



Edited by
Hung-Yi Chen
Pawee Jenweeranon
Nafis Alam

Global Perspectives in FinTech

Law, Finance
and Technology

palgrave
macmillan

Global Perspectives in FinTech

Hung-Yi Chen · Pawee Jenweeranon ·
Nafis Alam
Editors

Global Perspectives in FinTech

Law, Finance and Technology

palgrave
macmillan

Editors

Hung-Yi Chen
Meta Intelligence
Kaohsiung, Taiwan

Pawee Jenweeranon
Faculty of Law
Thammasat University
Bangkok, Thailand

Nafis Alam
School of Business
Monash University Malaysia
Kuala Lumpur, Malaysia

ISBN 978-3-031-11953-8 ISBN 978-3-031-11954-5 (eBook)
<https://doi.org/10.1007/978-3-031-11954-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer
Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG

The registered company address is: Gewerbstrasse 11, 6330 Cham, Switzerland

FOREWORD BY NAOYUKI YOSHINO

The banking and financial landscapes have been inundated with technology over the last decade, with FinTech, InsurTech and RegTech being just some of its new applications in finance. *Global Perspectives in FinTech: Law, Finance and Technology* helps readers in clarifying key terms that have emerged in the vivid field of FinTech. It links keywords, from law and regulations, to finance and technology.

This book highlights the idea of understanding different disciplines in FinTech. It commences with introducing readers to the fundamentals of FinTech and the importance of regulation. It emphasises the importance of privacy issues and criminal activities caused by new forms of finance driven by FinTech. The book delves into understanding regulatory innovation with the aim of providing best practices and lessons learned from countries across the world. It advances with digital assets in FinTech and ends with financial inclusion where Fintech can contribute to building a better society.

This edited volume distinguishes itself by focusing on the academic works of scholars with a different area of specialisation in the FinTech field, including technology, innovation and regulation. A practical compendium that explains concepts and follows through on applications in FinTech, including its challenges and evolving nature, this book will

cover updated information in the area of Fin Tech which will be of interest to students, scholars, practitioners, as well as regulators and policymakers.

Naoyuki Yoshino
Former Dean, Asian Development
Bank Institute
Professor Emeritus
Keio University
Tokyo, Japan

Director, Financial Research
Center (FSA)
Government of Japan
Tokyo, Japan

Adjunct Professor
GRIPS
Tokyo, Japan

Visiting Lecturer, Graduate
School of Public Policy
University of Tokyo
Tokyo, Japan

FOREWORD BY BRYAN ZHENG ZHANG

The increasing adoption of technology in financial services has enabled the emergence of new financial instruments, channels, assets and systems in the last decade, blurred the lines of institutional arrangements and challenged the existing regulatory and policy boundaries. *Global Perspectives in FinTech: Law, Finance and Technology* is therefore a timely publication, contributing to academic literature and furthering our understanding of Fintech and its business, legal and regulatory implications. This book provides a comprehensive and multidisciplinary analysis of FinTech from various perspective, at both global and regional levels. It covered important topics such as FinTech regulation, data privacy and protection, financial crimes, regulatory innovation, regulatory issues surrounding digital assets and policy considerations for financial inclusion.

Fintech has never been purely about technological advancement, or the development of tech-enabled innovative business models, but it needs to be understood in a socio-economic as well as a political-cultural context. With rapid growth across almost all Fintech verticals in the last few years, especially during the global pandemic, issues such as consumer protection, financial stability, data privacy, cybersecurity and financial inclusion become increasingly pertinent for regulators and policymakers to consider around the world. With a flurry of new entrants to the market, including financial incumbents and BigTechs, and a wide array of new activities and business models, we need to research more urgently and critically about the legal, regulatory and policy implications of digital financial services,

especially in relation to the millions of consumers and SMEs that they are serving on a daily basis. This book makes a positive step in that research direction, and I hope readers from across disciplines will find it informative and useful

On a personal level, I have had the pleasure in working with all three editors Hung-Yi, Pawee and Nafis through the collective work that we have done at the Cambridge Centre for Alternative Finance at the University of Cambridge Judge Business School in the last few years. This book is a great example and indeed a fruit of academic collaboration that I hope may long continue and thrive.

Bryan Zheng Zhang
Co-Founder and the Executive
Director of the Cambridge Centre
for Alternative Finance (CCAF)
Judge Business School
University of Cambridge
Cambridge, UK

FOREWORD BY DAVID DONALD

Finance has been tied to available technology since the Mesopotamians first used stone engraving to memorialise debt obligations; millennia later, the Rothschilds perfected communications within their European network of carrier pigeons to anticipate market developments and Scottish Widows applied statistical analysis of data to create a pension fund. Today, however, the process has taken a quantum leap: enormous quantities of data come together at high speed to be processed by artificially intelligent systems with precision human thought cannot match. This concentration of data and processing power applied to finance has thus earned its own the name – “FinTech”.

The resulting, radical changes in market operation are occurring within an ideological context in which powerful private actors aspire to replace traditional prerogatives of government by introducing private cryptocurrency and stablecoin to supplement or even replace fiat currencies.

The issues of market integrity, consumer protection and data privacy that arise within this explosive context are of course many, and pressing. *Global Perspectives in FinTech: Law, Finance and Technology* offers insightful analysis of the major market innovations and the regulatory challenges, as well as a look at the future private challengers to central bank currency.

Although FinTech has been widely discussed for many years, the academic literature on its nature and regulatory challenge is still incomplete. *Global Perspectives in FinTech* presents useful conceptual modelling

of the legal challenges of FinTech, detailing its innovative achievements, their regulation, data privacy risks, potential and novel forms of crime, as well as opportunities for financial inclusion.

Global Perspectives in FinTech lives up to its name by providing expert analysis of many jurisdictions leading FinTech innovation in Asia and Europe. We can expect this book to become essential reading for students seeking to understand the future of finance, and also expect the book to be found on the bookshelves of market participants, financial lawyers, regulators and policymakers.

David Donald
Emeritus Professor
The Chinese University of
Hong Kong
Hong Kong, Hong Kong
Attorney at Law
New York, NY, USA

CONTENTS

1	Introduction: Global Perspectives in FinTech—Law, Finance and Technology	1
	Hung-Yi Chen, Pawee Jenweeranon, and Nafis Alam	
2	FinTech Regulation—A Key to Financial Stability	9
	Nafis Alam	
3	Privacy, Data Protection, and Public Interest Considerations for Fintech	25
	Aleksandr P. Alekseenko	
4	Financial Crimes in the Age of the Digital Economy and FinTech	51
	Eva Huang, Xi Nan, and Jun Zhao	
5	Regulatory Innovation in FinTech	79
	Hung-Yi Chen	
6	Digital Assets and Central Bank Digital Currency in ASEAN	97
	Pawee Jenweeranon	
7	Cryptocurrency, Stablecoins, and Blockchain	117
	Pawee Jenweeranon	

8 Fintech for Financial Inclusion	155
Felix Honecker and Dominic Chalmers	
Index	175

LIST OF CONTRIBUTORS

Alam Nafis School of Business, Monash University Malaysia, Subang Jaya, Malaysia

Alekseenko Aleksandr P. Department of Commercial Law, Saint-Petersburg University, Saint-Peterburg, Russia

