GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	Katelyn DeAgro
Student number:	3136053
Dissertation title:	Regulating and Advancing Smart Contracts: A Comprehensive Study of Legal Frameworks, Technological Progress, and International Cooperation
Supervisor's name:	**DENIS HEALY**
Supervisor's signature:	**8th August 2024**

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signature of student: *Katelyn DeAgro* **Date:** 09/08/24

Candidate Declaration

Candidate Name (please print): Katelyn DeAgro

I certify that the dissertation entitled: Regulating and Advancing Smart Contracts: A Comprehensive Study of Legal Frameworks, Technological Progress, and International Cooperation

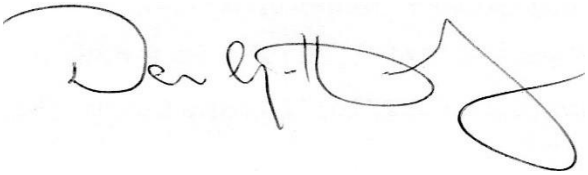
submitted for the degree of: LLM in International Commercial Law (QQI)

is the result of my own work and that where reference is made to the work of others, due acknowledgment is given.

Candidate signature: *Katelyn DeAgro*_____

Date: 09/08/2024_____

Supervisor Name (please print): Denis Healy

Supervisor signature: 

Date: 8th August 2024

Regulating and Advancing Smart Contracts: A Comprehensive Study of Legal Frameworks, Technological Progress, and International Cooperation

Research dissertation presented in partial fulfilment of the requirements for the degree of LLM in International Commercial Law (QQI)

Law School, Griffith College Dublin

Katelyn Elizabeth DeAgro

2024

Acknowledgements

I would like to express my deepest gratitude to my father, whose unwavering support and guidance have been instrumental in the completion of this dissertation. From a young age, you instilled in me the values of perseverance, curiosity, and dedication, which have guided me throughout my academic journey.

Your encouragement and belief in my potential have been a constant source of motivation, especially during challenging times. Whether it was through late-night conversations or your calming presence, you have always been there to provide wisdom and insight, pushing me to strive for excellence.

Thank you for being my biggest supporter and for inspiring me to pursue my dreams with passion and confidence. This dissertation is a testament to your enduring love and commitment, and I am forever grateful for everything you have done for me.

With love and appreciation,

Katelyn

Table of Contents

List of Definitions 8

Abstract 11

Chapter 1: Introduction **12**

1.1 Are smart contracts the way forward? 12

1.2 Methodology 14

Chapter 2: The Evolution and Legal Framework of Smart Contracts: Definitions, Formation, and Electronic Signatures 16

2.1 Potential Legal and Regulatory Hurdles 17

2.2 Jurisdictional Conflicts 18

2.3 Regulatory Disparities 19

2.4 Alignment with Traditional Legal Principles 20

2.4.1 Contractual and Governance Issues 21

2.4.2 Formation of Smart Legal Contracts 22

2.5 Law of Contract 24

2.5.1 Offer and Acceptance 24

2.5.2 Form of Contract 27

Chapter 3: Smart Contracts and Their Legal Enforceability: Enhancing Compliance, Transparency, and Security in Cross-Border Fintech Transactions 31

3.1 Traceability and Transparency 32

3.2 Auditing and Reporting 33

3.3 Security and Flaws 34

3.4 Scalability and Privacy 36

3.6 Challenges Posed by Blockchain Technology 36

3.7 Technical and Legal Constraints of Smart Contracts 37

3.8 The Role of Regulatory Sandboxes 39

Chapter 4: Balancing Data Privacy and Blockchain Technology in Cross-Border FinTech Operations 41

4.1 Impact of Operational Efficiency 41

4.2 Importance of Regulatory Clarity and Harmonization 42

4.3 Security Challenges in Cross-Border FinTech Transactions 43

4.4. Impact of Blockchain Technology on Security 45

4.5 Privacy Regulations and Cross-Border Transactions 47

4.6 Data Protection Principles and Blockchain 47

4.6.1 Addressing Data Protection Challenges 48

4. 7 Legal Recognition of Smart Contracts 49

4.7.1 Data Protection and Smart Contracts 50

4.7.2 Addressing GDPR Compliance in Blockchain and Smart Contracts 51

4.7.3 Anonymization and Pseudonymization 53

Chapter 5: Stakeholder Perspectives and Recommendations 55

5.1 Stakeholder Perspectives 55

5.1.1 Policymakers and Regulators 56

5.1.2 Industry Stakeholders 58

5.2 Recommendations 59

1. Develop Standardised Protocols for Smart Contracts 59
2. Harmonise Regulatory Frameworks 61
3. Foster International Regulatory Collaboration 63
4. Leverage Technological Advancements 65
5. Expand Regulatory Sandboxes 66
6. Promote Global Cooperation 67
7. Address Consumer Protection Concerns 69
8. Clarifying Legal Status and Enforceability 70

Chapter 6: Concluding Remarks 72

Bibliography 79

List of Definitions

Smart Contract

A smart contract is a self-executing digital agreement with terms and conditions directly encoded into software. It automatically executes and enforces actions when specified conditions are met, eliminating the need for intermediaries and reducing the potential for disputes.

Blockchain

A blockchain is a decentralised, distributed ledger that records transactions across multiple computers. Each block contains a list of transactions, and once a block is completed, it is added to the chain, creating a permanent and tamper-proof record. Blockchain technology underpins the operation of smart contracts.

Decentralisation

Decentralisation involves distributing authority and control across a network rather than concentrating it in a single entity. In blockchain and smart contracts, decentralisation enhances security and transparency by ensuring that no single party can alter or control the system.

Distributed Ledger Technology (DLT)

DLT is a digital system for recording transactions of assets where the transaction details are simultaneously stored across multiple locations. Unlike traditional databases, distributed ledgers have no central data store or administrative function.

Node

A node is a fundamental unit of a blockchain network that stores and processes data. Nodes can be full nodes, which maintain a complete copy of the blockchain, or lightweight nodes, which store only a subset of the blockchain's data. Nodes participate in validating and relaying transactions and blocks, contributing to the network’s overall security and integrity.

Network Consensus

Network consensus refers to the process by which nodes in a blockchain network agree on the validity of transactions and the state of the ledger. Consensus mechanisms ensure that all participants in the network reach an agreement on the data without requiring a central authority.

Peer-to-Peer Network

A peer-to-peer (P2P) network is a decentralised network structure where each node (or peer) acts as both a client and a server. In blockchain systems, P2P networks enable direct communication and transaction exchange between nodes, facilitating the decentralised nature of the system.

Layer 2 Solutions

Layer 2 solutions are secondary protocols built on top of existing blockchain networks to improve scalability and efficiency by processing transactions off-chain.

zk-Rollups

zk-Rollups aggregate multiple transactions into a single batch and generate a succinct cryptographic proof submitted to the main blockchain. This approach enhances transaction processing speed and reduces costs while maintaining security.

Optimistic Rollups

Optimistic Rollups assume transactions are valid by default, performing detailed verification only when disputes arise. This approach reduces the on-chain transaction load and improves scalability.

Artificial Intelligence (AI)

AI simulates human intelligence processes in machines, especially computer systems. In smart contracts, AI enhances decision-making capabilities, allowing contracts to execute complex and adaptive actions based on real-time data analysis.

Machine Learning (ML)

ML is a subset of AI focused on developing algorithms that enable computers to learn from data and make decisions. In smart contracts, ML can enable contracts to adapt and improve over time based on new information and experiences.

Cryptography

Cryptography is the practice of secure communication in the presence of third parties. It is fundamental to blockchain technology and smart contracts, ensuring data privacy, integrity, and authentication through advanced algorithms.

Abstract

Blockchain technology has significantly transformed the financial sector through the advent of smart contracts—self-executing digital agreements that automate and secure transactions via decentralised networks. Despite their transformative potential, the widespread adoption of smart contracts is impeded by regulatory fragmentation, technological limitations, consumer protection concerns, and issues of legal enforceability. This dissertation offers a comprehensive analysis of these challenges and proposes strategies to facilitate the integration of smart contracts into global financial systems.

The study begins with an examination of the current regulatory landscape, identifying inconsistencies and gaps that obstruct effective implementation. It underscores the need for regulatory harmonisation and standardised protocols to address legal uncertainties and enhance operational efficiency. Key initiatives for fostering international regulatory collaboration, including information-sharing platforms and cross-border regulatory sandboxes, are evaluated for their potential to streamline compliance processes and improve interoperability.

Technological advancements are also a critical focus of this research. The dissertation explores how Layer 2 solutions—such as zk-Rollups and Optimistic Rollups—and emerging technologies like artificial intelligence (AI) and machine learning (ML) can address scalability and efficiency issues. These innovations hold promise for enhancing smart contract performance, security, and adaptability, making them more suited to complex financial transactions.

Consumer protection is addressed through an analysis of disclosure requirements, dispute resolution mechanisms, and fairness in smart contract transactions. The study emphasises the necessity of transparent practices and robust protection measures to build trust and foster broader adoption.

Finally, the dissertation investigates the legal status and enforceability of smart contracts, advocating for legislative clarity and judicial recognition to provide certainty for stakeholders. It also explores the advantages of international coordination in establishing a consistent legal framework for cross-border smart contract applications.

By integrating insights from regulatory, technological, and legal perspectives, this dissertation offers actionable recommendations to support the effective adoption and integration of smart contracts into the global financial ecosystem. It aims to contribute to the development of a more cohesive and innovative financial landscape, driving progress and efficiency in international transactions.

Chapter 1

Introduction

1.1 Are smart contracts the way forward?

Smart contracts, which are self-executing contracts with terms encoded directly into a blockchain, are a revolutionary idea that blockchain technology has brought to the world of modern finance. These digital contracts, which automate contract execution and lessen dependency on conventional middlemen, promise to improve the effectiveness, transparency, and security of financial transactions. Smart contract integration into international financial systems is becoming an increasingly popular topic of study as financial institutions and technology companies investigate the potential of these contracts

Smart contracts have the potential to be revolutionary, but there are a number of important obstacles in the way of their general implementation. The regulatory environment is still disjointed, with different legal systems in different countries posing obstacles to international trade. Businesses' capacity to implement smart contracts largely is impacted by the legal ambiguities and operational inefficiencies brought about by this lack of standardisation and regulatory clarity. Further, the integration of smart contracts into established financial systems is made more difficult by consumer protection concerns and the requirement for a well-defined legal framework to ensure their enforceability.

By thoroughly examining all of the facets of smart contract integration, this dissertation seeks to overcome these issues. The first step will involve a review of the current regulatory environment in order to pinpoint the main obstacles and contradictions that affect the use and operation of smart contracts. The basis for developing uniform protocols and harmonising regulatory frameworks to enable worldwide adoption will be provided by this analysis.

Additionally, the dissertation will look at how international regulatory cooperation might improve the efficacy and interoperability of smart contracts. Important projects like cross-border regulatory sandboxes and information-sharing platforms will be investigated as means of promoting global cooperation and minimising regulatory fragmentation. Through the promotion of a common

strategy, these initiatives can facilitate the smooth operation of smart contracts across jurisdictions and aid in the streamlining of compliance procedures.

Technological developments are yet another important component of this research. The dissertation will look into how new technologies like artificial intelligence (AI) and machine learning (ML) and Layer 2 solutions (such zk-Rollups and Optimistic Rollups) might solve the present issues with scalability, efficiency, and adaptability. These technologies present viable ways to improve the security and performance of smart contracts, which will make them more appropriate for intricate and dynamic financial transactions.

The main focus will be on consumer protection, specifically on how to create transparent disclosure standards, efficient dispute resolution processes, and equitable smart contract transactions. Building trust and promoting the wider use of smart contracts need addressing these issues.

In conclusion, the dissertation will examine the enforceability and legal standing of smart contracts, highlighting the necessity of establishing judicial precedents and legislative actions to validate their legitimacy. It will also take into account how international cooperation might be used to establish a uniform legal framework that facilitates cross-border integration of smart contracts.

Finally, the goal of this dissertation is to present a thorough examination of the technological, legal, and regulatory issues surrounding smart contracts. It attempts to promote the integration of smart contracts into the global financial ecosystem, advancing advancement and improving efficiency in cross-border financial transactions, by putting forth workable solutions and investigating novel techniques.

1.2 Methodology

Doctrinal Analysis

The doctrinal method has been selected as a primary approach due to the need for an in-depth legal analysis of regulatory frameworks, legal challenges, and the compatibility of smart contracts with established legal principles. This methodology involves a meticulous examination of statutory law, regulations, and case law relevant to data protection, blockchain technology, and cross-border

fintech transactions. By engaging with the "black letter of the law," this research aims to understand the existing legal landscape governing cross-border fintech operations, assess the challenges fintech companies face in complying with data protection regulations such as the GDPR, and evaluate how smart contracts can be effectively integrated within these legal frameworks.

In particular, the doctrinal analysis will focus on key legal texts, such as the General Data Protection Regulation (GDPR) in the EU, and relevant statutes and case law in the United States and other jurisdictions. This approach will provide a foundation for identifying potential legal barriers and opportunities for blockchain technology and smart contracts in the fintech sector.

Law and Economics

The law and economics methodology will be employed to analyse the economic implications of legal rules and institutions on cross-border fintech transactions. This approach will involve a quantitative analysis of how smart contracts impact transaction speed, cost savings, and efficiency in the fintech industry. By examining these factors, this research aims to highlight the potential economic benefits of adopting blockchain technology and smart contracts while considering the regulatory challenges that may arise.

The law and economics perspective will also inform the development of recommendations for potential changes in regulation and law. By analysing the economic outcomes associated with different regulatory approaches, this research seeks to propose legal improvements that enhance efficiency without compromising safety. This methodology provides a valuable lens through which to assess the broader economic impact of legal decisions and regulatory frameworks in the fintech sector.

Critical Legal Studies

To supplement the doctrinal and law and economics approaches, this research will also draw on Critical Legal Studies (CLS), particularly the political economy and economic context of legal decisions and issues. This subcategory of CLS allows for a critical examination of the underlying power dynamics and social implications of legal frameworks and practices.

By challenging accepted norms within traditional legal practice, the CLS perspective will enable this research to propose necessary changes to current regulatory frameworks. Rather than engaging in a comparative analysis of legal systems in the EU and the United States, this research will focus on how these jurisdictions have cooperated or failed to cooperate in addressing data protection and blockchain technology issues. This analysis will underscore the importance of international collaboration and inform recommendations for improving cross-border cooperation in the fintech sector.

Through a combination of doctrinal analysis, law and economics, and critical legal studies, this research aims to provide a comprehensive understanding of the legal challenges and opportunities associated with cross-border fintech transactions. By examining the intersection of data protection regulations, blockchain technology, and smart contracts, this study seeks to develop informed recommendations for legal and regulatory improvements that promote greater efficiency, security, and international collaboration in the fintech industry.

Chapter 2

The Evolution and Legal Framework of Smart Contracts: Definitions, Formation, and Electronic Signatures

Fintech's explosive growth has transformed financial transactions by removing geographical restrictions and facilitating easy value transfers across borders. Regulators and fintech companies alike face formidable obstacles as a result of this shift, which has brought about a complicated regulatory environment. This chapter aims to investigate in detail the various regulatory obstacles that arise in cross-border fintech transactions, looking at their wide-ranging effects on transaction security, operational effectiveness, and the overall contractual governance structure. Furthermore, it will explore in detail how established contract law concepts and blockchain-based smart contracts interact, with the goal of clarifying each other's roles and guaranteeing that legal requirements and technological advancements are in line. Technology is advancing faster than regulatory frameworks in the dynamic environment that the fintech industry operates in.

Regulatory norms must change and adapt as a result of the difficulty regulators have in striking a balance between oversight and innovation. The swift rise of fintech technologies, like cryptocurrency and blockchain, has forced authorities to revise current legislation and develop new legal frameworks. In order to handle the global nature of fintech operations, this evolutionary process entails both domestic modifications and international cooperation.

Regulatory sandboxes and innovation hubs are two ways that regulatory authorities are interacting with industry stakeholders as they become more proactive.[1] Through controlled environments and innovation-fostering practices, these initiatives enable fintech companies to test new products and services while maintaining compliance. Such cooperative efforts are essential to creating a regulatory environment that fosters the fintech industry's sustained growth.

Fintech's explosive growth has transformed financial transactions by removing geographical boundaries and facilitating easy value transfers across borders. But in this environment, blockchain-based platforms such as Tezos have surfaced, providing distinctive answers to the problems that conventional financial systems face.[2] The decentralised blockchain platform offered by Tezos, which was founded by Arthur and Kathleen Breitman, is intended to support smart contracts and decentralised applications.[3] Tezos sets itself apart with its on-chain governance approach that gives token holders the ability to cast votes for protocol updates, promoting a blockchain environment that is more democratic and flexible.[4] It is imperative to comprehend the legislative ramifications and operational obstacles unique to platforms such as Tezos in order to effectively navigate the dynamic terrain of cross-border fintech transactions.

