expanding this model to public blockchains could further improve interoperability.

To extend the reach of interoperability, explore how smart contracts can automate IoT operations (Sadawi et al., 2022). A key challenge is the diversity of IoT devices, which can lead to single points of failure. The authors propose integrating blockchain technology with IoT systems, citing a successful use case in carbon trading. This integration, they argue, can reduce the limitations associated with IoT device diversity while promoting trust and operational efficiency.

The study also introduces the concept of "Trusted Oracles", which play a crucial role in ensuring the accuracy and reliability of the data used in smart contracts. These oracles validate data from various IoT devices, but they present privacy and technical challenges. To overcome these issues, the authors propose a comprehensive IoT-Blockchain-Oracle architecture, comprising three layers: IoT, Blockchain, and Oracle.

While this framework offers a robust solution for integrating IoT and blockchain, the authors emphasize the need to address the “Oracle Problem” by improving oracle mechanisms in terms of scalability, interoperability, security, and regulatory and ethical considerations. Some authors further expand on this discussion by examining how different types of oracles hardware, software, human, inbound, and outbound can be effectively integrated into smart contract platforms (Popchev et al., 2023). They also highlight cross-chain oracles, which enhance interoperability across multiple blockchain platforms, and demonstrate a specialized blockchain platform for smart agriculture, showcasing its potential to improve data exchange and automate civil contracts.

The authors call for more research into enhancing interoperability between blockchain platforms and evaluating the effectiveness of Decentralized Oracle Networks (DONs). They stress the importance of improving data validation and verification within oracle systems and making oracle integration more scalable, user-friendly, cost-effective, and regulatory-compliant to fully realize blockchain’s potential across various applications.

Smart contracts, when integrated with blockchain, hold significant potential for enabling seamless cross-border payments. Research by Safiullin (2023) and Capocasale & Perboli (2022) highlights the transformative potential of smart contracts, such as faster transactions, reduced reliance on intermediaries, and enhanced security through tamper-proof ledgers. Permissioned blockchains can further streamline integration by providing controlled access, while tools like escrow help manage trade finance risks (Safiullin et al., 2023), (Capocasale & Perboli, 2022).

However, several challenges remain. Regulatory uncertainty around smart contracts and the lack of legal frameworks for consumer protection create significant obstacles. Technical limitations, such as restricted access to the global blockchain ecosystem and resistance from established institutions to adopt blockchain and smart contracts, further complicate integration and interoperability.

In summary, while smart contracts hold great promise for accelerating cross-border payment systems, challenges related to integration and interoperability must be addressed before widespread adoption. Integrating IoT devices and implementing oracle networks in blockchain platforms can significantly improve the reliability, efficiency, and interoperability of smart contracts. However, further research is needed to evaluate their effectiveness in terms of scalability, user-friendliness, cost-efficiency, and regulatory compliance.

Standardizing Smart Contracts for Cross-Border Payment Efficiency

To overcome the challenges of cross-border payments, standardizing smart contracts is crucial. By establishing uniform rules for blockchain networks, we can enhance their efficiency, scalability, security, and trustworthiness. This standardization is essential for widespread adoption of blockchain technology, especially in international financial transactions.

One author investigated how blockchain technology and smart contracts can address trust issues in business transactions (Fandl, 2020). He noted that limited access to technology, particularly among informal firms, hinders their adoption of these platforms. Fandl suggests that future research should explore how smart contracts can support economic growth in small and medium-sized enterprises (SMEs) and emerging markets, considering local contexts and technical challenges.

Additionally, the study emphasizes the importance of educating these firms on the advantages and applications of smart contracts to build trust. To address trust issues, Fandl recommends incorporating compliance mechanisms directly into smart contract platforms. While smart contracts aim to reduce reliance on intermediaries, he argues that fully replacing legal institutions may not be practical.

To mitigate scalability concerns, propose a standardization framework combining Trusted Execution Environments (TEEs) with the Ekiden platform (Cheng et al, 2019). This approach enhances the security and privacy of blockchain applications, especially smart contracts. By separating execution from consensus, Ekiden enables independent scaling of compute and consensus resources, addressing scalability limitations in traditional blockchain systems.