Chalmers Dominic University of Glasgow, Glasgow, UK

Chen Hung-Yi Meta Intelligence, Kaohsiung, Taiwan

Honecker Felix University of Glasgow, Glasgow, UK

Huang Eva University of Sydney Business School, Darlington, NSW, Australia

Jenweeranon Pawee Thammasat University, Bangkok, Thailand

Nan Xi University of Sydney Business School, Darlington, NSW, Australia

Zhao Jun University of Sydney Business School, Darlington, NSW, Australia

LIST OF FIGURES

Fig. 2.1	FinTech risk to financial stability (<i>Source</i> Author view)	17
Fig. 4.1	Questions to ask in the data labelling process	74
Fig. 4.2	A post on Instagram that relates to tax evasion activities	75
Fig. 4.3	Regtech demo results	76

LIST OF TABLES

Table 2.1	Financial service offerings by BigTech companies	15
Table 2.2	Identified FinTech regulations by Key Jurisdictions	19
Table 5.1	FinTech governance matrix	92



Introduction: Global Perspectives in FinTech—Law, Finance and Technology

Hung-Yi Chen, Pawee Jenweeranon, and Nafis Alam

INTRODUCTION

FinTech is an emerging field, and most of the existing literature appears in the form of industry reports, consulting reports, working papers and policy recommendations. Although the FinTech subject has been widely discussed for many years, there is a lack of literature on some categorizations of FinTech. It is evident that technological innovations in financial services are increasingly transforming the way financial services

H.-Y. Chen
Meta Intelligence, Kaohsiung, Taiwan
e-mail: hungyi@meta-intelligence.tech

P. Jenweeranon
Thammasat University, Bangkok, Thailand
e-mail: paweejen@tu.ac.th

N. Alam (✉)
School of Business, Monash University Malaysia, Subang Jaya, Malaysia
e-mail: nafis.alam@monash.edu

are provided and used by consumers. This transformation varies across the globe and brings the way FinTech is being understood, applied and regulated in different jurisdictions. Globally, FinTech has opened up new and innovative opportunities for the financial services industry but, at the same time, has been engulfed with potential risks to consumers and investors and, more broadly, to financial stability. Thus, it is important to understand the global perspectives in FinTech with a focus on technology, innovation and regulation.

Many countries are trying to develop regulatory instruments in response to financial technologies (FinTech). Specifically, proper regulatory instruments for FinTech are needed to strike a balance between market simulation and risk management. This can lead to the use of new technologies in finance in many ways, such as digital finance to enhance financial inclusion in developing countries. However, in terms of law, finance and technology, it is still challenging for all stakeholders, including regulators, to identify a proper regulatory approach to achieve the goal as mentioned above in a sustainable way.

Globally, there are lessons learned from many countries across the globe in the past many years in terms of regulatory responses for FinTech. It is widely accepted that strict regulation can result in overregulation problems that impede innovation and competition. In the meantime, unregulated businesses can mitigate consumers' risks.

It is important to explore various aspects of FinTech, the legislative efforts of countries and its relation to technological development. This is necessary to demonstrate different levels of regulatory frameworks in relation to certain categories of FinTech businesses. In particular, it will be interesting to observe how regulatory innovations such as a regulatory sandbox initiative and innovation offices, along with other supporting initiatives are pushing FinTech growth in certain jurisdictions.

Nowadays, it can be seen that regulators are receptive to fast-growing technologies such as FinTech; however, they continue to face difficulties in supervising and regulating FinTech businesses due to a number of factors. For instance, the lack of understanding of the technologies presents regulators with difficulties in regulating such businesses. On the other hand, resource insufficiencies with respect to staff, expertise and tools are key concerns amongst regulators. In other words, regulators across the globe are actively responding to fast-growing technologies, including those that are being used in the financial sector. While FinTech-related regulations have only recently been developed in a number of

jurisdictions and regulators in many jurisdictions are still attempting to balance the above-mentioned FinTech regulatory goals, new innovative regulatory tools such as the regulatory sandbox, innovation offices and Regulatory Technology (RegTech) have the potential to be tools for regulators in implementing and drafting suitable regulations for such technologies.

In terms of regulatory responses, to design proper regulatory framework for FinTech is challenging. This is also because the restrictions must be specified by each regulator depending on different local contexts; for example, in Singapore, the country ranked as the most innovative according to the innovation index¹ and outlined various options for its regulatory sandbox, in particular a normal sandbox and express sandbox to support different kinds of innovations.²

To overview, for the FinTech regulatory framework, the following issues should be included in such regulations—qualifications of digital financial services businesses (market entry) and requirements or restrictions to prevent operational risks and to protect consumers and other stakeholders involved. All requirements and restrictions need not over-regulate such platforms, as they may possibly impede the utilization of innovations. However, the situation may be different in a country which had a well-established regulatory framework and supervisory mechanism such as Singapore. Non-binding guidance could be more proper to provide clarity in this case. To this, this book presents regulatory analysis of various FinTech sectors that consist of different challenges and its stage of development.

In terms of the advantages of FinTech, FinTech is promising to be utilized in many ways due to a variety of factors, including the number of internet users, social users and mobile subscriptions. These statistics are significant in terms of the use of digital finance to expand access to financial services. However, again, financial technology is a fast-growing area of innovation, and its characteristics have led to difficulties for regulators

¹ “Singapore flexes its standing as Asia’s technology’s capital”, EDB Singapore, accessed August 10, 2019, <https://www.edb.gov.sg/en/news-and-events/insights/innovation/singapore-flexes-its-standing-as-asias-technology-capital.html>.

² “MAS Launches Sandbox Express for Faster Market Testing of Innovative Financial Services”, *Monetary Authority of Singapore*, August 7, 2019, <https://www.mas.gov.sg/news/media-releases/2019/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial-services>.

in identifying a suitable regulatory approach. For example, to demonstrate the general benefit of FinTech, FinTech can be used to enhance access to finance for households and to strengthen the capacity of SMEs in accessing it. First, FinTech can increase the institutional innovation capacity of traditional banks and/or financial institutions. Second, it can provide alternative sources of funding through innovative channels. Third, FinTech can enhance access to credit by making use of alternative sources of data. Also, as an indirect consequence of FinTech development, FinTech also has promise in non-urban areas, the economic development of which rely heavily on local products or small and medium enterprises.

Globally, the success of many countries such as China and India in the use of digital financial inclusion³ reflects the promising use of digital or alternative finance in ASEAN countries. However, there are many regulatory difficulties in adopting digital finance as a tool to solve financial exclusion problems in emerging economies. In particular, the most significant difficulty would be the lack of regulatory support and/or the overregulation of digital finance-related businesses. This can reflect correlation between law, finance, and the way to utilize technologies.

Accordingly, it is significant to explore challenges in FinTech field. Basically, it is still challenging for regulators, especially in developing countries, to make laws that can keep pace with fast-growing technologies in particular in financial sectors. Such fast-growing technologies include various types of technologies utilized in many industries. The most notable example may be the challenge regulators have faced in regulating blockchain technology due to the technology's inherent features. These include its decentralized nature, which means that regulations cannot focus on any specific points, as in centralized cases.⁴

Experience from other countries should also be taken into consideration for developing such digital ecosystems at the domestic level for local enterprises and all stakeholders in general. However, lessons learned at the domestic level also demonstrate the failure of the adaptation of foreign legislations that are not applicable in the context of some other countries.