2.1 Potential Legal and Regulatory Hurdles

[1] Nathaniel Popper, 'Where Finance and Technology Come Together' *New York Times* (New York, 14 November 2016) <https://www.nytimes.com/2016/11/15/business/dealbook/where-finance-and-technology-come-together.html> accessed 9 August 2024; 'Singapore Tries to Become a Fintech Hub' *The Economist* (London, 12 January 2017) <https://www.economist.com/news/finance-and-economics/21714384-city-state-wants-fintech-bolsters-not-disrupts-mainstream> accessed 9 August 2024.

[2] Yueh-Ping Yang, 'When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?' (2023) 6 Stanford Journal of Blockchain Law & Policy 137

[3] Ibid.

[4] Ibid

Smart contract integration into current international legal frameworks is fraught with difficulties, notwithstanding their potential. First off, the global applicability of smart contracts may be called into question by varied legal interpretations in different jurisdictions. Cross-border transactions are made more difficult by differences in contract formation procedures, the acceptance of electronic signatures, and the interpretation of contractual terms. Furthermore, the irreversible nature of smart contracts can conflict with legal precepts that permit contract amendments or termination in specific situations. Another difficulty is making sure that international laws—like those pertaining to data protection and consumer rights—are followed. Moreover, the general acceptance and enforceability of smart contracts may be hampered by the absence of uniform smart contract templates and clear regulations. The decentralised character of blockchain technology presents notable jurisdictional obstacles for smart contracts.

Interoperability problems arise because different blockchain platforms currently employ disparate code languages and protocols. Standardising the creation and implementation of smart contracts might improve their compliance with accepted legal norms and ease international trade. International organisations are attempting to provide standards and rules for smart contracts, including the United Nations Commission on International Trade Law (UNCITRAL) and the International Organization for Standardization (ISO). The objective of these endeavours is to establish a unified legal structure that facilitates the worldwide acceptance of smart contracts while guaranteeing their conformity with conventional legal doctrines.

2.2 Jurisdictional Conflicts

Because fintech businesses are often global, there is sometimes jurisdictional ambiguity resulting from transactions that cross several legal jurisdictions, each with its own unique regulatory framework. Conventional legal theories base their determination of jurisdiction on the parties' residential locations and physical locations. For example, in the European Union (EU) the *Brussels II* regulation is the guiding principle which states that as a general rule jurisdiction is based on the defendant's domicile.[5] In this circumstance, blockchain transactions take place in an international

[5] Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility [2003] OJ L338/1, art 4(1).

digital environment, which makes it challenging to determine which legal framework applies to a specific smart contract. International collaboration and the creation of legislative frameworks that acknowledge the special qualities of blockchain technology are necessary to resolve this conflict of laws issue.

The absence of uniformity among regulatory frameworks has the ability to lead to inconsistencies and overlaps, posing significant obstacles for fintech enterprises trying to negotiate the intricate web of compliance requirements.[6] Furthermore, regulatory standards are interpreted differently in various jurisdictions, which increases the burden of compliance and creates legal uncertainty and potential liabilities for market participants. International regulatory organisations must work together to standardise norms and create precise rules for cross-border fintech businesses in order to resolve jurisdictional problems.

Moreover, the emergence of blockchain technology has presented new difficulties in determining jurisdiction, especially with regard to distributed ledger and decentralised network technologies. Traditional jurisdictional boundaries are blurred by the borderless and immutable nature of blockchain transactions, making regulatory oversight and enforcement more difficult.[7] Because of this, regulatory bodies have the difficult task of modifying current frameworks to suit the special features of fintech operations based on blockchain technology, protecting investors and maintaining market integrity in a global financial ecosystem that is becoming more interconnected by the day.

Because fintech businesses are often global, there is sometimes jurisdictional ambiguity resulting from transactions that cross several legal jurisdictions, each with its own unique regulatory framework. Projects like Tezos, which run on decentralised blockchain networks devoid of a central authority, highlight this complexity. In this case, the platform's decentralised structure raises concerns around regulatory enforcement and jurisdictional control.[8] Even though the project was started by founders in Switzerland and Northern California, Tezos is a worldwide platform with users and contributions from many nations. Because of this, selecting the right country for

[6] Yueh-Ping Yang, 'When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?' (2023) 6 Stanford Journal of Blockchain Law & Policy 148.
[7] Ibid
[8] Yueh-Ping Yang, 'When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?' (2023) 6 Stanford Journal of Blockchain Law & Policy

regulatory purposes is extremely difficult and necessitates carefully taking into account the platform's global user base and decentralised governance style.

2.3 Regulatory Disparities

The smooth execution of cross-border fintech transactions is significantly hampered not just by jurisdictional conflicts but also by regulatory differences between various countries. Fintech companies that operate in several markets face operational inefficiencies and compliance difficulties due to jurisdiction-specific variations in reporting requirements, enforcement methods, and compliance standards.[9] Lack of consistent regulatory standards frequently leads to redundant compliance efforts, raising the cost of compliance and preventing market growth.

Moreover, as fintech companies struggle to balance competing regulatory requirements, regulatory discrepancies may stifle innovation and slow the expansion of cross-border fintech transactions. Divergent approaches to cybersecurity, consumer privacy, and data protection further compound regulatory challenges, as will be discussed in chapter 5 of this paper, and require customised compliance strategies for each state. International regulatory agencies must work together to create shared regulatory standards and advance regulatory convergence in order to address regulatory differences. This will create an atmosphere that is favourable to cross-border fintech innovation and market expansion.

Apart from jurisdictional disputes, regulatory discrepancies across various countries present notable obstacles to the smooth execution of cross-border fintech transactions employing platforms such as Tezos.[10] The legislative environment around token issuance and decentralised applications differs greatly throughout nations, despite Tezos offering a strong foundation for these activities. For instance, the Tezos Foundation, as previously noted as founded in Switzerland, is in charge of the platform's advancement and marketing.[11] Nonetheless, Switzerland, the US, and other jurisdictions have quite different token offering and securities laws and regulatory procedures.[12] Fintech companies that use platforms like Tezos must take a customised approach to compliance

[9] William Magnuson, 'Regulating Fintech' (2018) 71 Vanderbilt Law Review 1167.
[10] Yueh-Ping Yang, 'When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?' (2023) 6 Stanford Journal of Blockchain Law & Policy
[11] Ibid
[12] Ibid

in order to navigate these regulatory discrepancies, taking into account the many regulatory contexts in which they operate.

The convergence of jurisdictional difficulties and blockchain technology is exemplified by the In re Tezos case, specifically with regard to judicial jurisdiction determination.[13] In order to establish personal jurisdiction over Tezos Foundation, the court used the purposeful direction test, highlighting the substantial marketing efforts that are aimed at the US market.[14] The case does, however, illustrate the potential difficulties in determining jurisdiction for truly global initial coin offerings (ICOs), as the distributed nature of blockchain technology makes standard jurisdictional analysis more difficult.[15] The function of verification nodes and other blockchain components may merit additional investigation in future cases involving blockchain-based activities, even though the court did not specifically take blockchain-related considerations into account while making its jurisdictional finding.

2.4 Alignment with Traditional Legal Principles

For smart contracts to be legitimate and enforceable, they must adhere to established legal precepts. Smart contracts require mutual consent, offer, acceptance, and consideration in the same manner as traditional agreements. To ensure compliance with contract law requirements, the underlying code of smart contracts must accurately reflect the intentions of the parties. In addition, smart contracts can facilitate performance by automatically carrying out contractual duties upon the satisfaction of predetermined criteria, in accordance with the pacta sunt servanda concept (agreements must be kept). Similar to conventional legal procedures, smart contract dispute resolution features like arbitration provisions and preset escalation protocols are designed to settle disputes quickly.

The way smart contracts are interpreted is crucial to their compliance with accepted legal norms. Conventional contracts are construed according to the wording employed, the situation, and the parties' intentions. It is crucial to make sure the code for smart contracts—which are expressed in

[13] *In re Tezos Securities Litigation* (United States District Court, ND Cal, 7 August 2018) Case No 17-cv-06779-RS.
[14] Tezos case
[15] Yueh-Ping Yang, 'When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?' (2023) 6 Stanford Journal of Blockchain Law & Policy

code—truly reflects the intentions of the parties. If there is a difference between the intended agreement and the coded terms, legal problems could occur. To close the gap between legal and technological interpretations, the smart contract code must be accompanied by clear and understandable documentation.

In classical contracts, the parties' execution of the agreed terms constitutes the principle of performance. This is improved by smart contracts, which fulfil contractual obligations automatically when certain circumstances are satisfied. But there are difficulties since blockchain technology is immutable, meaning that once smart contracts are implemented, they cannot be changed.[16] Conventional legal frameworks permit contract amendments, revocation, or termination in specific situations, such when parties agree to it or when an unanticipated occurrence (or force majeure) occurs. Innovative approaches are needed to address these issues inside the smart contract framework, such as adding amendment procedures or adding backup plans for unanticipated circumstances.

2.4.1 Contractual and Governance Issues

For international fintech transactions, the fusion of blockchain-based smart contracts with conventional contract law concepts offers both new potential and obstacles. Smart contracts are self-executing computer programs that are kept on blockchain networks. They automate contracts and make it possible to exchange digital assets safely and without the need for middlemen. Smart contracts must, however, be carefully considered in order to ensure their legal validity and enforceability. Important contractual and governance concerns include offer, acceptance, and the time of contract finalisation.

The effects of blockchain-based smart contracts on contract law are a topic of discussion among academics.[17] Given that they are just lines of code, that the blockchain is a new technology, and that there are legal prerequisites for creating legally enforceable agreements, the key question is whether they can be regarded as contracts.[18]

[16] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 118
[17] Ibid
[18] Ibid

In order for a contract to be legally binding, parties must objectively demonstrate their intention, which is a necessary component of contract formation. When interpreting a contract, transparency, good faith, and consent from both parties are essential. This is especially true when there are large power differentials or when one side unilaterally adopts standard terms and conditions. To prevent ambiguities and misinterpretations, parties must make sure that their intentions are appropriately expressed in the smart contract code, which presents particular issues when expressing contracts in code.

2.4.2 Formation of Smart Legal Contracts

For smart legal contracts to be legally legitimate and enforceable, whether they are created on- or off-chain, they must follow the rules of traditional contract law. The act of uploading smart contract code to a blockchain and having it accepted by other network users necessitates giving offer, acceptance, and consideration considerable thought in addition to the desire to establish legal relationships.[19] The integration of blockchain-based smart contracts into current legal frameworks will be made easier by creating standardised protocols for their use and encouraging openness in contractual governance.

The term "smart contract" is deceptive. It brings to mind contracts. Nick Szabo coined the term "smart contracts" to describe his theory of incorporating contractual stipulations into the hardware and software to make contract violations costly.[20] The development of blockchain technology has made this concept feasible. In fact, blockchain technology was initially designed for virtual currency trading.[21] It thus made it possible to register each digital object. The most sophisticated blockchain apps enable the uploading of deterministic computer programs, which run automatically under preset parameters.[22] Consequently, it is also possible to carry out contractual agreements using blockchain technology. For this reason, the term "smart contract" is commonly used to describe this blockchain feature when discussing it. Contracts are not always associated

[19] Mateja Durovic and André Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law' (2019) *European Review of Private Law* 753, 772.
[20] Karolina Kasprzyk, 'The Concept of Smart Contracts from the Legal Perspective' (2018) 34 *Revista Europea de Derecho y Derecho Comparado* 101.
[21] Michael Rauchs et al., *Distributed Ledger Technology Systems: A Conceptual Framework* (2018)
[22] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 118

with smart contracts. A computer code that can run automatically in response to a predetermined condition is known as a smart contract. A blockchain can be used to process and store this code, and it records any changes made to it.[23] Smart contracts have the potential to automate everything. For example, a smart contract might be a thermostat that uses preset settings to control the inside temperature of a home.[24] Smart contracts are meaningless legally in certain situations. When they are utilised to automate legally relevant actions or procedures, they take on legal significance. When all conditions are met, a smart contract could, for example, grant an administrative authorization.

For this reason it was proposed to refer to "smart legal contracts" while discussing the application of smart contracts in the contractual arena.[25] Scholars typically differentiate between smart legal contracts as instruments to carry out pre-existing contracts and as new contracts.[26] Regardless of how the agreement was made, the latter refers to the employment of computer code to automate the performance of an agreement that arose outside of the blockchain, either fully or partially. According to this theory, a smart contract serves as a tool to carry out a contract rather than being a contract in and of itself.[27] The compelled party's performance is substituted with automated performance. The earlier theory discusses the potential for agreements to be expressed as lines of code. It is questioned whether smart legal contracts may be considered contracts on this aspect.[28] Someone correctly begins their response to the question by defining what a contract is in law.

A legally enforceable agreement between two or more parties is called a contract. Thus, the agreement serves as the contract's fundamental building block. By exchanging an offer and an acceptance, the parties get to a mutual accord (the agreement). The parties' declaration of their intent to be legally bound by the contract is another essential prerequisite. This indicates that the

[23] Ibid
[24] Ibid
[25] Karolina Kasprzyk, 'The Concept of Smart Contracts from the Legal Perspective' (2018) 34 *Revista Europea de Derecho y Derecho Comparado* 106
[26] R. Weber, *Smart Contracts: Do we need new legal rules?*
[27] Karolina Kasprzyk, 'The Concept of Smart Contracts from the Legal Perspective' (2018) 34 *Revista Europea de Derecho y Derecho Comparado* 107
[28] Ibid

offeror and the offeree intended to engage into a contract that would have legal standing in a court of law.[29]

2.5 Law of Contract

It takes some form of expression from both parties for there to be a so-called "meeting of the minds." The informality principle states that parties are free to pick any format for contract completion in the absence of legal restrictions.[30] Electronic contracts can be concluded thanks to this principle. This assertion is supported by the non-discrimination principle, which is another globally acknowledged value. As such, computer code can likewise be used to express contracts.[31]

There are several methods in which the meeting of the minds (exchange of offer and acceptance) might take place. It is important to note that smart legal contracts can be signed on- or off-chain, according to Durovic and Janssen.[32] The authors use the uploading of a proposed contract in a coding language on the Ethereum platform and its subsequent acceptance by an Ethereum network participant that interacts with the uploaded smart contracts (by, for instance, making a payment in ethers) to describe the formation process of on-chain contracts.[33] Stated differently, when a smart contract code is uploaded to the blockchain without a signed agreement, a smart legal contract is created inside the blockchain. Here, the smart contract serves as a means for a user to express her contractual will in conjunction with the blockchain. A contract is created and the smart contract becomes a smart legal contract if the user who uploaded it and another user have similar wills.[34]

2.5.1 Offer and Acceptance

[29] Ibid
[30] UNIDROIT Principles of International Commercial Contracts (PICC) 2010, art 1.2; Principles of European Contract Law (PECL) 2002, art 2:101(2); Draft Common Frame of Reference (DCFR) 2009, II.–1:106
[31] Art. 5 of the MLEC and Art. 8(1) of the United Nations Convention on the Use of Electronic Communications in International Contracts. Art. 46 of the Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (e-IDAS Regulation)
[32] *Mateja Durovic and André Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law' (2019) 6 European Review of Private Law 760*
[33] Ibid
[34] Ibid

According to conventional contract law, a legally binding agreement usually requires an offer and an acceptance. The offeror makes an offer that includes all necessary terms for the contract, and the offeree indicates acceptance by making a statement or acting in an implicit manner. Similar to this, uploading a smart contract to the blockchain in the context of blockchain-based smart contracts can be understood as making an offer, which can be accepted directly by making a statement or implicitly by acting, like by running the smart contract code.[35]

The exact time at which a smart contract is completed varies according to legal regulations and contractual clauses, which are impacted by real notice, reception, and dispatch laws, among other criteria. Contract conclusion in blockchain transactions happens when the offeror receives the acceptance transaction from the offeree after it has been validated. On the other hand, acceptance through behaviour, such as giving up financial power to a smart contract code, indicates contract fulfilment through execution.[36] Therefore, in order to guarantee legal clarity and enforceability in cross-border fintech transactions, it is crucial to reconcile conventional contract law principles with the special qualities of blockchain-based smart contracts.

Certain commentators have noted that the uploading of a smart contract to the blockchain by a party is equivalent to making an offer.[37] The offer ought to have every component that makes a contract enforceable. If not, the other party is invited to engage in discussions rather than receiving an offer. Regarding this, Durovic and Janssen believe that it will typically be held to constitute an offer, not an invitation to treat, as the offeror uploads his "contract" onto the blockchain in a binary computer code which specifies precisely the parameters of the transaction.[38]

---

[35] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 118

[36] Ibid

[37] JM Smits, *Contract Law: A Comparative Introduction* (Edward Elgar Publishing 2017) 41

[38] *Mateja Durovic and André Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law' (2019) 6 European Review of Private Law 760*

Regarding acceptance, other than the offeree's consent to all terms of the offer, it need not satisfy any special conditions. Consequently, the offeree may accept the offer by using a private key to sign a transaction after the offeror has uploaded the smart contract.[39]

It is a counter-offer rather than an acceptance if the offeree's declaration does not specifically mention every term in the offer or does not agree to all of the terms.[40] In the latter instance, in order to create a contract, the counter-offer must be accepted. The immutability of blockchain technology is the issue here.[41] On the blockchain, the smart contract's code cannot be changed. As such, the only course of action is to either accept the offer or reject it. The offeree would become the offeror and the upload would correspond to a new offer.