While incorporating TEEs through Ekiden can be more cost effective than traditional Ethereum-based smart contracts, further research is needed to explore performance optimizations and enhance security protocols. This will ensure the broader applicability of this framework in cross-border finance and other domains.

To enhance the applicability of this framework in cross-border finance, propose standardized funding models supported by blockchain-based smart contracts. The authors identify two potential use cases involving the integration of smart contracts with Central Bank Digital Currencies (CBDCs), Milestone-Based Funding and End-Use Programming for Early-Stage Startups (Garg & Rao, 2023). These models can improve efficiency, autonomy, and transparency in cross-border investments.

However, the authors caution that several challenges must be addressed before these models can achieve widespread adoption. Key issues include information asymmetry in cross-border investments, market fluctuations, and regulatory inconsistencies across jurisdictions require attention.

While technical standardization of smart contracts remains a challenge, a study by (Dai et al, 2017) highlights the advantages of the Qtum framework. Qtum's blockchain framework offers notable performance benefits due to its more energy-efficient proof-of-stake (PoS) consensus model. This PoS model enhances scalability, efficiency, and transaction validation, making it a more viable solution for industrial applications. Additionally, Qtum's broad compatibility with well established cryptocurrencies allows for easier integration with existing systems and supports a wider range of applications.

In terms of security and formal verification, the Qtum framework also provides advanced features. It supports formal verification through verifiable smart contract languages and reduces the risk of future hacks. Moreover, its smart contract template libraries enable rapid deployment in industrial settings, and it offers mobile accessibility, making it more versatile for real-world use. Despite these strengths, the framework still requires further research to develop standardized smart contract languages specific to Qtum. Additionally, a comparative analysis with real-world enterprise use cases is necessary to fully assess its potential.

To improve existing cross-border payment systems, the International Monetary Fund (IMF) in (Adrian et al, 2022) proposes a Centralized Multilateral Exchange and Contracting Platform (X-C). This platform leverages advanced technologies to streamline compliance processes, enhance efficiency, transparency, privacy, and security. However, the platform's success hinges on overcoming challenges such as establishing a common regulatory framework, addressing market liquidity. trust issues, and ensuring privacy.

One autor delve into the integration of KYC and AML technologies within DeFi platforms to enhance smart contract standardization and ensure regulatory compliance (Hou Sak, 2024). Their research proposes the use of Decentralized Identity Frameworks (DIDs) and cryptographic techniques to empower users with control over their personal data while conducting KYC checks without compromising confidentiality.

To ensure successful integration with existing international payment transmission policies, banking compliance technologies like KYC and AML must be seamlessly integrated with blockchain and smart contract solutions. A study by (Zhu et al., 2019) emphasizes the potential of integrating permissioned blockchain technology with the SWIFT platform. While SWIFT is a globally

recognized standard for international payments, it faces limitations such as slow transaction speeds, high costs, and security vulnerabilities. The authors propose a conceptual framework called "BCSWIFT," which introduces a dual-layer network structure to enhance the safety, accuracy, and efficiency of cross-border payments.

Despite its promise, the BCSWIFT framework faces several challenges, including scalability, interoperability, and regulatory issues. These hurdles must be overcome for BCSWIFT to achieve its potential in improving international financial services. Blockchain-powered smart contracts hold significant advantages for accelerating cross-border payments. By making smart contract transactions KYC and AML compliant, incorporating blockchain technology into the SWIFT system, adopting CBDC platforms, and developing specialized privacy-focused blockchain platforms like Qtum and Ekiden, we can significantly boost standardization. However, challenges of scalability, privacy, and regulatory uncertainty need to be addressed prior to large-scale adoption by SMEs and fintech startups.

In conclusion, this discussion section examined the techno-legal standardization of smart contracts for cross-border payments. To address this primary question, the review analyzes four key sub-questions: standardization with reference to technical granularity and regulatory compliance, navigating diverse regulatory fragmentation, analyzing integration and interoperability challenges, and assessing the importance of standardization of smart contracts in the cross-border payment system. However, if the exisiting banking solutions can be elevated to include the blockchain based solutions then the process of standardization will truly commence hence presumptively making the smart contract a legitimate trading tool for cross-border trading.