³ David Lee Kuo Chuen and Robert Deng, *Handbook of Blockchain, Digital Finance, and Inclusion* (Academic Press, 1st Edition, 2017), 39.

⁴ Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 1st Edition, 2019), 56.

GLOBAL PERSPECTIVES IN FINTECH: SPECIFIC ISSUES

The emergence of Financial Technology (FinTech) startups has created a new breed of financial services providers. The rapid adoption of digital platforms, Neobanks and investment in digital assets has forced regulators to go beyond traditional regulatory and supervisory guidelines. Some big FinTech startups are now not too small to be ignored and if not regulated well can create challenges for financial stability. This issue has been captured in Chapter 2 which explores the risk emerging from FinTech and how it can impact financial stability. In addition the chapter also provides commentary on the recent regulatory responses to FinTech across different jurisdictions.

FinTech is all about the processing of information about customers and its analyses. The cross-border transfer of personal data by FinTech companies raises many issues concerning the regulation of data privacy. Currently there are not any internationally adopted standards for data protection. Chapter 3 on privacy, data protection and public interest considerations for FinTech presents problems concerning the lack of universal data protection standards globally. FinTech businesses' cross-border transfers of personal data create a slew of concerns about data privacy laws. On the one hand, it is critical to protect consumers' privacy, yet anonymity may jeopardize the public's interest. This chapter also examines the issues posed by FinTech in terms of data privacy laws based on comparative research. It's concluded that a model for an international legislative framework on data privacy is required. It has the potential to coordinate government methods and standardize FinTech policy.

In the digital age, financial crime against banks and other financial services institutions are accelerating rapidly. In 2021, global online fraud attack rates grew by a staggering 223%.⁵ Chapter 4, Financial Crimes in the Age of the Digital Economy and FinTech, analyses financial crimes in the age of the digital economy and FinTech, briefly explaining different types of financial crimes, such as money laundering, tax evasion, financial fraud or dishonesty, cybercrime in finance, terrorist financing, bribery and corruption. More specifically, this chapter also provides an illustrative scenario of the detection of financial crimes through the detection of cross-border transaction-based tax evasion on social media platforms. Through an instructive example in the shape of a Regtech tool, this

⁵ <https://opengovasia.com/cybersecurity-malysias-astounding-achievements/>.

chapter tries to shed light on this darker side of FinTech. It aims to unpick the complexity of how to harness the potential of FinTech.

FinTech innovations have led to a more mainstream presence prompting the regulators to explore suitable regulatory environments. Covid-19 has also increased the overdependence on FinTech solutions which prompted to more regulatory innovations. A study conducted by the World Bank and CCAF in 2020 indicated that during the COVID-19 pandemic “The majority of respondent regulators have either accelerated existing regulatory innovation initiatives or introduced new initiatives. For example, 72% of respondents have either accelerated or introduced initiatives on digital infrastructure, 58% have either accelerated or introduced initiatives regarding RegTech/SupTech, and 56% did so in regard to innovation offices. Regulators from emerging market and developing economies are more likely to have developed new initiatives or accelerated planned initiatives. [...] in light of Covid-19”.⁶ This sentiment on regulatory innovation has been captured in Chapter 5, Regulatory Innovation in FinTech, where the author reviews the existing theories and academic discussion and better options for FinTech governance. The chapter provides a matrix to map out four types of regulatory approaches based on case studies across jurisdictions, spanning various mechanisms, which includes regulation, innovation offices, regulatory sandboxes, industry associations, credit ratings agencies and government-linked accelerators. How these different mechanisms operate in theory and practice is the subject of this comparative analysis.

The limited usage of cash and the popularity of cryptocurrency has led to many governments considering the digital form of money, leading to the birth of the Central bank Digital Currency (CBDC). Over 90 central banks⁷ globally are exploring CBDCs with countries such as Nigeria (e-Naira) and East Caribbean countries that have already launched CBDCs, while a majority of the developed and emerging markets are either in pilot or research and development phase. Chapter 6, Sovereignty and Cryptocurrencies: Towards Central Bank Digital Currency, explores the regulatory and legal responses to the rise of cryptocurrencies. The chapter provides a comparative overview before delving into some of the major

⁶ World Bank, CCAF and WEF, The Global Covid-19 FinTech Regulatory Rapid Assessment Report, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-reportfintech-regulatory-rapid-assessment.pdf>.

⁷ <https://www.atlanticcouncil.org/cbdctracker/>.

technical factors that underpin cryptocurrencies and their marketplaces. With the goal of determining if and how cryptocurrencies will be able to undermine the traditional notion of a state's monetary sovereignty. From this vantage point, the chapter examines the potential and actual provisions of the CBDCs and their regulation via a comparative lens. The chapter also discusses and contrasts various private, public and hybrid efforts throughout the world, despite its concentration on the EU framework.

The varied features of cryptocurrencies and stablecoins from security to non-security tokens can lead to complexity from a regulatory standpoint. Keeping this in perspective, Chapter 7 tries to differentiate “crypto assets” from “digital assets” in the blockchain ecosystem. The varied features of digital assets, from security to non-security tokens, lead to complexities from a regulatory standpoint. A token's legal status depends on its main function or the type of token being considered; accordingly, the tokens' categories are helpful for capturing the complexities of digital assets and for guiding effective regulatory responses. The complexity of the structure of digital assets has led to concerns from regulators and all relevant stakeholders, such as consumer risk and money laundering concerns. It aims to catalogue the main types of crypto assets in the market as is necessary for the regulatory analysis.

FinTech innovations are also revolutionizing the finance industry and yielding significant benefits on underserved populations and thus increasing the financial inclusion. It is overwhelming to see that FinTech is helping to make financial services accessible to populations who were left from the traditional financial services system. In this regard, Chapter 8 delves into the intricacies of the debates around FinTech for financial inclusion and outlines some of the main issues affecting practitioners and policymakers today. This chapter provides a comprehensive overview of the causes and consequences of financial exclusion. It also outlines the FinTech opportunity by illustrating how FinTech introduces a new toolkit for addressing these intractable problems and how it enables approaches that had previously not been at our disposal. Three success stories are included to illustrate how FinTech for financial inclusion is making an impact in markets as diverse as Kenya, China and Scotland.

CONCLUSION

It can be seen from above that the FinTech landscape is evolving at a rapid pace due to rapid transformations. These transformations are impacting the technology behind FinTech, the application of these technologies on the financial services industry and the overall legal environment of the FinTech ecosystem. The rich field of FinTech has thus far lacked a holistic and concerted scholarly focus on comparative and global perspectives. This work offers new inroads into the global and comparative streams within FinTech by presenting emerging frameworks and approaches to topics ranging from privacy and cryptocurrency to innovative regulation and financial mathematics. The volume brings together a group of international FinTech scholars to highlight emergent global, interdisciplinary perspectives within the field of FinTech, particularly as they have importance for comparative legal analysis. The book aims to present a timely addition to the literature given the urgent FinTech issues that continue to surface in an age of rapid globalization.