When the acceptance is implied by the offeree's actions, it might also happen without a formal declaration. More specifically, the offeree's conduct may be seen as a legitimate acceptance of the offer if she begins carrying out the terms of the agreement. It is necessary for the offeree to act in a way that makes it obvious that they accept.[42] Giving up control over a certain sum of money to the code, for instance, may be accepted on a blockchain.[43]

When there is a lag between the offer and acceptance and the parties are not present, the situation becomes more complicated. If that is the case, the applicable legal system determines when a contract is concluded. Three primary guidelines apply generally: The three rules are as follows: 1) the dispatch rule (also called the "mailbox" or "postal" rule), which states that acceptance takes effect at the time of sending; 2) the receipt rule, which establishes that a contract is finished when the offeror receives the acceptance; and 3) the actual notice rule, which states that a contract is formed at the time the offeror learns of the acceptance.[44] In any case, the jurisdictions that follow the actual notice rule lessen the impact by assuming that the offeror learns of the acceptance as

[39] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 120
[40] Ibid
[41] Ibid
[42] JM Smits, *Contract Law: A Comparative Introduction* (Edward Elgar Publishing 2017) 41
[43] Ibid
[44] Ibid

soon as it gets to her address, unless the offeror can demonstrate that she was unable to learn of the acceptance for reasons unrelated to her. [45]

These regulations apply to electronic contracts by keeping in mind the functional equivalence principle.[46] Electronic addresses are used to send and receive data messages in the form of proposals and acceptances. According to the receipt rule, a contract is considered concluded when the electronic message containing the acceptance reaches the offeror's information system and is accessible to them, whereas the dispatch rule suggests that a contract is concluded when the electronic communication representing the acceptance leaves the information system under the control of the offeree. The latter is likewise permissible under the actual notice requirement, barring the offeror from demonstrating that she was not responsible for her inability to learn of the acceptance.[47]

Determining which actions relate to the sending and receiving of the acceptance in the blockchain is the last task. It can be relied on that the offeree transmits her acceptance when, after signing the contract with her private key, she sends the transaction of acceptance from her address to the smart contract's address.[48] Regarding the receipt, this paper contends that the offeror gets the acceptance when the authenticated transaction of acceptance likewise reaches her node.[49]

2.5.2 Form of the Contract

The parties must typically sign the contract when the law requires certain formalities to be followed in order for it to be legal or serve as proof. Electronic signatures are defined as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message" in UNCITRAL Model Law on Electronic Signatures, Art. 2(a).[50] Electronic signatures are defined as "data in electronic form which is attached to or logically

[45] United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce 1996, art 2(1)(a); United Nations Convention on the Use of Electronic Communications in International Contracts 2005, art 4(1)(c)
[46] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 119
[47] Ibid
[48] Ibid
[49] Ibid
[50] UNCITRAL Model Law on Electronic Signatures 2001, art 2(a).

associated with other data in electronic form and which is used by the signatory to sign" under Article 3(10) of the e-IDAS Regulation.[51] Unlike electronic signatures, traditional signatures are based on images and are produced by human interactions with the document. Therefore, the question of when electronic signatures would be deemed to be equal to handwritten signatures arose.

Regarding this, Article 7(1) of the UNCITRAL Model Law on Electronic Commerce states that:

> "Wherever a person's signature is required by law, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any relevant agreement."[52]

Similar clauses can be found in the United Nations Convention on the Use of Electronic Communications in International Conventions and the UNCITRAL Model Law on Electronic Signatures.[53]

Two tiers are used in the e-IDAS Regulation. Three types of electronic signatures are recognized by it: qualified electronic signatures, advanced electronic signatures, and simple electronic signatures. The courts will determine how to evaluate the other signatures; only the latter will have the same weight as a handwritten signature.[54] Users use their private keys to sign transactions on the blockchain. Data messages are transferred between accounts using transactions. Uploading a new smart contract code to the blockchain is the first transaction involving a smart contract. An action to "deploy" is signed by the user. The address of the smart contract code is linked to it and posted to the blockchain. Subsequently, the state of the smart contract code is modified based on the received transactions.

---

[51] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (e-IDAS Regulation) art 3(10).
[52] UNCITRAL Model Law on Electronic Commerce 1996, art 7(1).
[53] UNCITRAL Model Law on Electronic Signatures 2001, art 6; United Nations Convention on the Use of Electronic Communications in International Contracts 2005, art 9
[54] Art. 3 of the e-IDAS Regulation;Art. 25(2) of the e-IDAS Regulation.

A qualified certificate for electronic signatures must serve as the foundation for qualified electronic signatures, which must be generated using a qualified electronic signature production device.[55] A qualified signature creation device is a piece of hardware or software that has been set up to produce an electronic signature that complies with Annex II of the Regulation.[56] Compared to the previous meaning of Directive 1999/93/EC, which made reference to codes or private cryptographic keys, the concept of electronic signature generating data is more ambiguous.[57] Because of the principle of technology neutrality, when the Regulation speaks of electronic signature generating data, it also subtly refers to cryptographic private keys.[58] Blockchain transactions are also signed using cryptographic private keys.

The security and secrecy of the information needed to create the electronic signature are the main concerns of Annex II's criteria. In line with qualified electronic signature generating devices' Art. 29(2). It is assumed that the device complies with Annex II requirements if it meets those criteria. In accordance with Art. 29(2), the Commission has not established reference numbers for standards. Under Art. 30(3), it has, nevertheless, approved Implementing Decision (EU) 2016/650.[59] In fact, according to Art. 30 of the Regulation, relevant public or private entities must certify that the devices comply with Annex II's criteria by conducting a security evaluation process in line with the standards set by the Commission.

An attestation that connects electronic signature validation data to a real person and verifies at least that person's name or alias is known as a qualified certificate for electronic signatures. It satisfies the standards outlined in Annex I of the Regulation and is issued by a certified trust service provider.[60] The purpose of the certificate is to associate the signature with a certain person. The

[55] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 129

[56] Ibid

[57] The directive has since been repealed by the e-IDAS Regulation.

[58] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 130

[59] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (e-IDAS Regulation) arts 29(2), 30(3); Commission Implementing Decision (EU) 2016/650 of 26 April 2016 on the criteria for the security of qualified electronic signature creation devices.

[60] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 130

connection between a signatory and a signature has a higher level of security if the certificate is qualified. A natural or legal person who offers qualified trust services and has been given the qualified status by the supervisory body is known as a qualified trust service provider. Although a set of general requirements has been developed and the idea of technology neutrality has been upheld, a crucial component of a certificate is a specific electronic signature system known as the PKI Infrastructure, which is also utilised to verify signatures in the blockchain.[61] A set of two keys—one public and one private -are given to each user. The secret private key is employed in transaction signing. Everyone is aware of the public key.

Considering the aforementioned, electronic signatures can only be deemed qualified when a qualified certificate and a qualified signature generating device are present, even though blockchain transactions are signed using cryptographic private keys and a PKI infrastructure. As a result, the wallet holding the keys needs to adhere to certain standards that ensure the privacy and security of the data used to create the electronic signature. Additionally, the wallet needs to have a certificate from an accredited provider of trust services attesting to the connection between the keys and a specific identity.

If an electronic signature satisfies the following criteria, it can be deemed advanced if: (a) it is uniquely associated with the signatory; (b) it can identify the signatory; (c) it is generated using electronic signature creation data that the signatory can use under his sole control with a high degree of confidence; and (d) it is linked to the data signed therewith in a way that makes any subsequent changes in the data detectable.[62] This dissertation contends that criteria (a) is satisfied by the use of PKI in the blockchain. Asymmetric cryptography protects data security by preventing unauthorised access to the private and public keys that each user needs to transact. It is true that with asymmetric cryptography, the keys used to encrypt and decode data are different. Because a shared key is not required to decrypt a message, asymmetric cryptography is therefore more secure than symmetric cryptography.[63] The recipient can confirm the message's integrity and provenance with the use of asymmetric cryptography. The sender uses her private key to encrypt the data

[61] Ibid
[62] Art. 26 of the e-IDAS Regulation.
[63] I Bashir, *Mastering Blockchain* (Birmingham – Mumbai 2018)

before sending the hashed version of the encrypted message.[64] Using the public key of the sender, the recipient decrypts the communication. The recipient can be certain that the communication came from the sender and was not altered by third parties if the outcome matches the hash.

Permissioned blockchains, as opposed to permissionless blockchains, are closed networks with pre-identified participants, hence such signatures might be employed in certain scenarios.[65] The fulfilment of requirement (b) may depend on the ability to identify the signatory. This makes sense in B2B situations since companies may be able to afford to outfit themselves with these tools.[66] Further, there is a stronger requirement to use written contracts because it is more likely that their transactions will have a higher economic value than B2C transactions. According to the authors, these systems could also satisfy requirement (c), for example, by using biometric authentication or OTP tokens.[67]

Finally, even after the subscription, requirement (d) calls for safeguards over the integrity of signed data.[68] The usage of asymmetric cryptography in conjunction with the immutable nature of blockchain (due to distribution and concatenated hashes) can guarantee the detectability of any modifications over time. Hashes, which are unique representations of data, are linked to data. Any attempt to tamper would result in the hash changing, as would all following hashes in the chain. Because they are in an electronic format or don't match the requirements for qualified electronic signatures, simple or advanced electronic signatures cannot be denied legal significance or admissibility as evidence in court. The Member States determine when electronic signatures are deemed to be equal to handwritten signatures, according to Recital 49 of the e-IDAS Regulation.[69]

[64] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 130
[65] Ibid
[66] Ibid
[67] Ibid
[68] UE Blockchain Observatory and Forum, *Legal and Regulatory Framework of Blockchains and Smart Contracts* (n 12)
[69] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market [2014] OJ L257/73, Recital 49.

Chapter 3

Smart Contracts and Their Legal Enforceability: Enhancing Compliance, Transparency, and Security in Cross-Border Fintech Transactions

Incorporating smart contracts into international fintech transactions offers a promising solution to the regulatory challenges faced by traditional banking systems. Leveraging blockchain technology, smart contracts can enhance the efficiency, security, compliance, and transparency of cross-border transactions. One of the most significant advantages of smart contracts is their ability to automate regulatory compliance, reducing the risk of human error and non-compliance in complex multinational transactions. By encoding regulations and standards directly into smart contracts, transactions can autonomously adhere to legal requirements, ensuring adherence to applicable laws and regulations.

Blockchain technology has the potential to significantly enhance compliance with complex regulatory frameworks such as Basel III, which imposes stringent risk management and capital adequacy standards on financial institutions.[70] By leveraging blockchain's decentralised and immutable ledger, banks can automate compliance processes and improve data integrity. Smart contracts, which are self-executing contracts with terms directly written into code, enable the embedding of Basel III regulatory requirements directly into the transaction process.[71] This ensures that each transaction is automatically verified for compliance before execution, reducing the need for manual checks and, therefore, human error. Blockchain's real-time verification capabilities provide transparency and an accurate, tamper-proof record of all transactions, which is crucial for risk management and auditing purposes. The enhanced transparency and reliability of data help banks monitor counterparty risks, manage liquidity, and maintain accurate records for reporting.

Further, blockchain facilitates compliance with cross-border transactions by standardising transaction protocols, thereby reducing the complexity of dealing with differing regulatory requirements across jurisdictions. Smart contracts can be tailored to account for varying

[70] Basel Committee on Banking Supervision, *Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems* (Bank for International Settlements 2010, revised June 2011).
[71]Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1083

regulations, ensuring consistent compliance with Basel III and local laws.[72] This capability is particularly beneficial for international trade and finance, where differing regulatory environments pose significant compliance challenges. Blockchain also improves liquidity and capital management by providing real-time data on liquidity positions, allowing banks to maintain the necessary liquidity coverage ratios (LCR) required by Basel III.[73] In the event that liquidity drops below predetermined levels, smart contracts can sound an alarm or take automatic action, allowing for proactive liquidity management. Furthermore, blockchain ensures that banks maintain sufficient capital buffers in compliance with Basel III rules by automating the tracking of capital reserves. Blockchain technology not only lowers the complexity and expense of compliance but also improves the general efficiency and dependability of financial operations by enabling faster cross-border transaction settlements and guaranteeing automated compliance checks.[74]

3.1 Traceability and Transparency

Traceability and transparency are critical for meeting the legal requirements of international financial transactions. Smart contracts, built on blockchain technology, provide an immutable and transparent record of all transactions, accessible to all relevant parties. This ensures that every transaction can be traced back to its origin, facilitating compliance with regulations aimed at fraud detection and money laundering prevention.

For example, Everledger uses blockchain to track the provenance of diamonds, ensuring that every stage of the supply chain is transparent and traceable.[75] This approach can be applied to fintech transactions, where similar strategies can help meet regulatory requirements for transparency in areas such as fraud detection and money laundering prevention. Blockchain technology guarantees transparency and auditability by recording every transaction on a public ledger. This feature is especially helpful in meeting regulatory requirements for know-your-customer (KYC) and anti-money laundering (AML) compliance. Because of this transparency, authorities are better

[72] Ibid

[73] Philipp Paech, 'Securities, Intermediation and the Blockchain—An Inevitable Choice between Liquidity and Legal Certainty' (2016) *Uniform Law Review* 21

[74] Eva Micheler, 'Custody Chains and Asset Values: Why Crypto-Securities Are Worth Contemplating' (2015) 74 *Cambridge Law Journal* 509.

[75] Everledger, 'Technology' (Everledger) https://everledger.io/technology/ accessed 9 August 2024

equipped to stop and identify fraudulent activity by being able to track the history of transactions and confirm the identity of all parties involved.

3.2 Auditing and Reporting

When distributed records are utilised in blockchain networks, all stakeholders involved in managing and holding an asset always have access to the most recent version of the record. The purpose of this record is to guarantee consistency and dependability by preventing inconsistencies with other copies.[76] More data depth is also made possible by blockchain technology, allowing records to hold more complicated information than are now possible in standard accounts.

For instance, ownership of securities is recorded but specific details are missing from a standard brokerage account. It is frequently necessary to produce and maintain more detailed information about these securities in separate records. In a blockchain context, ownership information on a particular share could also include information about the service providers managing it, if the share is encumbered, and if so, who is the holder.[77] Likewise, ownership data can be recorded with self-executing programs, or "smart contracts." Upon maturity, these smart contracts have the ability to autonomously handle interest or dividend payments.[78]

In essence, the industry could transition from maintaining multiple records related to the same asset for different purposes, which are often not properly coordinated, to a single distributed record used by all parties, or at least significantly reduce the number of different records.[79] Because the blockchain record is distributed among all nodes, relevant financial institutions and infrastructures can provide their services related to a specific asset based on the same information. Many significant players in the financial industry have recognized these benefits as a common interest and have formed consortia supporting technology startups like R3CEV and Hyperledger, which are currently developing the necessary blockchain software.[80]

[76] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1080
[77] Ibid
[78] Ibid
[79] P Ortolani, 'Self-enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36 **OJLS** 595, 608.
[80] https://www.r3cev.com and https://www.hyperledger.org.

As a result, the considerable operational complications caused by multiple records could be eliminated in the future, along with the associated uncertainty and costs. The speed of settling transactions would increase, and reporting to the appropriate supervisory bodies would be simplified, as relevant data could be made available by granting supervisors access to the blockchain record.[81]

Smart contracts also facilitate a continuous compliance verification process that aligns with regulatory requirements for timely disclosures and risk management, making real-time audits and reporting easier. Since smart contracts are automated, regulators can receive real-time reports on transaction statuses, significantly reducing the time gap between transaction execution and regulatory reporting. For instance, Deloitte leverages blockchain technology to provide real-time financial transaction auditing services.[82] Smart contracts ensure accurate and current financial records by automating the auditing process, aiding regulatory reporting and compliance.

Through this interface with current auditing systems, transactions may be continuously monitored, giving regulators the ability to see possible problems early on and take proactive measures to rectify them. Because these real-time features guarantee that compliance criteria are regularly completed, they improve the overall efficacy of regulatory oversight.[83] Consequently, the financial industry can anticipate not only a streamlined approach to managing records but also improved transparency, efficiency, and trust in the financial system.

3.3 Security and Flaws

Because there is a greater chance of fraud and illegal changes during cross-border transactions, security is of utmost importance. By using cryptographic techniques to safeguard transactions, smart contracts greatly reduce the possibility of fraud and guarantee data integrity. The state channels of Aeternity, for example, use cryptographic techniques to safeguard private financial information in order to facilitate safe off-chain transactions.[84] Parties can transact quietly and securely through these state channels, which guarantee adherence to data protection laws. As a

[81] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1080
[82] Deloitte, 'Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession' (2020)
[83] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1081
[84] Aeternity, 'State Channels' (Aeternity) https://aeternity.com/state-channels accessed 9 August 2024.

result of transactions being tamper-proof once they are recorded on the blockchain, the immutability of blockchain records further improves security by offering a trustworthy and permanent record that facilitates compliance with legal requirements for transaction integrity.[85]

Even while blockchain technology has significant security advantages, smart contracts are not impervious to flaws. The 2016 DAO assault, in which money was stolen by taking advantage of a coding defect, emphasises the necessity of strong security protocols and extensive code audits to stop these kinds of intrusions.[86] It is necessary to continuously assess and enhance security measures and coding techniques in order to guarantee the security of smart contracts.