CONCLUSION

Blockchain technology and smart contracts in cross-border payments present significant challenges in ensuring regulatory compliance across diverse jurisdictions. While smart contracts offer potential for efficiency and automation in international financial transactions, their legal status, enforceability, and compliance with various national regulations remain ambiguous. hence opening possibilities for standardization through a techno-legal perspective.

Therefore, this research aims to uncover the importance of developing a framework for standardizing smart contracts to acheive regulatory compliance in cross-border payments, addressing a key research gap that is whether the smart contract is legally and technically sound for cross border trading?.Through a detailed exploration of key regulatory challenges, current limitations of smart contract technology, this study assessed both the opportunities and obstacles to industry-wide adoption of smart contracts. Moreover, this research identfifed a key research gap between the evolving technology of smart contracts and the diverse, often conflicting, regulatory frameworks that govern international financial transactions and offers potential wayforward towards successful standardization practices that might be explored by future hybrid studies.

The lack of a standardized framework that addresses both the technological and legal dimensions of smart contracts creates barriers to widespread adoption. This research aims to make an intersection between technology, law, and finance by exploring how smart contracts can be standardized from a techno-legal perspective, ensuring regulatory compliance in cross-border payments as well as balancing technical adaptability with legal certainty across multiple jurisdictions.

By addressing the discovered gaps in current literatures, particularly the lack of comprehensive research on the techno-legal aspects of smart contract, this study offers a novel contribution to the fields of law, finance, and blockchain technology. The integration of legal, technical, and regulatory perspectives is unique, providing holistic approach to smart contract and its potential for technological and legally sound standardization.

This research, therefore, is not only timely but also pioneering in its approach, contributing significant value to both academia and industry stakeholders. It offers a forward-thinking solution to one of the key challenges in the evolving landscape of international finance and blockchain technology and

would be significantly insightful for diverse stakeholders such financial institutions, crypto startups, Financial technologists, governments and blockchain developers.

Conflict of Interest

All the authors declare that there are no conflicts of interest.

Funding

This study received no external funding.

How to cite:

Rahman, S. (2025). Standardizing smart contracts for regulatory compliance in cross-border payments. *International Journal of Law, Social Science and Humanities (IJLSH)*, *2*(3), 295-306. https://doi.org/10.70193/ijlsh.v2i3.260.

REFERENCES

Adrian, T., Grinberg, F., Griffoli, T. M., Townsend, R. M., & Zhang, N. (2022). A multi-currency exchange and contracting platform. *IMF Working Papers*, *2022*(217). https://doi.org/10.5089/9798400224188.001.A001

Aleinieh, T. K., & Zoboli, L. (2021). Increasing standardization for smart contracts. *Uniform Law Review*, *26*(3), 583–598. https://doi.org/10.1093/ulr/unab022

Andriyanov, D. V. (2020). Application of smart contracts and blockchain platforms in cross-border oil and gas transactions: aggravation of conflict-of-laws problem. *Actual Problems of Russian Law*, *15*(6), 84–94. https://doi.org/10.17803/1994-1471.2020.115.6.084-094

Cali, U., Sebastian-Cardenas, J., Saha, S., Chandler, S., Gourisetti, S. N. G., Hughes, T., Khan, K., Lima, C., Rahimi, F., & Tillman, L. C. (2022). *Standardization of smart contracts for energy markets and operation*. https://www.authorea.com/doi/full/10.36227/techrxiv.19142081.v1?commit=d57647ce827d90b4ef2a1dd30a1f584edc501c97

Capocasale, V., & Perboli, G. (2022). Standardizing smart contracts. *IEEE Access*, *10*, 91203–91212. https://doi.org/10.1109/ACCESS.2022.3202550