FinTech Regulation—A Key to Financial Stability

Nafis Alam

INTRODUCTION

The financial system is experiencing a rapid transformation thanks to the incorporation of new technologies, the rise of startups, and the heightened interest of the big technology (BigTech) firms in the financial sector. Even though the technological advancement and introduction of new players are driving the growth of financial services, it also brings some never seen risks and intensifies some of the existing risks. This creates many challenges for the regulators to manage the risks entailed by FinTech. FinTech can pose risks to the consumers who are using products and services originating from FinTech startups to the firms themselves who are part of the FinTech ecosystem and the overall financial stability of the country where they are incorporated. When it comes to the regulators and policymakers, even though consumers and FinTech firms will be equally important to them, financial stability is the key focus within their

N. Alam (✉)

School of Business, Monash University Malaysia, Subang Jaya, Malaysia
e-mail: nafis.alam@monash.edu

regulatory perimeter. To set the direction of the chapter, the next section will talk about the risks posed by FinTechs, with a particular emphasis on the risk to financial stability. The chapter will then focus on the key regulatory approaches to safeguard financial stability in the major jurisdictions. The chapter will also outline how the regulators can be well prepared to overcome any anomalies arising from FinTech, which can threaten financial stability.

FINTECH RISK

As per the report of KPMG,¹ regulators have identified risks arising from FinTech-related drivers, namely the increased dependence of financial services firms on technology and the growing interconnectedness within the financial sector, leading to a greater concentration of similar technology solutions within the financial sector. Most Financial Institutions (FIs) are overly dependent on technology solutions to automate their activities. Usage of technology such as machine learning, blockchain, artificial intelligence, cloud computing, and Robo advisory is mainly used for automation and strategic decision-making with limited human intervention. On one side, this brings cost and process efficiency but can also make them prone to technology-fuelled biases and misalignment between technology and business strategies. Due to the interconnectedness of the financial sector, FinTech as a Service (FaaS) is gaining prominence as most FIs will be either outsourcing for FinTech capabilities or using the same big tech solution providers giving rise to a systemic level of FinTech-related risk. In case there are vulnerabilities in one tech solution, it will impact many FIs. FIs' reliance on third-party providers for critical technology services must also understand the third party's resiliency and recovery capabilities in the event of technology disruption.

FinTech risk can impact the users of FinTech, providers of FinTech and both, in turn, can affect the overall financial stability of the system. We will next explain the impact of FinTech risk on each segment.

¹ <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf>.

FinTech Risk to Consumers

Although it is anticipated that FinTech should bring convenience and benefit to the consumers, there are areas of FinTech applications that can pose a substantial risk to the consumers. The dangers posed by FinTechs to consumers can be broadly categorized around the loss of privacy; personal data breach; use of digital channels leading to risks of fraud and scams; lack of consumer understanding of FinTech products and services; mis-selling of FinTech products; harmful manipulation of consumer behaviour, financial exclusion of tech knowledge deficient customers as well as risks emanating from tech firms entering the financial regulatory space that lack adequate knowledge of the financial ecosystem, operational effectiveness, and financial stability.

Out of the above FinTech risks, the two most common themes are either related to cyber fraud or data privacy and data security.

One of the biggest concerns for consumers dealing with FinTech products and transacting through digital means is suffering losses from cyber fraud. Consumers dealing with FinTech startups may face a heightened risk of encountering financial losses due to the vulnerability of the platform or technology unreliability or vulnerability. Consumers may be more vulnerable to cyber fraud when acquiring fintech products than when accessing financial products through more traditional channels because interaction with providers is largely or exclusively via digital and remote means. Platform or other technology malfunctions can have adverse impacts on consumers ranging from the inconvenience and poor service to monetary loss and loss of data integrity, the risk of which may be increased due to heavier reliance on automated processing of transactions.

Customer data is the most important asset of the financial ecosystem as it is being used extensively by product and service providers. Data privacy and data security issues may arise from the growing volumes of customer data, access to and secure storage of these data, and the flows of data between financial institutions and third-party service providers. In order for FinTechs to flourish and gain customer trust, data privacy and data security should be the utmost priority.

In addition to the above, customers are further exposed to the vulnerability of the FinTech platform due to underlying technology unreliability. In the early days of the startups' life cycle, due to lack of resources, the security system can be vulnerable. This can expose consumers to higher risks of loss and other harm, including third-party fraud. Generally, online

financial services platforms are subject to far higher rates of fraud than are traditional branch-based financial institutions. Another data-related risk for consumers arising from FinTech is the usage of customer data by the platforms. It is evident that the availability of non-traditional data can bring tremendous benefits to FinTechs, enabling digital lending platforms to authenticate identity and safely underwrite loans to people with complex credit profiles. However, this identity authentication can also be misused or abused as FinTech platforms leverage Big Data and Artificial Intelligence in algorithmic analysis to guide business decisions like targeted marketing and pricing thus putting consumers at the receiving end.

Risk to FinTech Providers

In the financial services industry, it is a well-known fact that FinTech is *one* of the most well-funded and *fastest-growing* areas. Such is the euphoria in the market that investors have poured US\$91.5 billion into FinTech firms in 2021, nearly doubling the previous year's figure and it is expected that the FinTech market is all set to reach US\$324 billion by 2026.² But, unfortunately, a sad reality is that nine out of ten startups fail and FinTech ³startups are not immune to it. In fact, the stakes are much higher and risks are far greater for FinTech startups.

Apart from the technology risks to the FinTech platforms which is an apparent risk, many FinTech platforms fail due to a flawed business model or lack of funding to run a viable startup in a long run. Even though with a huge amount of investment available, it is true that many platforms fail to have sustained investment to survive in the long run. For FinTech startups, to have innovative products and solutions, retain top talent, and continue to innovate, funds upfront with continuous investments is significant for these startups. Compliance costs and legal aspects of the business model are also significant risks for FinTechs. FinTech startups need to stay compliant with their offerings and should be cognizant of know-your-customer (KYC), anti-money laundering laws, anti-terrorist funding regulations, and consumer data protection aspects which can augment the risk of product failure leading to startups failure.

² <https://innovate.u.plus/state-of-fintech-2022-report>.

³ <https://startupgenome.com/report/gser2021>.

As much as consumers have the cybersecurity risk of using FinTech services, FinTech platforms are vulnerable to hacks and cyberattacks. Research by ImmuniWeb has found that 98% of the top 100 global FinTech startups are vulnerable to major cyberattacks⁴ including phishing, app security attacks on mobile and web, etc. Given that FinTech's operation is very much investment-driven, many FinTech platforms are struggling to keep up with the rapid pace of new technologies and, as a result, are not making the appropriate investments to increase operation's efficiency and reduce technology risk attached to their operation.

FinTechs also encounter customer retention risks. Due to competitive pressures within a given vertical where the customers have a high propensity to switch between providers more easily making it challenging for the small players to survive in a cut-throat competitive market. In addition, FinTechs also face governance risks. Due to the involvement of the same group of investors or founders having a huge stake in the platform, FinTechs also face CEO duality challenges (position, where the CEO is holding two positions first, holds an office as a CEO and also serves as a chairman of the board of directors). Most FinTechs fail to disclose corporate governance indicators which can also lead to failures such as Wirecard bankruptcy.⁵

FinTech Risk to Financial Stability

It is well established that FinTechs bring cost efficiency and increased financial inclusion to the financial services industry. But, at the same time, it can also lead to a greater concentration (perhaps even to the point of single dominant operators) of some big players in some FinTech segments, arising from economies of scale in the application of emerging technologies like Machine learning, Artificial intelligence, etc. There could be negative financial stability implications from over-dependence on a limited number of FinTech providers in some markets, the complexity and opacity of their partnership activities, and potential incentives for risk-taking by incumbent financial institutions to preserve profitability (FSB, 2022). In order to understand FinTech's risk to financial stability, it is important to define what is financial stability. Financial stability can be

⁴ <https://www.immuniweb.com/blog/fintech-application-security.html>.