Notably, smart contracts lessen the need for middlemen in international transactions, which lowers the chances of errors, delays, and fraud that come with using third parties. Smart contracts improve security and expedite the transaction process by enabling direct transactions between parties. One blockchain-based payment network that demonstrates how smart contracts can be used to enable direct international payments is Ripple.[87] Ripple lessens its reliance on conventional banking middlemen by utilising blockchain technology, which facilitates quicker and more secure transactions.[88] Because there are fewer parties participating in the transaction process, there is less regulatory burden and related compliance expenses, which makes cross-border transactions more efficient and cost-effective. This decrease of intermediaries also streamlines regulatory supervision.

Smart contracts need to be compatible with current legal and financial frameworks in order to properly handle regulatory issues. By guaranteeing compatibility and adherence to existing regulations, interoperability makes it possible for smart contracts to smoothly integrate into the larger financial ecosystem. The goal of projects like Cosmos and Polkadot is to build interoperable blockchain networks that enable communication and cross-chain transactions.[89] Through

---

[85] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*

[86] J I Wong and I Karr, 'Everything You Need to Know About the Ethereum "Hard Fork"' **Quartz** (18 July 2016) http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/ accessed 9 August 2024.

[87] J. Paul, 'How Blockchain Is Transforming the Entire Financial Services Industry' **Forbes** (7 June 2023) https://www.forbes.com/sites/forbestechcouncil/2023/06/07/how-blockchain-is-transforming-the-entire-financial-services-industry/ accessed 9 August 2024.

[88] Ibid

[89] Bitcoin Insider, 'Top 5 Blockchain Projects Driving Cross-Chain Interoperability in 2024' **Bitcoin Insider** (17 July 2024) https://www.bitcoininsider.org/article/252542/top-5-blockchain-projects-driving-cross-chain-interoperability-2024 accessed 9 August 2024.

facilitating the interaction of several blockchain platforms, these projects seek to create a unified ecosystem that promotes regulatory compliance across multiple nations. Furthermore, the development of standardised templates for smart contracts, such as those published by the International Swaps and Derivatives Association (ISDA), can aid in ensuring regulatory compliance by bringing smart contracts into line with recognized legal standards.[90] These templates offer a structure for developing smart contracts that adhere to legal specifications while yet being adaptable to particular transaction circumstances.

3.4 Scalability and Privacy

Virtual currencies and blockchain technology have drawn a lot of attention due to their potential advantages, but they also come with a lot of drawbacks, especially when it comes to illegal activities like money laundering and financing terrorists. Early on in the emergence of virtual currencies, worries about these problems surfaced, prompting legislative actions in states like New York and heated discussion in Europe and beyond.[91]

3.5 Challenges Posed by Blockchain Technology

There are two fundamental features of blockchain technology that greatly aid illicit activity. One benefit over account-based transfers is the increased level of secrecy it offers. It becomes challenging to identify the persons involved in, say, a bitcoin payment due to the rapid nature of international transactions. Furthermore, even in the unlikely event that blockchain-based networks did not maintain anonymity, there would still be no central authority to carry out the tasks necessary for anti-money-laundering laws.[92] In the conventional financial system, it is the duty of intermediaries like banks to identify transaction participants, carry out due diligence, and alert authorities to any questionable activity. [93] However, blockchain networks do not inherently require intermediaries, posing a challenge for regulatory enforcement.

[90] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[91] Ibid
[92] Ibid
[93] Ibid

Intermediation is needed only when blockchain networks intersect with external markets, such as when users exchange virtual currency for fiat money through exchanges.[94] Although these exchanges are the most practical places for regulation to begin, this strategy ignores blockchain activities that don't require exchanging money, such as using virtual currency to pay for products and services directly. Virtual currency exchanges would need to be recognized as regulated entities in order to be regulated, which would open up new regulatory issues and create a new sector of the financial system.[95] Currently, no common strategy has emerged to effectively regulate blockchain networks, and outright bans are impractical due to enforcement challenges.

Blockchain technology is being utilised to develop new payment and money transfer services in spite of these challenges, with providers functioning as middlemen akin to virtual currency exchanges. These middlemen are amenable to regulation and make good targets for anti-money-laundering policies, such as "know-your-customer" (KYC) mandates. Establishing precise roles for enforcing these regulations is essential, nevertheless, especially in situations when the intermediary's function is ambiguous or shared. For example, people in charge of the platform should be accountable for compliance in blockchain-based remittance services that depend on nearby merchants for cash transactions, making sure that access and handling are properly managed.[96]

3.7 Technical and Legal Constraints of Smart Contracts

Smart contracts offer numerous benefits but also face technical and legal challenges that must be addressed for successful implementation. Scalability and privacy are two primary technical issues that need resolution to comply with regulations. Scalability challenges, such as those seen during the 2017 CryptoKitties craze on Ethereum, highlight the need for solutions that can handle high transaction volumes without compromising efficiency.[97] Layer 2 solutions like zk-Rollups and

[94] EU Commission, 'Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 [etc]' COM (2016) 450 final, 5 July 2016
[95] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[96] Ibid
[97] BBC News, 'Bitcoin Hits Record High Amid Currency Concerns' **BBC News** (15 December 2017) https://www.bbc.com/news/technology-42237162 accessed 9 August 2024.

Optimistic Rollups aim to enhance scalability by offloading transactions from the main blockchain while maintaining security and decentralisation.[98]

Privacy concerns are also paramount, especially in jurisdictions with stringent data protection laws. Blockchain platforms prioritising privacy demonstrate how smart contracts can be adapted to protect user information while ensuring compliance with privacy regulations. Legally, smart contracts are recognized and accepted differently across jurisdictions. While some countries, such as Malta and Switzerland, have established favourable legal frameworks for smart contracts, others lack clear legal structures, necessitating ongoing efforts to harmonise international legal frameworks.

Malta has emerged as a leading jurisdiction for blockchain technology and smart contracts. In 2018, Malta introduced a comprehensive legal framework through the Virtual Financial Assets Act (VFAA), the Technology Arrangement and Services Act (TAS), and the Innovative Technology Arrangement and Services Act (ITAS).[99] These laws provide a clear regulatory environment for blockchain technology, including smart contracts. Malta's approach includes detailed provisions for the creation, execution, and enforcement of smart contracts, thus offering legal certainty and promoting innovation within its jurisdiction. This proactive stance has attracted numerous blockchain businesses to Malta, reinforcing its position as a hub for technological advancement.

Switzerland also stands out with its supportive regulatory environment, particularly through its "Crypto Valley" in Zug. Swiss authorities have implemented regulations that align with blockchain technologies and smart contracts, integrating them into the existing legal framework. The Swiss Financial Market Supervisory Authority (FINMA) has issued guidelines that address various aspects of blockchain technology, including initial coin offerings (ICOs) and smart contracts.[100]

---

[98] Amanda J Sharp and Orly Lobel, 'Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens' (2023)
[99] Virtual Financial Assets Act (VFAA) 2020 (Malta); Technology Arrangement and Services Act (TAS) 2021 (Malta); Innovative Technology Arrangement and Services Act (ITAS) 2022 (Malta).
[100] The Swiss Financial Market Supervisory Authority (FINMA), 'Guidelines on Initial Coin Offerings (ICOs) and Blockchain Technology' (FINMA, 2018) https://www.finma.ch/en/news/2018/02/20180216-mm-ico/ accessed 9 August 2024

The clarity provided by these regulations fosters a secure environment for smart contract applications, enhancing Switzerland's reputation as a global leader in blockchain innovation.

In contrast, many other countries still grapple with the integration of smart contracts into their legal systems. For example, in the United States, the legal status of smart contracts can vary significantly between states. While some states like Arizona and Nevada have enacted laws recognizing smart contracts and blockchain records, others have yet to establish clear legal frameworks.[101] This patchwork of regulations creates uncertainty for businesses operating across state lines and complicates the enforcement of smart contracts.

Similarly, in the European Union, efforts are underway to create a cohesive legal framework for blockchain technology, but progress has been uneven. The EU has initiated several projects, such as the European Blockchain Partnership and the EU Blockchain Observatory and Forum, to address these challenges.[102] However, the lack of a unified approach across member states means that businesses face regulatory fragmentation when dealing with smart contracts and blockchain technology.

Globally, the absence of standardised international regulations poses additional challenges. The lack of a consistent legal framework makes it difficult to address cross-border issues related to smart contracts, such as jurisdictional disputes and enforcement challenges. To overcome these obstacles, international organisations and regulatory bodies are working towards harmonising regulations and establishing global standards. Initiatives like the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce aim to provide a foundation for the recognition and enforcement of electronic contracts, including smart contracts, across different jurisdictions.[103]

3.8 The Role of Regulatory Sandboxes

[101] Arizona Revised Statutes § 44-7001 (Arizona) (2017); Nevada Revised Statutes § 719.240 (Nevada) (2017).
[102] European Blockchain Partnership (European Commission, 2018) https://ec.europa.eu/digital-strategy/our-policies/european-blockchain-partnership_en accessed 9 August 2024; EU Blockchain Observatory and Forum(European Commission, 2018) https://www.eublockchainforum.eu/ accessed 9 August 2024.
[103] United Nations Commission on International Trade Law (UNCITRAL), Model Law on Electronic Commerce (1996).

Regulatory sandboxes provide a controlled environment for testing innovative fintech products, including smart contracts. Sandboxes allow companies to test new technologies under regulatory supervision, enabling authorities to assess compliance and address potential issues before broader deployment. Countries like Singapore and the UK have implemented regulatory sandboxes to promote innovation within a regulated framework. These sandboxes offer fintech companies the opportunity to refine their smart contract solutions while regulators gain valuable insights into the technology's implications.

While smart contracts offer numerous benefits, they also raise ethical and security concerns that need to be addressed. The immutable nature of blockchain records means that errors or malicious code in smart contracts can have irreversible consequences. Ensuring the security of smart contracts requires rigorous code auditing and testing to prevent vulnerabilities that could be exploited by hackers. Additionally, the automation of contractual agreements raises ethical questions about accountability and control. As smart contracts replace human intermediaries, it is essential to consider who is responsible when things go wrong and how to address disputes that may arise. These considerations are critical for fostering trust and ensuring the responsible use of smart contracts.

Cross-border fintech transactions face significant regulatory challenges that impede operational efficiency and disrupt the smooth flow of financial activities. Navigating different regulatory frameworks across jurisdictions increases compliance costs and causes delays in settlement processes for fintech companies, leading to inefficiencies. Additionally, regulatory uncertainty and compliance difficulties discourage investment in international fintech projects, limiting innovation and market expansion.

The absence of well-defined regulatory frameworks and clear compliance requirements undermines investor trust and hinders the global scalability of fintech solutions. Security concerns such as fraud, cybersecurity threats, and illegal activities, compounded by inconsistent regulatory standards, pose further risks to the financial system's integrity and stability.

To fully realise the potential of cross-border fintech transactions and enhance operational efficiency in the global financial ecosystem, promoting regulatory clarity and harmonisation is crucial. This chapter will examine how blockchain technology, particularly smart contracts, can

address these challenges while adhering to data protection principles, focusing on compliance with the General Data Protection Regulation (GDPR).[104]

Chapter 4

Balancing Data Privacy and Blockchain Technology in Cross-Border FinTech Operations

Fintech companies face considerable problems in the field of cross-border fintech transactions due to the inherent complexity and uncertainty around regulatory compliance. These businesses have to negotiate a complex web of regulations that differ significantly between several jurisdictions, each of which has its own set of laws and regulations. For example, complying with various privacy and data protection rules is frequently necessary when sending sensitive and private financial information across international boundaries. One example is the General Data Protection Regulation (GDPR) of the European Union, which sets strict rules for data management that may conflict with national data privacy legislation.[105] Fintech firms face a significant difficulty as a

[104] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.
[105] Ibid

result of this regulatory diversity; in order to assure compliance, they must carefully manage these subtleties. Fintech organisations must implement strong data governance systems that integrate encryption, anonymization, and safe data storage techniques in order to adhere to many data protection regulations.[106] In order to ensure compliance across jurisdictions, they must also create clear data processing agreements with its overseas partners. Sustaining client confidence and protecting the integrity of international fintech transactions need the effective handling of privacy and data protection concerns.

The rising costs of operations and compliance related to following different regulatory regimes present another big obstacle.[107] Fintech companies may find it challenging to expand globally due to these regulatory expenditures. The problem is further complicated by the absence of uniform and clear regulatory frameworks, which can lead to regulatory ambiguity and deter investment in cross-border fintech ventures while also impeding innovation and growth.

4.1 Impact on Operational Efficiency

Operational efficiency in cross-border fintech transactions is also directly impacted by the ambiguity and complexity of regulatory compliance.[108] Settlement procedures frequently experience delays and inefficiencies as a result of regulatory ambiguity and compliance issues. An example of this would be the difficulty for businesses to function effectively and win over investors due to ambiguous regulatory requirements, these delays have the potential to undermine investor confidence and impede the global scalability of fintech solutions. As such, there are numerous obstacles that fintech companies must overcome in order to grow their market share and succeed internationally.

4.2 Importance of Regulatory Clarity and Harmonization

The fintech industry places great importance on regulatory clarity and uniformity in light of these problems. By fostering a stable and predictable business environment, well-defined and uniform regulatory frameworks may foster innovation and facilitate the growth of fintech enterprises. A

[106] Ibid
[107] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[108] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.

crucial component of this regulatory clarity is the incorporation of smart contracts into the current legal frameworks. For instance, the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) and the Uniform Electronic Transactions Act (UETA) in the US offer a framework for accepting electronic contracts and signatures.[109] In a similar vein, the General Data Protection Regulation (GDPR) of the European Union contains particular regulations pertaining to data privacy and protection that affect the use of smart contracts.[110]

Other countries, such as Singapore and Switzerland, are leading the way in developing laws that specifically address smart contracts and blockchain technology.[111] Despite these advancements, several challenges persist. Cross-border transactions often involve multiple legal systems, leading to jurisdictional complexities that complicate the enforcement of smart contracts.[112] Courts may find it challenging to interpret the code, particularly when disputes arise, and ensuring that smart contracts comply with the diverse legal requirements of different jurisdictions remains a significant hurdle.

Ultimately, enhancing regulatory clarity and harmonisation can streamline compliance processes, improve operational efficiency, and reduce transaction costs in cross-border activities. By creating a more coherent regulatory environment, governments and regulatory bodies can foster innovation, support the growth of fintech companies, and facilitate the global adoption of smart contracts in cross-border transactions.

Revolut, a prominent international fintech enterprise, adeptly navigates an intricate regulatory landscape concerning data protection in cross-border transactions.[113] Revolut is subject to a number of data privacy laws due to its broad worldwide operations, including the General Data privacy Regulation (GDPR) of the European Union and data protection laws in other

[109] Electronic Signatures in Global and National Commerce Act (E-SIGN Act) 15 USC § 7001 (2000); Uniform Electronic Transactions Act (UETA) (1999).
[110] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.
[111] Singapore: Electronic Transactions Act (Cap 88) (2002); Payment Services Act 2019 (Act 2 of 2019); Securities and Futures Act (Cap 289) (2001); Digital Payment Token (DPT) Regulation (2020); Switzerland: Federal Act on Data Protection (FADP) (2020); Federal Act on the Financial Market Infrastructure (FinMIA) (2018); Federal Act on Collective Investment Schemes (CISA) (2020); Swiss Blockchain Act (2021).
[112] B2C2 Ltd v. Quoine Pte Ltd
[113] Revolut, 'Privacy Policy' https://www.revolut.com/legal/privacy/ accessed 9 August 2024.

jurisdictions.[114] Revolut faces a great deal of difficulty in complying with the GDPR's strict regulations, which include the principles of data minimization, accuracy, and accountability, given that it handles and maintains enormous volumes of personal data in numerous jurisdictions.[115] Revolut has put in place a complex data governance architecture to handle these issues and guarantee GDPR compliance while accommodating local laws. This entails using cutting-edge encryption technology to safeguard private information both during transmission and storage, shielding it from breaches and unwanted access.[116] In accordance with the GDPR's data protection guidelines, the organisation also employs pseudonymization techniques to lower the possibility of re-identifying specific persons from stored data.