Çağlayan Aksoy, P. (2022). Smart contracts: To regulate or not? Global perspectives. *Law and Financial Markets Review*, *16*(3), 212–241. https://doi.org/10.1080/17521440.2023.2298192

Cheng, R., Zhang, F., Kos, J., He, W., Hynes, N., Johnson, N., Juels, A., Miller, A., & Song, D. (2019). Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. *IEEE European Symposium on Security and Privacy (EuroS&P)*, 185–200. https://doi.org/10.1109/EuroSP.2019.00023

Dai, P., Mahi, N., Earls, J., & Norta, A. (2017). *Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform*. *2*(2), https://doi.org/10.13140/RG.2.2.35140.63365

Daley. (2024). *Blockchain in Finance: What It Is and How It's Used*. https://builtin.com/blockchain/blockchain-banking-finance-fintech

Digital Finance CRC. (n.d). *Australian Central Bank Digital Currency Pilot Project*. (n.d.). https://dfcrc.com.au/cbdc/

Electronic Signatures in Global and National Commerce Act. https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf

Fandl, K. (2020). Can Smart Contracts Enhance Firm Efficiency in Emerging Markets? *Northwestern Journal of International Law & Business*, *40*(3), 333.

Garg, N., & Rao, R. (2023). A Case for Integrating Blockchain-based Smart Contracts in cross-border Investments, *SSRN Scholarly Paper*, 4561807. Social Science Research Network. https://doi.org/10.2139/ssrn.4561807

General Data Protection Regulation (GDPR) – Legal Text. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/

Gilcrest, J., & Carvalho, A. (2018). Smart Contracts: Legal Considerations. *2018 IEEE International Conference on Big Data (Big Data)*, 3277–3281. https://doi.org/10.1109/BigData.2018.8622584

Goh, G. R. D. E. (2022). Smart contract disputes and public policy in the ASEAN+6 region. *Digital Law Journal*, *3*(4), 32–70. https://doi.org/10.38044/2686-9136-2022-3-4-32-70

Goldenfein, J., & Leiter, A. (2018). Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique*, *29*(2), 141–149. https://doi.org/10.1007/s10978-018-9224-0

Gouda Mohamed, A., Alqahtani, F. K., Sherif, M., & El-Shamie, S. M. (2025). Scrutinizing the adoption of smart contracts in the MENA Region's Construction Industry. *Journal of Asian Architecture and Building Engineering*, *24*(3), 1558–1577. https://doi.org/10.1080/13467581.2024.2329354

Hou Sak, M. (2024). KYC/AML Technologies in Decentralized Finance (DEFI) (The Leonard N. Stern School of Business & Glucksman Institute. https://www.stern.nyu.edu/sites/default/files/2024-07/Glucksman_Sak_2024.pdf

Harsono, I., & Suprapti, I. A. P. (2024). The Role of Fintech in Transforming Traditional Financial Services. *Accounting Studies and Tax Journal (COUNT)*, *1*(1), 81–91. https://doi.org/10.62207/gfzvtd24

Hunn, P. G. & Accord Project, UK. (2019). Smart Contractsas Techno-Legal Regulation. *Journal of ICT Standardization*, *7*(3), 269–286. https://doi.org/10.13052/jicts2245-800X.735

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A Review of Blockchain Technology Applications for Financial Services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Jerry I-H Hsiao & Ph.D. (2017). "Smart" Contract on the Blockchain-Paradigm Shift for Contract Law? *US-China Law Review*, *14*(10). https://doi.org/10.17265/1548-6605/2017.10.002

Khorasani, K. E., Rouhani, S., Pan, R., & Pourheidari, V. (2024). Automated Gateways: A Smart Contract-Powered Solution for Interoperability Across Blockchains. *2024 IEEE International Conference on Blockchain (Blockchain)*, 611–618. https://doi.org/10.1109/Blockchain62396.2024.00090

Koulu, R. (2016). Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement. *SCRIPTed*, *13*(1), 40–69. https://doi.org/10.2966/scrip.130116.40