⁵ <https://www.ft.com/content/ac949729-6167-4b6c-ac3f-f0aa71aca193>.

defined as “a condition in which the financial system is not unstable” which can be due to the instability of either, institutions, market, or infrastructure. Financial stability is an essential requirement not only for price stability, the policy goal of the central bank but also for the healthy development of the economy. For this chapter, the discussion is focused on financial institutions (read FinTechs) stability. The stability of financial institutions refers to a condition in which individual financial institutions are sound enough to carry out their financial intermediation function adequately, without assistance from external institutions including the government.

The emergence of BigTech (refers to the major technology companies such as Apple, Google, Amazon, Facebook, and Microsoft, which have an inordinate influence on the global digital ecosystem) in the financial system has become prominent in recent times. Big tech firms’ involvement in finance started with payments, where they have reached a substantial market share in countries like China (Big Techs like Baidu, Alibaba, and Tencent). BigTechs are also expanding into other financial services such as the provision of credit, consumer financing, open banking, crowd-funding, asset management, and insurance among others. A snapshot of their activities can be seen in Table 2.1.

It can be seen from Table 2.1 that most BigTechs (including new startups) have ventured into the realm of traditional financial services and if they are not well regulated they can pose a threat to financial stability. To get a better insight into how FinTechs (including BigTechs) can have an implied risk to financial stability, it is important to understand how FinTechs can create risks to financial stability. Initially, FinTechs can be too small in size and thus regulators do not see a need to regulate in the sense that in isolation they might not create systemic risk but over the period of time can increase risk when carried out the activities cumulatively, partially due to lack of effective cross-sectoral regulation. But, over the period, through interconnectedness with incumbents in the market (banks and other regulated non-banking firms) and/or carrying out systemically important activities like payments, lending, etc. they can become too large to ignore and eventually they can create scenarios where FinTechs and BigTech become “too big to fail”, as shown in Fig. 2.1.

A related risk might also appear in the sense that competition from BigTech and FinTech entrants may create incentives for incumbent financial institutions to increase risk-taking. For instance, due to competitive pressure, incumbent banks and insurers could engage in riskier lending or

Table 2.1 Financial service offerings by BigTech companies

<i>Big tech</i>	<i>Main business</i>	<i>Banking</i>	<i>Credit provision</i>	<i>Payments</i>	<i> Crowd-funding</i>	<i>Asset management</i>	<i>Insurance</i>
Google	Internet search/advertising	✓*		✓			
Apple	Tech/producing hardware			✓			
Facebook	Social media/advertising			✓			
Amazon	E-commerce/online retail		✓	✓	✓		✓
Alibaba (Ant Group)	E-commerce/online retail	✓	✓	✓	✓	✓	✓
Baidu (Du Xiaoman)	Internet search/advertising	✓	✓	✓	✓	✓	✓
JD.com (JD Digits)	E-commerce/online retail	✓	✓	✓	✓	✓	✓
Tencent	Tech/gaming and messaging	✓	✓	✓	✓	✓	✓
NTT	Mobile communications	✓	✓	✓	✓		
Docomo							
Rakuten	E-commerce/online retail	✓		✓		✓	✓

(continued)

Table 2.1 (continued)

<i>Big tech</i>	<i>Main business</i>	<i>Banking</i>	<i>Credit provision</i>	<i>Payments</i>	<i>Crowd-funding</i>	<i>Asset management</i>	<i>Insurance</i>
Mercado Libre	E-commerce/online retail		✓	✓		✓	

✓Provision of financial service through big tech entity and/or in partnership with financial institutions outside big tech group in at least one jurisdiction. ✓* Launched in 2022 (with Open Banking)
Sources BIS (2019) Citi GPS (2018), FSB (2019), IBFED and Oliver Wyman (2020), van der Spek and Phijffer (2020); public sources; FSI
 Adapted from FSI Brief, 2021

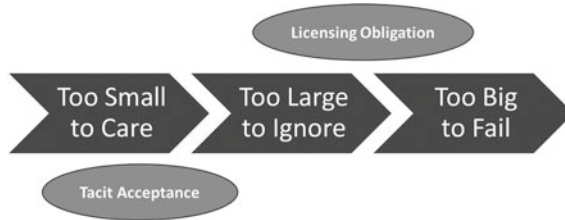


Fig. 2.1 FinTech risk to financial stability (*Source* Author view)

investment activities to preserve market share and profits.⁶ In addition to the financial stability risk emerging out of platforms, even crypto-assets can pose a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system.

It can be seen from the above discussion that there are various risks attached to FinTech impacting customers and platforms themselves but the biggest concern is the risk to financial stability. It is important for regulators to continue monitoring the developing risks to consumers, individual firms, and financial stability, and to intervene accordingly. This can be done by adopting the existing regulation (and supervision) of the incumbent financial and non-financial firms or by devising new regulations for FinTechs. In this regard, regulators can introduce new regulations for consumer protection, cyber security, data privacy, governance and disclosure frameworks data management as well as the authorization and regulation of new fintech firms. Regulations also need to expand to technology forms that are providing financial services or are an integral part of the financial ecosystem.

Good thing is that regulators across the world are taking the initiative to expand the regulatory perimeter to cover FinTech firms. The next section will discuss the regulatory measures taken by regulators to safeguard the FinTech ecosystem.

⁶ See Brits et al. (2021), Changing Landscape, Changing Supervision: Developments in the Relationship Between BigTechs and Financial Institutions, DNB, November. <https://www.dnb.nl/media/32apiuom/dnb-big-tech-supervision-changing-landscape-changing-supervision.pdf>.

FINTECH REGULATION

Regulators are becoming more proactive in the FinTech space in order to understand the risks and concerns associated with the FinTech industry and thus the list of regulatory and supervisory responses to FinTech-related risks continues to increase. Regulation is important for the financial services industry to have a level playing field for all participants, to establish an orderly and reliable market to attract customers, and to provide certainty to market actors as well as a provision to redress any challenges faced by the stakeholders. Almost all countries across the globe have some level of FinTech activities and have also established FinTech enabling regulations. The World Bank Global FinTech-enabling regulations database⁷ has compiled a list of key regulations across various FinTech-related activities. This database consists of nearly 200 countries around the globe primarily to compare and contrast FinTech-related regulations globally. The regulations cover the key areas of Anti-Money Laundering; Equity Crowdfunding; Digital ID; Central Bank Digital Currency (CBDC); Peer to Peer (P2P) lending; Electronic Money; Customer Due Diligence (CDD); Cyber Security; Electronic Payment/Transactions; Cryptocurrency; Data Protection; Innovation facilitators; Cyber security; Digital Banking; and Open Banking. Table 2.2 highlights regulations in some key jurisdictions from G20, OECD, and APAC.