Furthermore, Standard Contractual Clauses (SCCs) must be used for data transfers between jurisdictions due to Revolut's global operations.[117] This ensures that personal data is safeguarded even when transmitted outside of the EU. In an effort to strengthen data security, Revolut has created a network of Data Protection Officers (DPOs) who manage compliance initiatives in various areas, offering specialised knowledge and guaranteeing that the business complies with market-specific legal requirements.[118] Revolut still has to deal with persistent issues with cross-border data management, such as making sure that data breaches are handled quickly and effectively. In order to limit any harm to users and preserve regulatory compliance, the organisation has built a thorough incident response strategy that includes mitigation measures and notification protocols for quickly addressing any breaches.[119]

4.3 Security Challenges in Cross-Border FinTech Transactions

Cross-border fintech transactions are significantly at risk from fraud, cybersecurity threats, and illegal activities including money laundering and terrorist financing due to inconsistent regulatory standards. Malicious actors may take advantage of regulatory weaknesses and disjointed supervision mechanisms to create loopholes that compromise the integrity and stability of the

[114] Ibid
[115] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.
[116] Revolut, 'Privacy Policy' https://www.revolut.com/legal/privacy/ accessed 9 August 2024.
[117] Revolut, 'Data Privacy for Candidates' https://www.revolut.com/en-IE/legal/data-privacy-for-candidates/ accessed 9 August 2024.
[118] Ibid
[119] Ibid

financial system. These security flaws are made worse by the lack of uniform regulatory monitoring, which undermines customer confidence in international fintech services.[120]

Furthermore, as blockchain technology spreads, new security issues arise, namely with regard to the transparency and immutability of transaction records on decentralised ledgers. The widespread implementation of blockchain-based finance solutions is hindered by regulatory uncertainty surrounding blockchain acceptance and usage, despite the inherent security benefits that these systems offer, such as distributed consensus processes and cryptographic encryption. Therefore, tackling security issues and improving consumer protection in cross-border fintech transactions require coordination between regulatory bodies, industry stakeholders, and technology developers.

Cybersecurity threats and fraud pose significant challenges to the security of cross-border fintech transactions, primarily due to inconsistent regulatory standards across jurisdictions.The lack of uniform regulatory standards creates vulnerabilities that increase the risk of fraud, cyberattacks, and other malicious activities.[121] Malicious actors often exploit these regulatory gaps and fragmented supervision mechanisms to compromise the integrity of the financial system. Inconsistent standards can lead to weak points in the cybersecurity defences of fintech companies, allowing cybercriminals to launch attacks that may result in significant financial losses, data breaches, and damage to the reputation of affected companies.[122] This fragmented regulatory landscape complicates efforts to establish comprehensive cybersecurity measures, making it difficult for companies to protect sensitive financial data effectively. As a result, fintech firms must navigate a complex web of regulations and adopt robust security practices to mitigate the risks associated with cybersecurity threats and fraud in cross-border transactions.

4.4. Impact of Blockchain Technology on Security

Blockchain technology provides considerable promise to improve security in cross-border finance transactions, notwithstanding the limitations faced by cybersecurity threats. The decentralised

[120] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[121] Ibid
[122] Ibid

structure of blockchain, which disperses power over a network of nodes and does away with the necessity for a central authority, is one of its main advantages.[123] Decentralisation lessens the possibility of a single point of failure and increases the difficulty of system compromise by malevolent actors. Furthermore, by prohibiting illegal adjustments, the immutability of blockchain records maintains data integrity.[124] A transaction that is registered on the blockchain creates a permanent, unchangeable record that improves security because it cannot be removed or changed. This function is especially helpful in preserving the confidentiality of financial transactions and shielding private information from unwanted access.

Blockchain technology not only provides immutability and decentralisation, but also transparency, enabling all network users to view transactions. Because participants in cross-border transactions can independently verify transaction information and assure regulatory compliance, this transparency promotes confidence and accountability amongst parties involved in those transactions. As previously discussed, real-time auditing of transactions improves the system's overall security and lowers the risk of fraud. Through the utilisation of these characteristics, blockchain technology may effectively tackle several significant cybersecurity obstacles in cross-border fintech transactions, offering a more robust and safe structure for carrying out global financial operations.[125] To counter emerging risks and guarantee the security of cross-border transactions, fintech companies must, nevertheless, continue to develop and execute comprehensive security measures and maintain a high level of alertness.

Fintech companies can enhance their compliance procedures by emulating Revolut's strategy for operational efficiency in the face of regulatory obstacles. Revolut has incorporated automated compliance tools that help monitor and manage adherence to various standards across several jurisdictions in order to streamline regulatory compliance[126]. By providing real-time compliance checks, these solutions lessen the human labour involved in regulatory reporting and speed up the process of responding to changes in the law. Revolut, for instance, manages transaction monitoring

[123] Ibid

[124] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.

[125] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*

[126] Revolut, *Annual Report 2022* (Report, Revolut 2022) https://cdn.revolut.com/pdf/annualreport2022.pdf accessed 9 August 2024.

and reporting requirements through automated systems, which improves its capacity to identify and quickly address possible concerns.[127]

Furthermore, Revolut's integrated digital platform facilitates international transactions by offering a smooth user interface. One of the main inefficiencies in foreign payments is addressed by the platform's integration of real-time currency exchange and quick money transfers, which lowers transaction costs and operational delays. Revolut also makes use of cutting-edge technology to provide quick, low-cost international transactions, which improves overall operating efficiency.[128] The company's strong alliances with international financial networks, which aid in the rapid and seamless processing of cross-border payments, further bolster its capacity to provide these services on a large scale.

Revolut must constantly adjust to changing legal restrictions, though, and this can occasionally lead to operational complications. For example, modifications to operational procedures or updates to compliance systems may be necessary due to regulatory changes in various markets. Revolut tackles these issues by upholding an agile and adaptable compliance architecture that allows the business to minimise operational disruptions and promptly respond to new regulatory requirements.[129] In addition to improving overall operating efficiency, the company's robust customer service infrastructure is essential for handling any problems pertaining to transaction delays or regulatory compliance.

Data Protection in Cross-Border FinTech Transactions

The GDPR, which sets stringent regulations on data protection and has an impact on how blockchain technology is utilized within the EU, raises significant issues over data privacy when it comes to blockchain technology.[130] Blockchain must process just the necessary data in order to comply with the data minimization principle. The immutability of blockchain records makes it challenging to comply with the GDPR's right of deletion.[131] It is also challenging to identify the

[127] Ibid
[128] Ibid
[129] Ibid
[130] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.
[131] Ibid

data controllers and processors in a decentralized system under GDPR. Many strategies can be employed to address GDPR compliance, including storing personal data off-chain while using blockchain for transaction verification, encrypting and pseudonymizing data to improve privacy, and integrating privacy-enhancing technologies into blockchain system design from the start to balance transparency and data protection.

4.5 Privacy Regulations and Cross-Border Transactions

Transmitting sensitive financial data between countries with different privacy and data protection regulations is known as cross-border fintech transactions, and it poses serious difficulties for businesses that operate globally. The General Data Protection Regulation (GDPR) of the European Union is one of the most significant regulatory regimes affecting these transactions.[132] Fintech companies have compliance issues as a result of the GDPR's strong data protection standards, which may contradict with foreign privacy legislation.[133] For example, the GDPR compels firms to seek consumers' explicit consent before using their data and demands stringent safeguards to protect personal data. Fintech organisations frequently encounter challenges in adhering to the strict criteria of GDPR while navigating an assortment of differing privacy regulations. Because of this, fintech companies that conduct cross-border business need to create thorough data protection plans in order to properly handle these intricate regulatory environments and secure sensitive financial data.

4.6 Data Protection Principles and Blockchain

Although blockchain technology has many advantages, it also needs to follow the GDPR's guidelines for data protection, which include minimising data. Blockchain systems, which by nature retain vast volumes of data to maintain security and transparency, face difficulties in complying with this principle, which states that only data that is necessary should be processed. Furthermore, the GDPR's right to erasure—which requires data controllers to erase personal data upon request—confers with the immutability of blockchain.[134] Given that blockchain technology

[132] Ibid
[133] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.
[134] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.

is meant to provide everlasting records that are immutable, this poses a serious issue for its application. Finding the data controllers in a decentralised system is also crucial since it might be challenging to assign accountability in a blockchain network for data processing and GDPR compliance.[135] These difficulties call for creative solutions to bring blockchain technology into compliance with data protection regulations.

4.6.1 Addressing Data Protection Challenges

ain so that transaction verification is the main function of the blockchain.[136] Because sensitive data is kept off the immutable ledger, this method strikes a compromise between the requirements for data protection and the necessity for transparency.

Another practical method of guaranteeing adherence to data protection laws is to integrate technology that improves privacy into the design of blockchains. Additional levels of privacy and security can be offered via methods like safe multi-party computing and zero-knowledge proofs, which enable transactions to be validated without disclosing personal information.[137] Fintech organisations may take advantage of blockchain's advantages while complying with strict data protection regulations thanks to these solutions.[138] Fintech companies may solve data protection issues in cross-border transactions and guarantee compliance with changing privacy requirements by implementing these techniques, which will ultimately build trust and confidence among regulatory bodies and customers alike.

Revolut takes security very seriously since it tackles the many risks that come with doing cross-border fintech transactions. To counter dangers including identity theft, phishing attempts, and financial fraud, the organisation has made significant investments in cutting-edge fraud detection and prevention systems.[139] Revolut can quickly detect and stop fraudulent activity by using real-

[135] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[136] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[137] I Shaki and T Petr, 'Towards a Diverse Future: The Impact of Innovation and Technology on Sustainable Development' (2023) 37 *Advances in Climate Change Research* 262 https://www.sciencedirect.com/science/article/pii/S2214212623002624 accessed 9 August 2024.
[138] Ibid
[139] Revolut, *Annual Report 2022* (Report, Revolut 2022) https://cdn.revolut.com/pdf/annualreport2022.pdf accessed 9 August 2024.

time monitoring and sophisticated machine learning algorithms.[140] This improves transaction security and keeps user accounts safe from unwanted access.

By utilising the decentralised nature of blockchain technology to create a safe and transparent record for cryptocurrency transactions, Revolut's adoption of this technology significantly strengthens its security posture. This technology makes it harder for bad actors to change or tamper with data by lowering the possibility of single points of failure and guaranteeing that transaction records are unchangeable. Regulating blockchain technology is still fragmented, meanwhile, with different rules and criteria in different countries.[141] Revolut needs to make sure that its blockchain implementations adhere to regional laws while upholding strong security protocols in order to address this.

The cybersecurity of the company's digital infrastructure is another issue. Revolut regularly performs penetration tests and security audits to find and fix security flaws in its systems.[142] Revolut's incident response plan also consists of comprehensive procedures for handling cybersecurity breaches, guaranteeing that the business can react to possible dangers and lessen their effects.[143] Revolut's all-encompassing security strategy aids in preserving user confidence and protecting the integrity of its international transactions.

4. 7 Legal Recognition of Smart Contracts

Existing frameworks that support the acknowledgment of electronic contracts and signatures, such as the Uniform Electronic Transactions Act (UETA) and the United States' Electronic Signatures in Global and National Commerce Act (E-SIGN Act), lend support to the legal recognition of smart contracts.[144] In certain jurisdictions, these rules validate the legality of digital contracts, enabling smart contracts to serve as legally enforceable instruments. Cross-border transactions do, however, present jurisdictional issues since smart contract enforcement may become more difficult due to various legal frameworks. Establishing uniform enforcement and acceptance of these digital

---

[140] Ibid
[141] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review*
[142] Revolut, *Annual Report 2022* (Report, Revolut 2022) https://cdn.revolut.com/pdf/annualreport2022.pdf accessed 9 August 2024.
[143] Ibid
[144] Uniform Electronic Transactions Act (UETA) 1999; Electronic Signatures in Global and National Commerce Act (E-SIGN Act) 2000, 15 USC §§ 7001-7031.

agreements is difficult due to variations in national legal interpretations and legislation. In order to ensure smart contracts' smooth integration into global trade and promote a unified legal framework, it is imperative that these jurisdictional concerns are addressed as the technology continues to gain traction.

4.7.1 Data Protection and Smart Contracts

In order to guarantee that data processing complies with stringent privacy standards, smart contracts must abide by data protection rules, such as those specified in the General Data Protection Regulation (GDPR) of the European Union.[145] Safeguarding personal data and preserving the confidence of parties participating in cross-border transactions depend on compliance with GDPR. By automating compliance with data protection laws, such as gaining consent for data processing, smart contracts can lower the risk of non-compliance and improve data security. Smart contracts can guarantee that transactions are carried out clearly and securely, fulfilling regulatory obligations while safeguarding individuals' privacy, by incorporating data protection mechanisms into their code. This feature enhances the integrity and dependability of smart contract-based systems in managing sensitive data in addition to supporting legal compliance.

Revolut's dedication to striking a balance between privacy and transparency is demonstrated by its creative application of blockchain technology in data protection.[146] Blockchain provides immutability and transparency, which are advantageous for guaranteeing the integrity of transactions, but it also poses problems for data protection, especially when it comes to GDPR compliance. Revolut tackles these issues by utilising blockchain technology for transaction validation and pseudonymization and encryption methods to safeguard personal information.[147]

---

[145] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.

[146] Revolut, *Annual Report 2022* (Report, Revolut 2022) https://cdn.revolut.com/pdf/annualreport2022.pdf accessed 9 August 2024.

[147] Revolut, 'Privacy Policy' https://www.revolut.com/legal/privacy/ accessed 9 August 2024.

By using this strategy, the organisation is able to preserve blockchain transaction transparency while protecting confidential customer data.

Revolut uses techniques like off-chain storage to handle GDPR's right to erasure, which is incompatible with blockchain's immutability.[148] Sensitive data is kept apart from the blockchain so that, in compliance with GDPR regulations, personal data can be removed or changed while blockchain records are kept for transaction verification. Furthermore, Revolut integrates technologies that improve privacy, such as zero-knowledge proofs, into its blockchain platforms to validate transactions without disclosing personal information.[149]

Revolut uses these tactics to take use of blockchain technology's benefits while navigating the complexity of data protection laws. Revolut maintains a balance between privacy and openness to enable it to offer safe and legal services to its user base worldwide, building confidence and trust with its clients.

4.7.2 Addressing GDPR Compliance in Blockchain and Smart Contracts

If technology's design does not take into account the rights of data subjects as outlined by the General Data Protection Regulation (GDPR), it may be difficult for that technology to comply with the regulations. This implies that blockchain technology may not be appropriate for handling personal data because of its built-in capabilities, rather than that it must be modified to comply with GDPR regulations. The seeming inconsistency between the core tenets of blockchain technology and the principles of EU data protection law prompts questions about the efficacy of the GDPR—which is supposed to be technology-neutral—in protecting the vast amounts of data stored on blockchains.[150]

There are worries that the technological neutrality of the GDPR may not translate into sufficient protection for blockchain data, as mentioned in Recital 15 of the GDPR.[151] Regarding how

[148] Ibid
[149] Ibid
[150] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.
[151] Recital 15, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

effectively blockchain technology complies with data protection regulations, there is serious worry, even though the European Commission is optimistic that the GDPR would encourage continued innovation.[152] The dual nature of blockchain as both a promising and challenging technology in terms of data protection is reflected in David Meyer's 2018 article, Blockchain Technology and EU Privacy Law, as well as in the observations made by the Committee on Civil Liberties, Justice, and Home Affairs (LIBE) of the European Parliament.[153]

On the other hand, a closer examination of the fundamental ideas behind blockchain technology reveals that, despite their differing approaches, the objectives of the GDPR and blockchain are similar. Blockchain functions as a Personal Information Management System (PIMS) and Privacy Enhancing Technology (PET).[154] Because of its strong encryption techniques, it may be able to provide even more extensive data protection than the GDPR. Although a lot of personal data pertaining to persons in the EU is covered by the GDPR, it is crucial to remember that blockchain technology is merely a tool that may be used for a variety of purposes and does not itself handle data.[155] Therefore, whether blockchain technology's particular implementations comply with the GDPR rather than whether the technology itself is subject to the legislation is the pertinent point. These subtle considerations are highlighted in Enza Cirone's 2021 essay, Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?, which explores the intersection of blockchain technology and GDPR rules.[156]

Whether or not data kept on blockchains meets GDPR requirements for personal data is a crucial question to answer. The GDPR presents the terms anonymization and pseudonymization as well as defines personal data. An assessment of whether blockchain data falls within these categories is prompted by this definition. The immutability of blockchain technology poses a challenge to the GDPR's right to be forgotten since it makes it hard to erase data after it has been recorded.[157]

---

[152] European Commission, 'Data Protection: Better Rules for Small Businesses' (European Commission, 2018) https://commission.europa.eu/document/download/e167c4ce-8d28-47bf-84bd-170edcf28333_en?filename=data-protection-factsheet-sme-obligations_en.pdf accessed 9 August 2024.

[153] David Meyer, 'Blockchain Technology is on a Collision Course with EU Privacy Law' (International Association of Privacy Professionals, 12 March 2018) https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law accessed 9 August 2024

[154] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.

[155] Ibid

[156] Ibid

[157] Ibid

Furthermore, it can be difficult to assign liability for GDPR compliance in a decentralised blockchain system. The identifiability criterion, which is the foundation for the GDPR's requirements for personal data, is still undefined because the law does not outline the precise components needed to evaluate identification risk.[158] Recital 26 of the GDPR says that as technology develops, it may become harder to distinguish between personal and non-personal data, especially when methods for re-identifying data subjects are used.[159]

In terms of anonymization and pseudonymization, anonymous data is not covered by the GDPR since it cannot be linked to a specific person. Pseudonymous data, however, is still considered personal information if it can be connected to a specific person via an identifier.[160] Since the GDPR defines anonymization as information that cannot be linked to a specific individual, data that has been irrevocably anonymized may not be covered by the GDPR.[161] This means that data may not be governed by the GDPR's rules if it is suitably anonymized.