Lajoie-O'Malley, A., Bronson, K., van der Burg, S., & Klerkx, L. (2020). The Future(s) of Digital Agriculture and Sustainable Food Systems: An Analysis of High-Level Policy Documents. *Ecosystem Services*, *45*, 101183. https://doi.org/10.1016/j.ecoser.2020.101183

Li, X. H. (2021). Blockchain-based Cross-border E-business Payment Model. *2021 2nd International Conference on E-Commerce and Internet Technology (ECIT)*, 67–73. https://doi.org/10.1109/ECIT52743.2021.00022

Liao, G. Y., & Caramichael, J. (2022). *Stablecoins: Growth Potential and Impact on Banking*. https://www.federalreserve.gov/econres/ifdp/stablecoins-growth-potential-and-impact-on-banking.htm

Lipton, A., & Levi, S. (2018). An Introduction to Smart Contracts and Their Potential and Inherent Limitations. *The Harvard Law School Forum on Corporate Governance*.

https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Mashhour, O. F. A., Aziz, A. S. A., & Noor, N. A. M. (2023). Legal and Regulatory Aspects of Smart Contracts: A Systematic Review. *Eurasian Journal of Management & Social Sciences, 4*(2), 156–172. https://doi.org/10.23918/ejmss.V4i2p156

Mhlanga, D. (2023). Block Chain Technology for Digital Financial Inclusion in the Industry 4.0, Towards Sustainable Development? *Frontiers in Blockchain, 6.* https://doi.org/10.3389/fbloc.2023.1035405

Nevada State Legislature. (2017). *Senate Bill No. 398, 79th Legislature*. LegiScan. https://legiscan.com/NV/bill/SB398/2017

National Conference Of Commissioners On Uniform State Laws. (1999). Uniform Electronic Transactions Act. https://www.uaipit.com/uploads/legislacion/files/0000004550_UNIFORM%20ELECTRONIC%20TRANSACTIONS%20ACT.pdf

Panisi, F. (2017). Blockchain and "Smart Contracts": FinTech Innovations to Reduce the Costs of Trust, *Social Science Research Network*, 3066543. https://doi.org/10.2139/ssrn.3066543

Popchev, I., Radeva, I., & Doukovska, L. (2023). Oracles Integration in Blockchain-Based Platform for Smart Crop Production Data Exchange. *Electronics*, *12*(10), 2244. https://doi.org/10.3390/electronics12102244

Sadawi, A. A., Hassan, M. S., & Ndiaye, M. (2022). On the Integration of Blockchain With IoT and the Role of Oracle in the Combined System: The Full Picture. *IEEE Access*, *10*, 92532–92558. https://doi.org/10.1109/ACCESS.2022.3199007

Safiullin, M., Yelshin, L., & Sharifullin, M. (2023). Prospects for Using Blockchain in the System of International Supply Chains and Cross-Border Payments. *Revista Gestão & Tecnologia*, *23*(4), 360–376. https://doi.org/10.20397/2177-6652/2023.v23i4.2692

Sousa Batista & Associados, Sociedade de Advogados, & Gomes, D. (2018). Contratos Ex- Machina: Breves notas sobre a introdução da tecnologia Blockchain e Smart Contracts. *Revista Electrónica de Direito*, *3*, 39–55. https://doi.org/10.24840/2182-9845_2018-0003_0003

UNIDROIT. (2025). *Purpose*. https://www.unidroit.org/about-unidroit/

Vasiu, I., & Vasiu, L. (2023). A Framework for Effective Smart Contracting. *Bratislava Law Review*, *7*(2), 107–122. https://doi.org/10.46282/blr.2023.7.2.511

Vermont General Assembly. (2023.). *H0868: An Act Relating To Insert Bill Topic if Known.* https://legiscan.com/VT/bill/H0868/2023

Weninger, R. & House of Representatives. (2017). Signatures; Electronic Transactions; Blockchain Technology. *State of Arizona*. https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf

Zhu, J.-M., Ding, Q.-Y., & Gao, S. (2019). Distributed framework of SWIFT System Based on Permissioned Blockchain. *Journal of Software*, *6*(30), 1594–1613. https://www.jos.org.cn/jos/article/abstract/5738