It can be seen from the table below that almost every country on the list has foundational regulations for Anti-Money Laundering and combatting the financing of terrorism (CFT) while the regulations related to security and transmission of data. In terms of FinTech services, digital banking and electronic money are the highly regulated ones. It is disappointing to see that very few countries have issued regulations on cryptocurrency.

CONCLUSION

It is proven that FinTechs are now an integral part of the global financial system. They have reached a substantial market share in payments, digital currency, alternative finance, etc. in some jurisdictions and are actively involved in the provision of other financial services worldwide. FinTech

⁷ <https://www.worldbank.org/en/topic/fintech/brief/global-fintech-enabling-regulations-database>.

Table 2.2 Identified FinTech regulations by Key Jurisdictions

<i>Countries</i>	<i>Anti-Money Laundering</i>	<i>Equity Crowdfunding</i>	<i>Digital CBDC ID</i>	<i>P2P</i>	<i>Electronic Money</i>	<i>CDD</i>	<i>Cyber Security</i>	<i>Electronic Payment/Transactions</i>	<i>Cryptocurrency</i>	<i>Data Protection</i>	<i>Innovation facilitators</i>	<i>Cyber security</i>	<i>Digital Banking</i>	<i>Open Banking</i>
Australia	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Austria	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
Bangladesh	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Belgium	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Brunei	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Bulgaria	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Cambodia	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Canada	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Chile	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
China	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Colombia	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Costa Rica	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Croatia	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyprus	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Czech Republic	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Denmark	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Estonia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Finland	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
France	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Germany	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Greece	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Hungary	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Iceland	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
India	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

(continued)

Table 2.2 (continued)

<i>Countries</i>	<i>Anti-Money Laundering</i>	<i>Equity Crowdfunding</i>	<i>Digital ID</i>	<i>CBDC</i>	<i>P2P</i>	<i>Electronic Money</i>	<i>CDD</i>	<i>Cyber Security</i>	<i>Electronic Payment/Transactions</i>	<i>Cryptocurrency</i>	<i>Data Protection</i>	<i>Innovation factors</i>	<i>Cyber security</i>	<i>Digital Banking</i>	<i>Open Banking</i>
Indonesia	✓		✓			✓	✓	✓	✓		✓	✓	✓	✓	✓
Ireland	✓			✓		✓	✓	✓	✓		✓	✓	✓	✓	
Israel	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Italy	✓	✓				✓	✓	✓	✓		✓	✓	✓	✓	✓
Japan	✓		✓			✓	✓	✓	✓		✓	✓	✓	✓	✓
Latvia	✓		✓			✓	✓	✓	✓		✓	✓	✓	✓	✓
Lithuania	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Luxembourg	✓		✓			✓	✓	✓	✓		✓	✓	✓	✓	✓
Malaysia	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Malta	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mexico	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mongolia	✓	✓				✓	✓	✓	✓		✓	✓	✓	✓	✓
Myanmar	✓		✓			✓	✓	✓	✓		✓	✓	✓	✓	✓
Nepal	✓					✓	✓	✓	✓		✓	✓	✓	✓	✓
Netherlands	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
New Zealand	✓					✓	✓	✓	✓		✓	✓	✓	✓	✓
North Korea	✓					✓	✓	✓	✓		✓	✓	✓	✓	✓
Norway	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓

<i>Countries</i>	<i>Anti-Money Laundering</i>	<i>Equity Crowdfunding</i>	<i>Digital ID</i>	<i>P2P</i>	<i>Electronic Money</i>	<i>CDD</i>	<i>Cyber Security</i>	<i>Electronic Payment/Transactions</i>	<i>Cryptocurrency</i>	<i>Data Protection</i>	<i>Innovation Facilitators</i>	<i>Cyber security</i>	<i>Digital Banking</i>	<i>Open Banking</i>
Pakistan	✓		✓		✓	✓	✓			✓	✓	✓	✓	
Philippines	✓		✓		✓	✓	✓			✓	✓	✓	✓	
Poland	✓		✓		✓	✓	✓		✓	✓	✓	✓	✓	
Portugal	✓		✓		✓	✓	✓			✓	✓	✓	✓	
Romania	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
Russia	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	
Singapore	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
Slovak Republic	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
Slovenia	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	
South Korea	✓		✓		✓	✓	✓			✓	✓	✓	✓	
Spain	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
Sweden	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	
Switzerland	✓		✓		✓	✓	✓			✓	✓	✓	✓	
Thailand	✓		✓	✓	✓	✓	✓			✓	✓	✓	✓	
Turkey	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	
United Kingdom	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	
United States	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	

(continued)

Table 2.2 (continued)

<i>Countries</i>	<i>Anti-Money Laundering</i>	<i>Equity Crowdfunding</i>	<i>Digital CBDC ID</i>	<i>P2P Electronic Money</i>	<i>CDD</i>	<i>Cyber Security</i>	<i>Electronic Payment/Transactions</i>	<i>Cryptocurrency</i>	<i>Data Protection</i>	<i>Innovation facilitators</i>	<i>Cyber security</i>	<i>Digital Banking</i>	<i>Open Banking</i>
Vietnam	✓		✓		✓	✓	✓		✓		✓		✓

Source The World Bank/Global Fintech Regulations Database <https://www.worldbank.org/en/topic/fintech/brief/global-fintech-enabling-regulations-database>

business models are very different from traditional banks and non-banking entities giving rise to a variety of FinTech-specific risks. Many of these risks are new to regulators and thus relevant risks are not fully captured by the regulatory approach up to now. Regulators are taking steps to address some of the regulatory loopholes and trying to bring FinTechs (including BigTechs) under the purview of the financial regulatory perimeter. The key approach to FinTech regulation is to preserve consumer interest and most importantly have a stable and robust financial system.


REFERENCES

- Bank for International Settlements, 2019. Annual Economic Report, Chapter III, “Big tech in finance: Opportunities and risks”. Accessed on 15 Jan 2022. <https://www.bis.org/publ/arpdf/ar2019e.pdf>
- Barefoot, J. A., 2020. “Digital technology risks for finance: Dangers embedded in fintech and regtech”. M-RCBG Associate Working Paper Series. (151):1–26. Accessed on 17 Jan 2022. https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/AWP_151_final.pdf
- Citi GPS, 2018. “Bank of the future: The ABCs of digital disruption in finance”, Citi GPS: Global Perspectives & Solutions, Accessed on 15 Jan 2022. <https://www.bis.org/speeches/sp181205.pdf>
- Ehrentraud, J., Ocampo, D.C., Garzoni, L. and Piccolo, 2020. “Policy responses to fintech: A cross-country overview”, FSI Insights on policy implementation, no 23. Accessed on 20 Jan 2022. <https://www.bis.org/fsi/publ/insights23.pdf>
- Financial Stability Board, 2017. “Financial stability implications from fintech: Supervisory and regulatory issues that merit authorities attention”. Accessed on 20 Jan 2022 <https://www.fsb.org/wp-content/uploads/R270617.pdf>
- Financial Stability Board, 2019. “BigTech in finance: Market developments and potential financial stability implications”. Accessed on 15 Jan 2022. <https://www.fsb.org/wp-content/uploads/P091219-1.pdf>
- Financial Stability Board, 2022. “FinTech and Market Structure in the COVID-19 Pandemic: Implications for financial stability”. Accessed on 25 March 2022. <https://www.fsb.org/wp-content/uploads/P210322.pdf>
- Financial Stability Institute, 2021. “Big techs in finance: Regulatory approaches and policy options”. Accessed on 15 Jan 2022. https://www.bis.org/fsi/fsi_briefs12.htm
- International Banking Federation and Oliver Wyman, 2020. “Big banks, bigger techs? How policy-makers could respond to a probable discontinuity”. Accessed on 15 Jan 2022. <http://www.ibfed.org.uk/wp-content/uploads/2020/07/Big-Banks-Bigger-Techs-How-policy-makers-could-respond-to-a-probable-discontinuity.pdf>