4.7.3 Anonymization and Pseudonymization

If some technologies are not built to support data subjects' rights, they can have trouble complying with the General Data Protection Regulation (GDPR). This does not imply that blockchain technology has to be modified to comply with GDPR regulations; rather, it raises the possibility that some of blockchain's core features make it unsuitable for processing personal data. The question of whether the GDPR, which is meant to be technology-neutral, can effectively secure the vast amounts of data held on blockchains arises from the seeming inconsistency between the fundamental architecture of blockchain technology and EU data protection legislation.[162] Concerns are raised by Recital 15 of the GDPR regarding the possibility that its technology-neutral approach may not adequately protect data in blockchain systems.[163] As mentioned in David Meyer's 2018

[158] Ibid
[159] General Data Protection Regulation (EU) 2016/679, Recital 26
[160] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.
[161] Ibid
[162]David Meyer, 'Blockchain Technology is on a Collision Course with EU Privacy Law' (International Association of Privacy Professionals, 12 March 2018) https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law accessed 9 August 2024
[163] General Data Protection Regulation (EU) 2016/679, Recital 15

article and the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE) report, many observers have expressed concerns about the compatibility of blockchain technology with data protection laws, despite the European Commission's hope that GDPR will support continued innovation.[164]

However, an analysis of the fundamental ideas behind blockchain technology shows that while both the GDPR and blockchain have similar goals, their methods differ. Blockchain operates as a Personal Information Management System (PIMS) and is considered a Privacy-Enhancing Technology (PET). Compared to the GDPR's requirements, its robust encryption capabilities may provide a higher level of data protection. All personal data pertaining to individuals in the EU is subject to the GDPR, however it is important to understand that blockchain technology serves several purposes and is not a data processing entity in and of itself.[165] Therefore, whether or not blockchain applications comply with GDPR criteria is more important than whether or not blockchain technology itself is subject to the regulation. Blockchain and the General Data Protection Regulation: written by Enza Cirone in 2021, examines this confluence and emphasises its complexity.[166]

Whether or not data kept on blockchains qualifies as personal data under GDPR criteria is an important factor to take into account. In addition to defining personal data, the GDPR presents ideas like anonymization and pseudonymization. This begs the question of what constitutes personal data on blockchain. The unchangeable nature of blockchain technology makes the GDPR's right to be forgotten more challenging because it makes it more difficult to erase data after it has been stored. Furthermore, it can be difficult to determine who in a decentralised blockchain context is in charge of GDPR compliance. A data controller is defined by the GDPR as the organisation that chooses the goals and methods of data processing, regardless of technology.[167]

---

[164] David Meyer, 'Blockchain Technology is on a Collision Course with EU Privacy Law' (International Association of Privacy Professionals, 12 March 2018) https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law accessed 9 August 2024

[165] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.

[166] Ibid

[167] General Data Protection Regulation (Regulation (EU) 2016/679) [2016] OJ L119/1, applicable from 25 May 2018.

Because there is not a single controlling entity in decentralised systems, identifying the data controller needs to be done case-by-case.

Finding the data controller in decentralised networks—like public blockchains—is especially challenging as these networks are dispersed and open, lacking a single body to oversee data processing choices. According to experts, since users control the data processing procedures, they may be regarded as data controllers when they contribute data for commercial purposes.[168] Submissions of personal data for non-commercial purposes, however, may qualify for the "household" exemption; this is not the case here.[169]

Certain situations may include the sharing of data processing tasks among several parties, necessitating explicit agreements on their data protection obligations. The intricacies of joint controllership have been brought to light by recent decisions rendered by the Court of Justice of the European Union (CJEU), especially with regard to responsibility definition and accountability.[170]

The immutability of blockchain technology and the GDPR's right to erasure clash because blockchain data is recorded forever and is difficult to edit or remove. This intrinsic property of blockchain appears to run counter to GDPR Article 16 and 17's provisions for data erasure or modification.[171] But according to the European Data Protection Board's (EDPB) and the Court of Justice of the European Union's (CJEU) interpretive guidelines, erasing data need not always mean total destruction. Even in cases when total deletion is not practical, the GDPR permits the possibility of attaining an outcome that is nearly identical to erasure.[172] Cryptographic techniques such as "chameleon hashes" may provide solutions by enabling modifications to blockchain records while preserving data integrity.

Chapter 5
Stakeholder Perspectives and Recommendations

[168] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.
[169] General Data Protection Regulation (EU) 2016/679, Art 2(2)(c)
[170] Case C-25/17, Jehovas Zeugen (Witnesses) in Deutschland eV v Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [2018] ECR I-0000
[171] General Data Protection Regulation (EU) 2016/679, Art 16 and Art 17
[172] Ibid

Smart contracts, which leverage blockchain technology, have emerged as a promising means to expedite cross-border fintech transactions. They offer substantial benefits to regulators and industry stakeholders by improving transparency, automating compliance processes, and reducing transaction costs. However, for smart contracts to achieve widespread adoption, regulatory issues must be addressed, and established legal standards must be upheld. This chapter explores stakeholders' perspectives on the role of smart contracts in regulatory compliance and provides recommendations to facilitate their integration into international trade.

5.1 Stakeholder Perspectives

The underlying technology of blockchain has advanced dramatically, covering a broad range of financial assets in addition to its original uses in virtual currencies. The possibility of directly issuing, trading, and settling bonds or shares on blockchain networks is part of this expansion, and it has the potential to eventually replace clearinghouses, settlement systems, and existing stock exchanges.[173] With this technology, even central banks could issue fiat money, and derivative contracts could be concluded, administered, and settled within blockchain networks.[174] These capabilities represent a significant shift towards what can be termed "blockchain financial networks."[175] The financial sector has already invested over $1.4 billion in research on these networks, indicating that significant cost and productivity improvements are anticipated.[176] By 2022, banks anticipate that they might save $15–20 billion on infrastructure, and Fintech companies are well-positioned to provide cutting-edge blockchain services.[177] Notwithstanding this excitement, blockchain technology adoption is still in its infancy and developing, with usage ranging from the revolutionary ideas behind Bitcoin and Ethereum to more subdued applications like updating IT infrastructure.

[173] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1075
[174] Ibid
[175] Ibid
[176] World Economic Forum, 'The Future of Financial Infrastructure' (August 2016) https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/ accessed 9 August 2024.
[177] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1075

Similar to systemic hazards observed in traditional financial markets, new risks are introduced by the quick and independent way that transactions and smart contracts are carried out within these blockchain financial networks. 'Herding,' a phenomena where vast sectors of the market react consistently to specific occurrences, is one major issue that could exacerbate price swings. [178] In severe circumstances, this behaviour may lead to "flash crashes," which are marked by abrupt and significant asset devaluation without a matching shift in the underlying economic principles.[179] Since blockchain technology removes the flexibility typically found in financial markets, these impacts may be amplified due to the inherent lack of human control in these systems. Because of the potential for harmful feedback loops caused by blockchain's immediacy and interconnection, this could result in market distortions during times of crisis. An important shift in the market, for example, could set off a chain reaction of automatic responses that exacerbate the original disruption. This calls for a careful evaluation of smart contracts and blockchain financial networks in the context of current laws intended to control similar dangers, such as those pertaining to algorithmic trading and flash crashes.

5.1.1 Policymakers and Regulators

Regulators and policymakers understand how smart contracts may simplify regulatory compliance in cross-border fintech transactions. These blockchain-based, self-executing digital contracts have the potential to do away with the need for conventional middlemen like banks and clearinghouses.[180] Smart contracts have the potential to significantly improve operational efficiency by automating intricate compliance processes, which can speed up transaction processing and decrease the need for manual verification. Financial institutions are able to deploy resources more effectively and with a lower chance of human error because of this greater efficiency.

The intrinsic transparency of smart contracts is one of their main benefits. A transparent and traceable record is produced by recording transactions on a decentralised, irreversible ledger that is open to the public. Because of this transparency, regulatory monitoring is improved, allowing

[178] Ibid
[179] Ibid
[180] Ibid

authorities to promptly detect questionable activity and keep an eye on transactions in real time. Smart contracts have the ability to automate compliance procedures and guarantee conformity to pertinent laws without the need for manual intervention by integrating regulatory requirements directly into the code. This feature enables the automatic validation of participant identities, compliance with anti-money laundering (AML) requirements, and assurance that all required paperwork is in order prior to the transaction being completed.

Smart contracts do, however, come with a number of dangers and problems that should be carefully considered in addition to these benefits. Even with blockchain technology's security, smart contracts can still have security flaws. It is possible to take advantage of coding flaws or defects to conduct fraudulent transactions or incur losses financially. Blockchain transactions' pseudonymous character can make it more difficult to track down participant identities, which opens the door to financial crimes and money laundering. In order to reduce these risks, regulators stress the necessity of improved identity verification and monitoring systems. Furthermore, if customers do not understand the terms of the contract, the automated nature of smart contracts could have unexpected repercussions. Regulators emphasise the importance of clear contract terms and efficient dispute resolution procedures because they are worried about possible consumer exploitation.

To address these challenges and maximise the benefits of smart contracts, policymakers and regulators are advocating for several regulatory measures.[181] Robust regulatory frameworks are essential to address potential threats while leveraging technological advantages. Developing comprehensive guidelines and standards for the creation, deployment, and auditing of smart contracts is crucial. Policymakers are also focusing on establishing clear legal frameworks for the use of smart contracts in international transactions.[182] Developing pragmatic and efficient laws emphasises collaboration with industry stakeholders. Through strong collaboration with fintech

[181] European Parliament, Resolution of 26 May 2016 on Virtual Currencies (Doc No P8TA(2016)0228); Financial Conduct Authority, 'Financial Conduct Authority Unveils Successful Sandbox Firms on the Second Anniversary of Project Innovate' (Press Release, 7 November 2016)

[182] World Economic Forum, *The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services* (August 2016) https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services accessed 8 August 2024.

firms, legal specialists, and technology developers, regulators can acquire significant knowledge regarding the technical and functional aspects of smart contracts.

Adaptive regulation is essential given how quickly blockchain technology is developing. To make sure smart contract laws are current and useful, regulators must have procedures in place for ongoing observation and evaluation. Campaigns for awareness and education are also essential to fostering ethical use. Improving stakeholders' and customers' comprehension of smart contract technology can aid in decision-making and promote secure and efficient use in cross-border fintech transactions.

In summary, smart contracts raise issues that need to be carefully considered even if they have great potential to improve operational effectiveness and regulatory compliance in global fintech operations. Policymakers and regulators may leverage the advantages of smart contracts while reducing risks, guaranteeing consumer protection, and maintaining the integrity of the financial system by creating strong regulatory frameworks, encouraging cooperation with industry stakeholders, and implementing flexible regulatory strategies.

5.1.2 Industry Stakeholders

Industry participants view smart contracts as a transformative technology poised to revolutionise financial operations. Financial institutions and fintech companies recognize the potential for significant cost savings and efficiency gains through automated contract execution and compliance checks. By reducing the need for manual processing and third-party intermediaries, smart contracts can streamline complex transactions and reduce operational costs. This automation enhances speed and accuracy, allowing businesses to execute transactions more rapidly and with fewer errors. Fintech companies, in particular, see smart contracts as an opportunity to innovate and deliver more sophisticated financial products and services, which can lead to a more competitive and dynamic market landscape.

Despite these advantages, industry stakeholders emphasise the need for greater legal certainty and regulatory clarity to fully realise the potential of smart contracts. The current landscape of regulatory uncertainty and inconsistent legal frameworks across different jurisdictions can hinder the widespread adoption of this technology. Ambiguities or inconsistencies in legislation can

create barriers for businesses looking to implement smart contracts, as they may face challenges related to enforceability, compliance, and liability. Without clear legal guidelines, companies risk facing legal disputes or financial penalties, which can discourage investment and innovation in smart contract technologies.

Industry stakeholders advocate for the establishment of clear norms and standards that promote the adoption of smart contracts across various jurisdictions.[183] A consistent regulatory approach is essential to provide businesses with the confidence to invest in and develop smart contract solutions. Harmonising legal frameworks can help eliminate uncertainties and facilitate cross-border transactions, enabling businesses to expand their operations globally. Collaboration between regulators, industry leaders, and legal experts is crucial to developing comprehensive guidelines that address the unique challenges posed by smart contracts while encouraging innovation and growth.

Moreover, industry stakeholders stress the importance of fostering a supportive regulatory environment that balances innovation with consumer protection and risk management. Clear regulations can provide the necessary safeguards to protect consumers from potential risks associated with smart contracts, such as data breaches or unfair contract terms. By establishing transparent rules and ensuring accountability, regulators can create a level playing field that fosters healthy competition and promotes the responsible use of smart contract technology.

In conclusion, while smart contracts offer substantial benefits in terms of cost savings and operational efficiency, their full potential can only be realised through legal certainty and regulatory clarity. By working together to establish clear norms and standards, regulators and industry stakeholders can create an environment conducive to innovation and growth, paving the way for the widespread adoption of smart contracts in financial operations worldwide. This collaborative approach can help unlock the transformative potential of smart contracts, driving advancements in the fintech industry and reshaping the future of financial services.

[183] International Chamber of Commerce, *Policy Paper on Blockchain and Smart Contracts* (2021) https://iccwbo.org/content/uploads/sites/3/2021/03/icc-policy-paper-blockchain-smart-contracts.pdf accessed 9 August 2024; European Commission, *Blockchain and the Future of Smart Contracts* (2021) https://ec.europa.eu/info/publications/blockchain-and-smart-contracts_en accessed 9 August 2024.

5.2 Recommendations

To address these challenges and promote the widespread adoption of smart contracts, several key recommendations emerge:

1. Develop Standardised Protocols for Smart Contracts

In order to promote the broader integration of smart contracts into cross-border transactions, legislators and regulators must work closely with industry players to establish standardized procedures. These protocols ought to function as all-inclusive manuals that delineate optimal procedures for the creation, execution, and settlement of disputes pertaining to smart contracts. One of the main obstacles to the global integration of smart contracts can be removed by stakeholders by defining protocols that guarantee consistent and reliable implementation of smart contracts across various industries and jurisdictions.

Developing standardised protocols begins with creating a robust framework for contract formation.[184] This entails specifying precise requirements for the components of a smart contract, like terms, conditions, and parameters for execution. By standardising these components, smart contracts can be made more legally sound and ensure that all parties are aware of each other's rights and responsibilities. To ensure compatibility across various blockchain platforms and that contracts function as intended, protocols should also handle the technical parts of smart contract coding.

The efficacy of smart contracts also depends on performance standards. Performance measures, such as transaction speed, correctness, and dependability, should have benchmarks defined by protocols. Stakeholders may make sure smart contracts live up to their promises of efficacy and economy by setting performance benchmarks. Setting criteria for the validation and verification of contract terms is one way to do this, as is making sure that all requirements are satisfied prior to implementation. Performance criteria can also be used to track and evaluate the effects of smart contracts, giving important information for ongoing innovation and development.

Another essential element of standardized protocols is dispute resolution procedures. Clear mechanisms for resolution are necessary because of the potential for conflicts and

[184] Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15.

misunderstandings arising from the complexity and novelty of smart contracts. Protocols ought to delineate equitable, lucid, and proficient mechanisms for resolving disputes; these may encompass conventional legal structures as well as innovative methodologies such as blockchain arbitration. This dual strategy can offer flexibility, enabling parties to take advantage of the special qualities of blockchain technology and settle disagreements amicably. By creating efficient dispute resolution procedures, smart contracts can gain more credibility and acceptance.

By developing standardised protocols, stakeholders can achieve the consistency and legal certainty necessary for the seamless integration and functioning of smart contracts within the global financial system.[185] Establishing consistency is crucial for building confidence between parties since it lowers the possibility of ambiguity and misinterpretation. By integrating smart contracts with current legal and regulatory frameworks, standardized protocols can help make regulatory compliance easier and reduce the risk of legal issues. Additionally, they can foster innovation by offering a solid platform for programmers to create new services and apps.

For this endeavour to be successful, cooperation between regulators, legislators, and industry stakeholders is vital. Government officials and regulators offer valuable perspectives on legislative mandates and consumer protection standards, whilst industry participants offer proficiency in technology and market dynamics. When combined, they may design protocols that strike a compromise between innovation and regulation, making smart contracts both legally solid and cutting edge in terms of technology. In addition to promoting knowledge exchange and the distribution of best practices, this cooperative strategy can assist stakeholders in building on successful models and learning from one another's experiences.

2. Harmonise Regulatory Frameworks

To enable the global adoption of smart contracts, it is crucial to design regulatory frameworks that ensure compatibility between these digital agreements and established international legal principles. Harmonising legal standards across different jurisdictions is a foundational step in achieving this compatibility.[186] By aligning regulations with international legal norms,

[185] See examples, Enza Cirone, 'Blockchain and the General Data Protection Regulation: An Irreconcilable Regulatory Approach?' (2021) 2021 QMLJ 15; Philipp Paech, 'Securities, Intermediation and the Blockchain—An Inevitable Choice between Liquidity and Legal Certainty' (2016) *Uniform Law Review* 21

[186] William Magnuson, 'Regulating Fintech' (2018) 71 Vand L Rev 1167

stakeholders can reduce legal ambiguity, enhance predictability, and facilitate smoother cross-border transactions.

The first step towards harmonising regulatory frameworks is to recognize and resolve differences between national legal frameworks and smart contract functionality. Because they are self-executing and programmable, smart contracts may put conventional legal theories about the creation, execution, and enforcement of contracts to the test. Regulators must therefore assess how to include or modify current legal concepts to make room for these new technology.[187] This includes reconciling differences in contract law, property rights, and dispute resolution mechanisms across various jurisdictions.

Encouraging global cooperation is essential to the harmonisation process. Together, regulators and policymakers should create uniform rules and regulations that uphold various legal traditions and encourage the application of smart contracts. International conferences, working groups, and agreements that seek to harmonise regulatory norms and exchange best practices can enable this cooperative approach. States can resolve legal disputes and establish a unified framework that facilitates the implementation of smart contracts throughout the world by talking to each other and negotiating.

A sophisticated approach is needed to create legal frameworks that accommodate smart contracts while maintaining respect for national legal traditions. It is imperative for regulators to take into account the distinct legal environments of various nations and guarantee that novel legislation do not compromise established legal tenets. For instance, although some legal systems place a premium on formalistic contract requirements, others could give priority to practical methods of enforcement. These variations can be accommodated by a flexible and adaptable regulatory framework, allowing states to align their laws while maintaining their respective legal traditions.

Reducing legal ambiguity is a key objective of harmonising regulatory frameworks.[188] Clear and consistent legal standards for smart contracts can help minimise uncertainties and provide a reliable foundation for businesses and individuals engaging in cross-border transactions. When

[187] Giusella Finocchiaro and Chantal Bomprezzi, 'A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts' (2023) 10 Media Law 130
[188] William Magnuson, 'Regulating Fintech' (2018) 71 *Vand L Rev* 1167.

legal requirements are well-defined and uniformly applied, it falls to logic that parties are more likely to trust the technology and invest in its use. This clarity also helps in resolving disputes and enforcing smart contracts, as parties can rely on a shared understanding of their legal rights and obligations.

In addition to regulatory alignment, it is important to address the practical aspects of implementing harmonised frameworks. This includes developing mechanisms for cross-border legal cooperation, such as mutual recognition agreements and standardised documentation practices. These mechanisms can facilitate the seamless execution of smart contracts across different legal systems and ensure that they are recognized and enforced consistently.

Moreover, harmonising regulatory frameworks can also drive innovation by providing a stable and predictable regulatory environment. When businesses and developers are assured that their smart contracts will be treated consistently across jurisdictions, they are more likely to explore new applications and invest in innovative solutions. This, in turn, has the ability to stimulate economic growth and enhance the overall efficiency of global financial systems.

3. Foster International Regulatory Collaboration

In order to improve the efficiency and worldwide integration of smart contracts, legislators ought to place a high priority on encouraging cooperation between regulatory agencies in various jurisdictions. This cooperative strategy is essential for harmonizing laws and enhancing smart contract interoperability worldwide. Regulatory bodies can improve the coherence of the regulatory environment for smart contracts, solve regulatory framework inconsistencies, and expedite compliance procedures by cooperating.

One key initiative in fostering international regulatory collaboration is the establishment of information-sharing platforms.[189] Regulatory agencies can share information, lessons learned, and case studies about implementing and monitoring smart contracts on these platforms. Authorities

[189] Nathaniel Popper, 'Where Finance and Technology Come Together' *New York Times* (New York, 14 November 2016) <https://www.nytimes.com/2016/11/15/business/dealbook/where-finance-and-technology-come-together.html> accessed 9 August 2024; 'Singapore Tries to Become a Fintech Hub' *The Economist* (London, 12 January 2017) <https://www.economist.com/news/finance-and-economics/21714384-city-state-wants-fintech-bolsters-not-disrupts-mainstream> accessed 9 August 2024.

can better understand how smart contracts function across multiple jurisdictions and uncover common regulatory difficulties by exchanging information on best practices, regulatory challenges, and technology improvements. This body of knowledge can help shape more cohesive and efficient regulatory strategies, which will lessen fragmentation and improve the regulatory framework for smart contracts as a whole.

Cross-border regulatory sandboxes are another significant initiative that can facilitate international regulatory collaboration.[190] Regulatory sandboxes offer a safe haven where companies can test cutting edge financial technologies—like smart contracts—under the watchful eye of regulators. Companies can test smart contract apps while following legal requirements by taking part in these sandboxes; this enables the detection and resolving of compliance concerns prior to full-scale deployment. By extending the notion of regulatory sandboxes to a cross-border setting, companies can test their smart contract solutions concurrently in several jurisdictions.[191] This approach helps regulatory bodies gain a better understanding of the technology's impact and scalability in different regulatory environments and fosters a more coordinated regulatory response.

In order to facilitate the smooth functioning of smart contracts across borders, disparities in legal and compliance requirements must be addressed as part of the joint efforts to promote regulatory convergence. Countries can lower obstacles to cross-border transactions and guarantee that smart contracts are accepted and applied uniformly by harmonising their regulatory standards and procedures. The establishment of cooperative regulatory frameworks, mutual recognition agreements, and standardised compliance protocols that enable the seamless functioning of smart contracts in several jurisdictions can help accomplish this alignment.

Apart from venues for exchanging knowledge and regulatory sandboxes, policymakers ought to promote global forums and task forces devoted to deliberating and resolving regulatory issues concerning smart contracts. These discussion forums can act as avenues for interaction between industry participants, regulators, and technology specialists, encouraging cooperation and producing answers to shared regulatory problems. International stakeholders can strive toward

[190] Ibid

[191] Karolina Kasprzyk, 'The Concept of Smart Contracts from the Legal Perspective' (2018) 34 *Review of European and Comparative Law* 101.

developing a cohesive strategy for regulating smart contracts and resolving new regulatory difficulties by participating in continuing talks and negotiations.

Furthermore, fostering international regulatory collaboration can help build trust among businesses and consumers regarding the use of smart contracts.[192] Businesses are more inclined to invest in and use smart contracts when international regulatory organisations collaborate to create transparent and uniform regulations because they will be backed by a stable and predictable regulatory environment. This kind of trust is crucial for promoting creativity and propelling the broad implementation of smart contracts throughout international financial institutions.

4. Leverage Technological Advancements

Technological innovations provide promising solutions to the current challenges faced by smart contracts, particularly in terms of scalability, efficiency, and adaptability. One significant advancement is the development of Layer 2 solutions, such as zk-Rollups and Optimistic Rollups.[193] These technologies address critical scalability issues by processing transactions off the main blockchain, thereby reducing congestion and lowering transaction costs. zk-Rollups, for example, aggregate multiple transactions into a single batch and then submit a succinct proof to the main chain, which enhances processing speed and efficiency. Similarly, Optimistic Rollups operate by assuming transactions are valid by default, only conducting detailed checks when disputes arise.[194] Both of these Layer 2 solutions can significantly improve smart contract performance, enabling faster and more cost-effective transaction processing.

In addition to Layer 2 solutions, emerging technologies like artificial intelligence (AI) and machine learning (ML) offer transformative potential for smart contracts. AI can enhance smart contracts by enabling more sophisticated decision-making processes, such as predictive analytics and pattern recognition, which can improve the accuracy and efficiency of contract execution. For instance, AI algorithms can analyse vast amounts of data to identify potential risks or opportunities, allowing smart contracts to adapt their terms and conditions in real-time based on changing circumstances.

[192] Ibid
[193] Amanda J Sharp and Orly Lobel, 'Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens' (2023)
[194] Ibid

Machine learning models can further enhance this adaptability by continuously learning from new data and experiences, thereby refining the performance of smart contracts over time.

The integration of AI and ML into smart contracts could lead to more complex and dynamic functionalities, such as automated negotiations and personalised contract terms. These advancements could enable smart contracts to handle more intricate scenarios, such as multi-party agreements with variable conditions and adaptive responses to external events. By incorporating AI and ML, smart contracts can become more flexible and responsive, providing solutions that are tailored to the specific needs of users and evolving business environments.

Moreover, leveraging technological advancements can also address issues related to security and trust. Enhanced cryptographic techniques and advanced algorithms can improve the security of smart contracts, reducing the risk of vulnerabilities and malicious attacks.[195] By integrating cutting-edge technology, stakeholders can ensure that smart contracts are not only more efficient but also more secure, fostering greater confidence in their use across various applications.

In summary, technological advancements offer valuable opportunities to overcome the current limitations of smart contracts. Layer 2 solutions like zk-Rollups and Optimistic Rollups can resolve scalability issues by improving transaction speed and reducing costs, while AI and ML can enhance smart contracts with advanced decision-making capabilities and adaptive functions. By leveraging these innovations, smart contracts can become more versatile and efficient, making them better suited for complex and evolving transactions. Embracing these technological advancements will be crucial for the continued growth and integration of smart contracts in the global financial ecosystem.

5. Expand Regulatory Sandboxes

To encourage innovation while ensuring regulatory compliance, policymakers should consider expanding the use and scope of regulatory sandboxes. These controlled environments—such as those established in the UK and Singapore—offer a structured yet flexible framework for testing new technologies, including smart contracts and other fintech solutions, under the oversight of

[195]Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 *Modern Law Review* 1075

regulatory bodies.[196] Regulatory sandboxes are designed to create a safe and supervised space where companies can experiment with their innovations without facing the full regulatory burdens that typically apply to broader market operations. This approach allows businesses to identify and address potential compliance issues, refine their technologies, and adjust their strategies based on real-world feedback before they launch their products on a larger scale.

The primary advantage of regulatory sandboxes lies in their ability to balance the need for innovation with the requirement for regulatory oversight. By operating within these controlled environments, businesses gain valuable insights into regulatory expectations and operational challenges, which helps in crafting solutions that meet both market needs and regulatory standards.[197] For regulators, sandboxes offer a unique opportunity to observe emerging technologies in action, understand their impact, and develop informed regulatory approaches that can be scaled up or adapted as needed.

Expanding regulatory sandboxes can significantly benefit the fintech ecosystem by providing more opportunities for experimentation and development. Increasing the number of sandboxes and their geographical reach can help accommodate a wider range of technologies and business models, fostering a more dynamic and diverse innovation landscape. Additionally, extending the duration and scope of these sandboxes can allow for more comprehensive testing and refinement processes, leading to more robust and market-ready solutions.

In practice, an expanded network of regulatory sandboxes can also facilitate international collaboration and knowledge sharing. As countries and jurisdictions develop their own sandboxes, they can create mechanisms for sharing best practices, data, and insights, which can lead to more harmonised regulatory approaches and greater consistency across borders. This collaboration can help to align regulatory frameworks, reduce regulatory fragmentation, and promote the seamless integration of new technologies into the global market.

---

[196] Nathaniel Popper, 'Where Finance and Technology Come Together' *New York Times* (New York, 14 November 2016) <https://www.nytimes.com/2016/11/15/business/dealbook/where-finance-and-technology-come-together.html> accessed 8 August 2024; 'Singapore Tries to Become a Fintech Hub' *The Economist* (London, 12 January 2017) <https://www.economist.com/news/finance-and-economics/21714384-city-state-wants-fintech-bolsters-not-disrupts-mainstream> accessed 8 August 2024.

[197] Karolina Kasprzyk, 'The Concept of Smart Contracts from the Legal Perspective' (2018) 34 *Review of European and Comparative Law* 101.

Moreover, expanding regulatory sandboxes can address one of the key challenges faced by innovators—navigating complex and often uncertain regulatory landscapes. By providing a clear and supportive framework for testing and compliance, sandboxes can reduce the risk and uncertainty associated with launching new technologies. This support not only enhances the confidence of businesses and investors but also accelerates the pace of innovation, contributing to the overall growth and advancement of the fintech sector.

6. Promote Global Cooperation

Strong international collaboration is necessary to establish uniform regulatory frameworks for smart contracts. Cross-border cooperation is vital, as seen by the efforts of international organisations like the Financial Stability Board (FSB) and the G20 to coordinate fintech legislation. The significance of collaborating to establish a cohesive regulatory framework that can adapt to the distinctive features of smart contracts and other cutting-edge technology is underscored by these endeavours.

Improving international collaboration is essential to creating global norms for smart contract development. The current state of regulatory fragmentation between jurisdictions is somewhat problematic since differing standards and regulations can lead to misunderstandings and inefficiencies for multinational corporations. Countries might attempt to harmonise their legal and regulatory frameworks through international collaboration, which will lessen inconsistencies and streamline compliance procedures for businesses doing cross-border business.

The advancement of interoperability is a major advantage of international collaboration. The adoption and integration of smart contracts are facilitated when countries harmonize their legislative frameworks. This alignment lowers barriers to entry and facilitates more seamless international transactions for companies wishing to grow internationally by ensuring that smart contracts operate consistently across various legal systems.

Further, concerted efforts can result in the creation of thorough and well-coordinated regulatory frameworks that facilitate the broad adoption of smart contracts. Countries can establish a regulatory environment that is more predictable and stable by tackling shared challenges and

harmonising rules. Because it gives firms more assurance about compliance and operational standards, this stability can spur investment and innovation.

Insights and best practices can be shared among regulatory organizations through global cooperation, which can result in better regulatory strategies and more informed decision-making. Forums and collaborative platforms can be used as places to talk about new trends, address shared concerns, and work together to find solutions to problems. This information and experience sharing can improve regulatory frameworks' overall efficacy and facilitate the successful adoption of smart contracts globally.

7. Address Consumer Protection Concerns

It is imperative to tackle consumer protection issues in order to establish the credibility of smart contracts and enable their extensive use. Making sure smart contracts function fairly and openly is essential for safeguarding customers and preserving the integrity of the financial system as they become more and more integrated into financial operations. Legislators are essential in establishing and implementing policies that improve the accountability, equity, and transparency of smart contract transactions.

Establishing explicit disclosure rules is a crucial component of consumer protection. Before committing to any transaction, consumers must be fully educated on the terms, conditions, and implications of smart contracts. By ensuring that all parties are aware of their rights and responsibilities, transparent disclosure lowers the possibility of disputes and boosts public confidence in technology. Regulators can assist consumers in making educated decisions and averting potential hazards by requiring detailed and easily accessible information on smart contracts.

Effective dispute resolution mechanisms are also vital for addressing conflicts that may arise from smart contract transactions.[198] Because smart contracts are automated, traditional dispute resolution processes might not always be suitable. Legislators must design and support processes

[198] P Ortolani, 'Self-enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36 **OJLS** 595, 608.

that can fairly and successfully settle conflicts, ensuring that consumers may get appropriate redress if they have any complaints.[199] This could include establishing dedicated arbitration bodies or integrating dispute resolution features directly into smart contract platforms.

Moreover, ensuring fairness in smart contracts is crucial for protecting consumer interests.[200] The concept of fairness includes not just treating all parties equally but also stopping actions that could harm or exploit customers. The main goals of regulatory actions should be to stop discriminatory behaviours, unjust terms and conditions, and other such abuses that can erode consumer trust in the technology.

Smart contract technology can be more widely accepted and given more respect by addressing these consumer protection issues. If customers are assured that their interests are safeguarded and that the technology functions in an open and equitable manner, they are more inclined to accept and believe in smart contracts. Strong consumer protection regulations would not only boost smart contract confidence but also facilitate their integration into traditional financial institutions, spurring innovation and increasing transaction efficiency.

8. Clarify Legal Status and Enforceability

For smart contracts to be successfully integrated into the financial and commercial sectors, it is imperative that their legal status and enforceability are clarified. It is imperative for policymakers to proactively build a lucid legal framework that acknowledges smart contracts as legitimate and enforceable transactions. In order to give stakeholders—such as companies, consumers, and financial institutions—assurance and to enable the wider implementation of this game-changing technology, clarity is essential.[201]

Putting laws into place that specifically identify and acknowledge smart contracts is the first step toward elucidating their legal standing. To guarantee that smart contracts are seen by the law in a manner consistent with those of regular contracts, legislation should address important issues such contract creation, execution, and enforceability. To facilitate the usage and integration of smart

[199] Ibid
[200] Tatiana Cutts, 'Smart Contracts and Consumers' (2019) 122 W Va L Rev 389.
[201] Ibid

contracts, legislators can establish a clear legal framework by enacting new legislation or modifying current legislation.

Judicial precedents are crucial in determining the enforceability of smart contracts, in addition to legislative action. For smart contracts to remain legally enforceable, courts must acknowledge and maintain their legality in court cases. Smart contract enforceability can be upheld by judges' rulings, which can assist establish significant precedents and direct future legal interpretations. Judicial decisions that are unambiguous and consistent will help to lower legal ambiguities and boost trust in smart contract technology.

Furthermore, a wide range of financial and commercial applications will be significantly impacted by the acceptance of smart contracts as legally binding contracts. If businesses are certain that these agreements would be respected in court, they will be more likely to implement smart contracts. This enhanced self-assurance has the potential to stimulate creativity, simplify procedures, and enhance productivity in various fields.

International cooperation should be taken into account by policymakers when defining the legal standing of smart contracts. Because smart contracts frequently include cross-border transactions, it can be beneficial to have a uniform legal framework throughout different jurisdictions in order to reduce regulatory fragmentation and promote worldwide adoption. Global recognition of smart contracts could be facilitated by standardising legal norms through international agreements or model legislation.