- KPMG, 2018. “Regulation 2030, what lies ahead”. Accessed on 15 Jan 2022. <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/03/regulation-2030.pdf>
- World Bank, 2021. “Consumer risks in fintech: New manifestations of consumer risks and emerging regulatory approaches”. World Bank, Washington, DC. Accessed on 15 Jan 2022. <https://openknowledge.worldbank.org/handle/10986/35699>
- Van der Spek, L. and S. Phijffer. 2020: “Will bigtechs change the European payments market forever?”, *Compact*, 2020/2, “Payments & Business Technology”. Accessed on 17 Jan 2022. <https://www.compact.nl/articles/will-bigtechs-change-the-european-payments-market-forever/>



Privacy, Data Protection, and Public Interest Considerations for Fintech

Aleksandr P. Alekseenko 

INTRODUCTION

The last decade of innovations has become an integral part of the financial industry and has shaped a novel segment of the economy, which is now referred to as Fintech (a portmanteau of the terms “financial” and “technology”) (Gai et al, 2018). The positive consequences of the adoption of Fintech are easier access to financial products and services for a large number of customers, creation of a competitive environment in the banking and corporate sectors, introduction of digital projects that contribute to ensuring a stable financial system, a reduction in transaction costs, and fast and efficient payments settlements at the national and international levels. So today, Fintech provides consumers with opportunities in the sphere of: payments and transfers; asset management; crowdfunding; peer-to-peer lending; securities trading; online banking;

A. P. Alekseenko (✉)

Department of Commercial Law, Saint-Petersburg University, Saint-Peterburg,
Russia

e-mail: a.alekseenko@spbu.ru

online accounting; insurance; blockchain and cryptocurrencies (Soloviev, 2018).

Meanwhile, new technologies have caused the appearance of new types of financial scams which are outside of the traditional fraud detection approaches and methods, as well as increased perspectives of hacker attacks because of the vulnerabilities of network systems and web applications. For example, the largest Bitcoin exchanges, Bitstamp and Bitfinex lost 19,000 and 119,756 Bitcoins, valued at more than US\$77 million because of hacker attacks, and the cryptocurrency Ether, equivalent to about US\$150 million, were stolen from the Decentralized Autonomous Organization (DAO). Therefore, for developers of novel technologies, it is necessary to take into account a whole range of risks, including regulatory risks and data security (Mehrban et al, 2020).

Fintech companies use artificial intelligence (AI) and biometrics to improve authentication, the security of payments, and to enhance customer communications (Baba et al., 2020) but at the same time, they collect various consumer data provided directly to the company or even extracted from the consumer's web search requests and websites visited. So, due to the active growth of new services based on the collection of large amounts of data, the question of data privacy has become a major concern to Fintech platforms (Hernández et al., 2019), states, and consumers. Researchers rightly note that, "a growing number of governmental and private organizations now possess and currently use data processing in order to determine, predict and influence individual behavior in all fields of human activity" (Moura & de Vasconcelos, 2020).

Everyone should bear in mind that new financial services are not as easy as they seem and, of course, are not perfect in many cases. The collection, storage, and processing of big data raise serious questions not only about the protection of personal data from hacker attacks, but also from its usage for uncompetitive and unfair actions by e-commerce and payment platforms, financial marketplaces, etc. Personal data can be exploited by Big Tech companies to extract additional economic profits and strengthen their dominant position in the market (Chirita, 2018). An illustrative

example is the case of *Alibaba*, when this Chinese company settled its domination of the e-commerce market in China¹ and the *Google* case.²

The concentration of highly sensitive private data in the hands of Fintech companies and its analysis by machines has far-reaching consequences for individuals. Based on the processed information about race, gender, sexual orientation, health, financial opportunities, habits, and even behavior, the computer algorithms may directly or indirectly discriminate and segregate consumers (Cortez, 2020), depriving some persons from access to financial services. Also, Fintech platforms have technical opportunities to analyze customers' web search history and other personal data, compare its content, and foist targeted advertising or particular goods toward them. This means that the consumption choice of a client can be highly dependent on the market policy of the service provider, i.e., Fintech business has the tools to practice exploitative abuse based on behavioral economics (Chirita, 2018).

The COVID-19 pandemic has given a strong impetus for new technologies and stressed the question of online business development. The cross-border character of internet services as well as the novelty of technologies applied stresses the necessity to shape a legal framework explaining the perspectives of Fintech development. Therefore, this research aims to examine the rising challenges posed by Fintech for data privacy, to find grounds for mutually beneficial combination of private and public interests in this sphere, as well as work out perspectives of harmonization in the sphere of financial technologies.

The chapter is organized into three sections and a conclusion. It begins with an analysis of the meaning of sensitive data, describes legal regulations on data privacy, and discusses Fintech's impact on data privacy. Following this, the chapter then describes challenges raised by Fintech for data privacy. After this, theoretical ideas about a legal framework for Fintech are outlined. The chapter concludes with a proposal to reassess the role of the state and Fintech companies in the question of providing privacy protection.

¹ China Fines Alibaba \$2.8 Billion in Landmark Antitrust Case, retrieved from: <https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html>.

² Google dominates search. But the real problem is its monopoly on data, retrieved from: <https://www.theguardian.com/technology/2015/apr/19/google-dominates-search-real-problem-monopoly-data>.

FINTECH & DATA PROTECTION REGULATIONS

Personal Data and Its Categories

To talk about the challenges concerning data protection raised by Fintech it is necessary to understand the meaning of personal data. Lundqvist states that the “definition of personal data is wide since information that is non-personal might also indirectly, in combination with other information, identify a natural person and become personal data” (Lundqvist, 2018). This is a sound conclusion because even metadata could characterize a person; in particular, a user’s web search may describe consumption habits, health, etc. Consequently, it is very difficult to list all data characteristics which are sensitive for individuals. Meanwhile, there are examples of when a legislator has provided a definition of personal data. According to art. 4 (1) of the *EU General Data Protection Regulation* (GDPR)³ that has been in force in the EU since May 2018 and applies to any Fintech company processing data in the European Economic Area:

personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

A literal analysis of the GDPR shows that it contains a closed list of data which is protected, however, commentators have argued that the GDPR secures the private sphere of a person which includes “any information stored on a user’s terminal equipment, whether personal or otherwise” (Kuner et al, 2020). As a result, the GDPR notices guide judges and companies, and shapes general marks for understanding legally protected information.

In some states, the meaning of personal data hasn’t been identified. For example, in Russia, the *Federal Law On Personal Data* in art. 3 (1) describes personal data as any information relating directly or indirectly

³ 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, and repealing Directive 95/46/EC (General Data Protection Regulation), retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>.

to a specific or identifiable individual (subject of personal data). Thus, Russian legislation does not even have an approximate list of personal data, nor any clear criteria for attributing specific information about a person to personal data. It could raise questions about the possibility of attributing certain information about a person to personal data which is especially important in an environment where digital technologies are used.