Smart contracts enabled by blockchain technology have great potential to revolutionise international fintech transactions. By lowering transaction costs, enhancing transparency, and automating compliance procedures, they provide significant advantages to industry stakeholders and regulators. But before smart contracts are widely used, a number of regulatory concerns need to be addressed, and compliance with accepted legal standards needs to be made sure of. Stakeholders can assist in integrating smart contracts into the global financial ecosystem by creating standardised protocols, aligning regulatory frameworks, encouraging cross-border collaboration, utilising emerging technologies, and attending to consumer protection issues. These guidelines are intended to ensure regulatory compliance, safeguard consumer interests, and enable the effective use of smart contracts.

Chapter 6

Concluding Remarks

In conclusion, smart contracts, underpinned by blockchain technology, are poised to revolutionise the global financial ecosystem by offering enhanced transparency, automating compliance processes, and reducing transaction costs. However, their widespread adoption is contingent upon addressing several critical challenges that span regulatory, technological, and legal domains. To fully leverage the transformative potential of smart contracts, a comprehensive approach that involves regulatory innovation, technological advancements, international collaboration, and robust consumer protection is essential.

A primary challenge in integrating smart contracts into the global financial system is the need for regulatory harmonisation across jurisdictions. Smart contracts operate in a decentralised and borderless manner, which necessitates a coherent regulatory framework to ensure their seamless integration. Policymakers must prioritise fostering international regulatory collaboration to address inconsistencies in regulations and improve interoperability.

Establishing information-sharing platforms between regulatory bodies is a crucial step in this direction. These platforms can facilitate the exchange of insights, experiences, and data related to the implementation and oversight of smart contracts. By sharing information on best practices, regulatory challenges, and technological advancements, authorities can gain a better understanding

of how smart contracts function across different jurisdictions. This collective knowledge is instrumental in developing effective and consistent regulatory approaches, thus reducing fragmentation and enhancing the overall regulatory framework for smart contracts.

Cross-border regulatory sandboxes represent another significant initiative in fostering international collaboration. These sandboxes offer a controlled environment where businesses can test innovative technologies, including smart contracts, under regulatory supervision. By participating in these sandboxes, companies can experiment with smart contract applications while adhering to regulatory guidelines. This approach allows for the identification and resolution of compliance issues before full-scale deployment. Expanding the concept of regulatory sandboxes to a cross-border context enables businesses to test their solutions across multiple jurisdictions simultaneously. This not only helps regulatory bodies understand the technology's impact and scalability in different environments but also fosters a more coordinated regulatory response.

Promoting regulatory convergence through collaborative efforts involves addressing discrepancies in legal and compliance requirements that may hinder the seamless operation of smart contracts across borders. Aligning regulatory standards and practices can reduce barriers to cross-border transactions and ensure that smart contracts are recognized and enforced consistently. This alignment can be achieved through the development of joint regulatory frameworks, mutual recognition agreements, and standardised compliance procedures that facilitate the smooth operation of smart contracts in various jurisdictions.

International forums and working groups dedicated to discussing and addressing regulatory challenges related to smart contracts are also valuable. These platforms serve as venues for dialogue between regulators, industry stakeholders, and technology experts, fostering collaboration and generating solutions to common regulatory issues. Engaging in ongoing discussions and negotiations can lead to the creation of a unified approach to regulating smart contracts and addressing emerging regulatory challenges. This international cooperation can also build trust among businesses and consumers, encouraging the adoption of smart contracts by providing a predictable and stable regulatory environment.

Technological innovations offer promising solutions to the current challenges faced by smart contracts, particularly in terms of scalability, efficiency, and adaptability. Among the most significant advancements are Layer 2 solutions, such as zk-Rollups and Optimistic Rollups, which address critical scalability issues by processing transactions off the main blockchain. zk-Rollups aggregate multiple transactions into a single batch and submit a succinct proof to the main chain, enhancing processing speed and efficiency. Optimistic Rollups, on the other hand, operate on the assumption that transactions are valid by default, conducting detailed checks only when disputes arise. These Layer 2 solutions can significantly improve smart contract performance, enabling faster and more cost-effective transaction processing.

Emerging technologies like artificial intelligence (AI) and machine learning (ML) offer transformative potential for smart contracts. AI can enhance smart contracts by enabling more sophisticated decision-making processes, such as predictive analytics and pattern recognition, which can improve accuracy and efficiency. For instance, AI algorithms can analyse large volumes of data to identify potential risks or opportunities, allowing smart contracts to adapt their terms and conditions in real-time based on changing circumstances. Machine learning models can further enhance adaptability by continuously learning from new data and experiences, refining the performance of smart contracts over time.

The integration of AI and ML into smart contracts could lead to more complex and dynamic functionalities, such as automated negotiations and personalised contract terms. These advancements could enable smart contracts to handle intricate scenarios, such as multi-party agreements with variable conditions and adaptive responses to external events. By incorporating AI and ML, smart contracts can become more flexible and responsive, offering tailored solutions that address the specific needs of users and evolving business environments.

Moreover, leveraging technological advancements can also address issues related to security and trust. Enhanced cryptographic techniques and advanced algorithms can improve the security of smart contracts, reducing the risk of vulnerabilities and malicious attacks. By integrating cutting-edge technology, stakeholders can ensure that smart contracts are not only more efficient but also more secure, fostering greater confidence in their use across various applications.

Expanding the use and scope of regulatory sandboxes is crucial for encouraging innovation while ensuring regulatory compliance. Regulatory sandboxes, as established in jurisdictions like the UK and Singapore, offer a structured yet flexible framework for testing new technologies, including smart contracts and other fintech solutions, under the oversight of regulatory bodies. These environments allow companies to experiment with their innovations without facing the full regulatory burdens typically associated with broader market operations. This approach helps businesses identify and address potential compliance issues, refine their technologies, and adjust their strategies based on real-world feedback before launching their products on a larger scale.

Expanding regulatory sandboxes can significantly benefit the fintech ecosystem by providing more opportunities for experimentation and development. Increasing the number of sandboxes and their geographical reach can accommodate a wider range of technologies and business models, fostering a more dynamic and diverse innovation landscape. Additionally, extending the duration and scope of these sandboxes allows for more comprehensive testing and refinement processes, leading to more robust and market-ready solutions.

An expanded network of regulatory sandboxes can also facilitate international collaboration and knowledge sharing. As countries and jurisdictions develop their sandboxes, they can create mechanisms for sharing best practices, data, and insights, leading to more harmonised regulatory approaches and greater consistency across borders. This collaboration can help align regulatory frameworks, reduce fragmentation, and promote the seamless integration of new technologies into the global market. Furthermore, expanding sandboxes can address one of the key challenges faced by innovators—navigating complex and often uncertain regulatory landscapes. By providing a clear and supportive framework for testing and compliance, sandboxes reduce the risk and uncertainty associated with launching new technologies. This support not only enhances the confidence of businesses and investors but also accelerates the pace of innovation, contributing to the overall growth and advancement of the fintech sector.

Establishing consistent regulatory regimes for smart contracts necessitates robust international cooperation. Efforts by global organisations such as the Financial Stability Board (FSB) and the

G20 underscore the importance of cross-border collaboration in creating a unified regulatory landscape. These initiatives emphasise the need for countries to work together to develop international standards for smart contracts, which are crucial for reducing regulatory fragmentation and simplifying compliance processes.

Enhancing global cooperation is pivotal for promoting interoperability among smart contracts. When nations align their regulatory approaches, they create a more seamless environment for the adoption and integration of smart contracts. This alignment ensures that smart contracts function consistently across different legal systems, facilitating smoother international transactions and reducing barriers to entry for businesses seeking to expand their operations globally.

Coordinated international efforts can also lead to the establishment of comprehensive and cohesive regulatory frameworks that support the widespread use of smart contracts. By addressing common challenges and aligning policies, countries can create a more predictable and stable regulatory environment. This stability encourages investment and innovation by providing businesses with greater certainty regarding compliance and operational requirements.

Global cooperation allows for the sharing of best practices and insights among regulatory bodies, enhancing decision-making and regulatory strategies. Collaborative platforms and forums serve as venues for discussing emerging trends, addressing shared concerns, and developing joint solutions to common issues. This exchange of knowledge and experience can improve the overall effectiveness of regulatory frameworks and support the successful implementation of smart contracts on an international scale.

Addressing consumer protection concerns is essential for building trust and facilitating the widespread adoption of smart contracts. As smart contracts become more integral to financial transactions, ensuring their transparency and fairness is crucial for protecting consumers and maintaining the integrity of the financial system. Policymakers must introduce and enforce measures that enhance the transparency, fairness, and accountability of smart contract transactions.

A critical aspect of consumer protection involves establishing clear disclosure requirements. Consumers need to be fully informed about the terms, conditions, and implications of smart contracts before committing to any transaction. Transparent disclosure ensures that all parties understand their rights and obligations, reducing the likelihood of disputes and enhancing overall trust in the technology. Mandating comprehensive and accessible information about smart contracts helps consumers make informed decisions and avoid potential pitfalls.

Effective dispute resolution mechanisms are also vital for addressing conflicts that may arise from smart contract transactions. Given the automated nature of smart contracts, traditional methods of dispute resolution may not always be applicable. Policymakers should develop and promote mechanisms that handle disputes efficiently and fairly, ensuring that consumers have access to appropriate remedies if issues occur. This could include establishing dedicated arbitration bodies or integrating dispute resolution features directly into smart contract platforms.

Ensuring fairness in smart contracts is crucial for protecting consumer interests. Fairness encompasses not only the equitable treatment of all parties involved but also the prevention of practices that could exploit or disadvantage consumers. Regulatory measures should focus on preventing unfair terms and conditions, discriminatory practices, and other potential abuses that could undermine consumer confidence in the technology.

By addressing these consumer protection concerns, smart contract technologyBy addressing these consumer protection concerns, smart contract technology can gain greater credibility and facilitate broader adoption. Consumers are more likely to embrace and trust smart contracts if they feel confident that their interests are protected and that the technology operates transparently and fairly. Ensuring robust consumer protection measures will not only enhance trust in smart contracts but also support their integration into mainstream financial systems, driving innovation and improving efficiency in transactions.

Clarifying the legal status and enforceability of smart contracts is fundamental for their successful integration into financial and commercial sectors. Policymakers must establish a clear legal framework that recognizes smart contracts as valid and enforceable agreements. This clarity

provides certainty to stakeholders, including businesses, consumers, and financial institutions, and facilitates the broader adoption of this transformative technology.

The initial step in clarifying the legal status of smart contracts involves implementing legislative measures that explicitly define and recognize these digital agreements. Legislation should address key aspects such as contract formation, execution, and enforceability to ensure that smart contracts are treated similarly to traditional contracts under the law. Creating specific statutes or amending existing laws to accommodate smart contracts provides a clear legal foundation that supports their use and integration.

In addition to legislative action, judicial precedents play a critical role in establishing the enforceability of smart contracts. Courts must recognize and uphold the validity of smart contracts in legal disputes to reinforce their status as binding agreements. Judicial decisions that affirm the enforceability of smart contracts can help set important precedents and guide future legal interpretations. Clear and consistent judicial rulings will contribute to reducing legal uncertainties and enhancing confidence in smart contract technology.

The recognition of smart contracts as enforceable agreements will have significant implications for various financial and commercial applications. Businesses will be more inclined to adopt smart contracts if assured that these agreements will be upheld in legal proceedings. This increased confidence can drive innovation, streamline transactions, and improve efficiency across different sectors.

Policymakers should also consider international coordination in clarifying the legal status of smart contracts. Given that smart contracts often involve cross-border transactions, having a consistent legal framework across jurisdictions can mitigate regulatory fragmentation and facilitate global adoption. International agreements or model laws could provide a basis for harmonising legal standards and promoting the recognition of smart contracts worldwide.

Bibliography

Books

I Bashir, *Mastering Blockchain* (Packt Publishing, 2018)

M Rauchs and others, *Distributed Ledger Technology Systems: A Conceptual Framework* (University of Cambridge, 2018)

Journal Articles

M Durovic and A Janssen, ‘The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law’ (2019) 27 European Review of Private Law 753

G Finocchiaro and C Bomprezzi, ‘A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts’ (2023) 10 Media Law 118

K Kasprzyk, ‘The Concept of Smart Contracts from the Legal Perspective’ (2018) 34 Revista Europea de Derecho y Derecho Comparado 101

W Magnuson, ‘Regulating Fintech’ (2018) 71 Vanderbilt Law Review 1167

P Ortolani, ‘Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin’ (2016) 36 Oxford Journal of Legal Studies 595

P Paech, ‘The Governance of Blockchain Financial Networks’ (2017) 80 Modern Law Review 1073

AJ Sharp and O Lobel, ‘Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens’ (2023) 63 Journal of Intellectual Property Law & Practice 467

I Shaki and T Petr, ‘Towards a Diverse Future: The Impact of Innovation and Technology on Sustainable Development’ (2023) 37 Advances in Climate Change Research 262 <https://www.sciencedirect.com/science/article/pii/S2214212623002624> accessed 8 August 2024

Y-P Yang, ‘When Jurisdiction Rules Meet Blockchain: Can the Old Bottle Contain the New Wine?’ (2023) 6 Stanford Journal of Blockchain Law & Policy 137

Reports

World Economic Forum, “The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services” (World Economic Forum, 2016) <https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services> accessed 8 August 2024

Press Releases

Financial Conduct Authority, ‘Financial Conduct Authority Unveils Successful Sandbox Firms on the Second Anniversary of Project Innovate’ (Press Release, 7 November 2016)

European Parliament Documents

European Parliament, *Resolution of 26 May 2016 on Virtual Currencies* (Doc No P8_TA(2016)0228)

Websites

Aeternity, 'State Channels' <https://aeternity.com/state-channels> accessed 7 August 2024

BBC News, 'Bitcoin Hits Record High Amid Currency Concerns' **BBC News (**15 December 2017) <https://www.bbc.com/news/technology-42237162> accessed 9 August 2024

Bitcoin Insider, 'Top 5 Blockchain Projects Driving Cross-Chain Interoperability in 2024' **Bitcoin Insider** (17 July 2024) <https://www.bitcoininsider.org/article/252542/top-5-blockchain-projects-driving-cross-chain-interoperability-2024> accessed 9 August 2024

J Paul, 'How Blockchain Is Transforming the Entire Financial Services Industry' **Forbes** (7 June 2023) <https://www.forbes.com/sites/forbestechcouncil/2023/06/07/how-blockchain-is-transforming-the-entire-financial-services-industry/> accessed 9 August 2024

Revolut, 'Data Privacy for Candidates' <https://www.revolut.com/en-IE/legal/data-privacy-for-candidates/> accessed 7 August 2024

Revolut, 'Privacy Policy' <https://www.revolut.com/legal/privacy/> accessed 9 August 2024

Revolut, *Annual Report 2022* (Revolut, 2022) <https://cdn.revolut.com/pdf/annualreport2022.pdf> accessed 8 August 2024

The Swiss Financial Market Supervisory Authority (FINMA), 'Guidelines on Initial Coin Offerings (ICOs) and Blockchain Technology' (FINMA, 2018) <https://www.finma.ch/en/news/2018/02/20180216-mm-ico/> accessed 9 August 2024

JI Wong and I Karr, ‘Everything You Need to Know About the Ethereum "Hard Fork"’ *Quartz* (18 July 2016) <http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/> accessed 9 August 2024

Legislation and Regulations

Arizona Revised Statutes § 44-7001 (2017)

Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility [2003] OJ L338/1

Electronic Signatures in Global and National Commerce Act (E-SIGN Act) 2000, 15 USC §§ 7001-7031

European Commission, ‘Data Protection: Better Rules for Small Businesses’ (European Commission, 2018) <https://commission.europa.eu/document/download/e167c4ce-8d28-47bf-84bd-170edcf28333_en?filename=data-protection-factsheet-sme-obligations_en.pdf> accessed 8 August 2024

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, applicable from 25 May 2018

Nevada Revised Statutes § 719.240 (2017)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (e-IDAS Regulation)

Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group), “Draft Common Frame of Reference” (DCFR) (2009)

Singapore

Electronic Transactions Act (Cap 88) (2002)

Payment Services Act 2019 (Act 2 of 2019)

Securities and Futures Act (Cap 289) (2001); Digital Payment Token (DPT) Regulation (2020)

Switzerland

Federal Act on Data Protection (FADP) (2020)

Federal Act on the Financial Market Infrastructure (FinMIA) (2018)

Federal Act on Collective Investment Schemes (CISA) (2020); Swiss Blockchain Act (2021)

Uniform Electronic Transactions Act (UETA) 1999

UNIDROIT, "Principles of International Commercial Contracts" (PICC) (2010)

United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce 1996, art 2(1)(a)

United Nations Convention on the Use of Electronic Communications in International Contracts 2005, art 4(1)(c)

UNCITRAL Model Law on Electronic Signatures 200 Commission Implementing Decision (EU) 2016/650 of 26 April 2016 on the criteria for the security of qualified electronic signature creation devices

Cases

In re Tezos Securities Litigation (ND Cal, 7 August 2018) Case No 17-cv-06779-RS

C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECR I-0000