Legal uncertainty concerning the definition of private data in Russia could stress the question, whether the information received from the telecom operator allowing direct or indirect identification of the user as a specific individual is personal data. Courts have decided this issue in the following way: the data allowing the identification of the subscriber or their terminal equipment such as surname, first name, patronymic, or pseudonym of the subscriber-citizen, the subscriber's address (address of installation of terminal equipment), subscriber numbers, other data allowing the identification of the subscriber or his terminal equipment, data from databases of payment systems for communication services rendered including connections, traffic, and payments of the subscriber are considered personal data. This conclusion is from the Award of the Russian *Ninth Arbitration Court of Appeal* No 09AP-17574/16,⁴ where the court decided that personal information includes the information transmitted about subscriber's connections and traffic: cookies in the user's HTTP request, which allows distinguishing the user's traffic from the traffic of other users to get a list of his or her preferences; the IP address from the IP packet of the user's HTTP request, which allows getting the geographical location of the user with accuracy to the name of the locality; the user string hash ID, which allows determining the user hash IDs of subscribers who have expressed disagreement with data processing.

The recognition by the courts of customer requests, Internet addresses of web pages visited, IP addresses, etc., which allows identifying the person as personal data is an important step because it makes it possible to fill the gap in the legal regulation regarding the specification of data that relate to general personal data. At the same time, such a broad definition allows referring to any information as personal data, and as a consequence obstructs Fintech innovation development.

⁴ Award of the Ninth Arbitration Court of Appeal of May 23, 2016 No 09AP-17574/16, retrieved from: <https://base.garant.ru/61331067/>.

Personal Data traditionally includes special categories which are altogether called sensitive data. Sensitive data comprises information about payments, bank cards, and bank accounts; genetic, biometric, and health information; data about a user's religion, political, and sexual orientation; passwords and logins; and other information (Quinn, 2021). In other words, sensitive data is any information that is not freely available or accessible (Walters, Trakman, & Zeller, 2019) and the illegal use of which may lead to pricing, political, and other types of discrimination in their daily life or else cause damage or harm to an individual.

Regulators identify special categories of personal data among sensitive data. The GDPR settles the legal treatment concerning this in art. 9 (1). It reads as follows:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

In cases specified in art. 9 (2), prohibitions named in art. 9 (1) are invalid. Additionally, the GDPR not only introduced legal treatment for sensitive data, but also defines some of its types: genetic, biometric, and health data. Notably, in other jurisdictions, there are other special categories of personal data. According to the *Federal Law On Personal Data* art. 10 (1) in Russia, they are: data concerning race, nationality, political views, religious or philosophical beliefs, health status, and intimate life. In contrast to the GDPR, the Federal Law doesn't name personal data concerning trade union membership, sexual orientation, or genetic and biometric data.

Discrepancy in legal treatments of data is critical for Fintechs. Therefore, it is necessary to elaborate a common vision on the definition of personal data and its types. On the one hand, the unification or standardization of definitions will facilitate the supervision of cross-border transfer of data, and on the other hand, Fintech companies will have a clearer path for their algorithms and services development.

Overview of Data Protection Principles

International Principles of Data Processing

It is consistent with the provisions of a number of universal, regional, and bilateral international legal acts, including: Council of Europe Convention No. 108 on data protection of January 28, 1981, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*; *European Convention for the Protection of Human Rights and Fundamental Freedoms* of 1950; the *Geneva Convention on the Protection of Civilians during War* of 1949. The Organization for Economic Co-operation and Development (OECD) also issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which established the principles of data processing: collection limitation principle; data quality principle (data shall be relevant, accurate, up-to-date); purpose specification principle; use limitation principle; security safeguards principle; openness principle; individual participation principle, consideration of an individual's right of access and correction.

EU Principles of Data Processing

According to the EU Fintech Action plan, the GDPR is of critical importance for the proper use of innovative data-driven financial services. The GDPR could be counted as a legal regulation most adapted to modern conditions and indicative in the field of personal data protection. It has a direct effect in 28 EU countries and applies to organizations engaged in professional or commercial activity.

The core question for data protection in the Fintech epoch is how to regulate data processing and what data processing is. The GDPR in art. 4 (2) defines processing very broadly. It makes it possible to apply the GDPR's data processing provisions to profiling, including the use of self-learning computer algorithms and technologies of Big Data analysis. Therefore, the level of data protection in the EU was increased and led to enforcement actions against companies collecting and transmitting private data (Houser & Voss, 2018).

Data processing in the EU is only allowed when the user has given their consent. The consent, according to art. 4 (11) of the GDPR, means freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The GDPR in art. 5 establishes the principles of personal data processing. They are:

- lawfulness, transparency and fairness of such processing in relation to the subject of personal data (lawfulness is defined in art. 6 of the GDPR);
- prohibition of further data processing unrelated to the original purpose of collection;
- data minimization, i.e. adequate, relevant limited purpose of data processing;
- processing accuracy;
- storage limitation i.e. permission for identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, except cases indicated in art. 89 (1) of the GDPR;
- data integrity and confidentiality, i.e. protection against unauthorised or unlawful processing and against accidental loss.

Named principles formulate the basis for mechanisms of personal data protection during their collection and processing. Therefore, the GDPR “might lead to better data management and greater transparency, and will force organisations to improve their security” (Sydekum, 2018). It should be noted that the GDPR was adopted not only to optimize the functioning of the market, but to protect the private interests of personal data subjects, which in the end can affect the market, while such an impact is ambiguous and not always positive. So the deletion of information is the essential right of the data subject. At any time and in any case, the subject is empowered to withdraw one’s consent to the processing of personal data and request its deletion from a processor. Taking into account the fact that the GDPR extends its effect to any controller or data processor, the compliance with these principles is necessary both within the EU and outside it, since their violation may entail appropriate liability.

The U.S. Approach

Regulation of personal data storage in processing in the United States is complicated by a legal system consisting of federal legislation and the separate legislation of 50 states. There is not a single data protection act in the United States, therefore foreign Fintechs may be regulated by federal and state data protection laws (Pittman & Levenberg, 2021). Moreover,

the U.S. legislation doesn't provide unified definitions of personal data, data processing, controller, and sensitive personal data. However, the lack of uniform regulation is explained by the fact that personal data is considered as an integral part of the right to personal integrity guaranteed by the 4th Amendment of the U.S. Constitution, which is also of interest to large IT companies registered on their territory (for example, Amazon, Google, and others).

Brief analyzes of American legislation demonstrate that currently at the federal level, personal data is regulated by:

- Fair Credit Reporting Act;
- Electronic Communications Privacy Act;
- Computer Fraud and Abuse Act;
- Health Insurance Portability and Accountability Act;
- Financial Services Modernization Act.

The closest to the European data processing standards is the California Consumer Privacy Act (CCPA), which equates any digital footprint to personal data.⁵ Following the adoption of the law in California; the U.S. Congress began developing a federal law on the protection of personal data—the Data Protection Act⁶. Also, there are proposals to adopt the Consumer Online Privacy Rights Act and the United States Consumer Data Privacy Act.

Thus, it can be argued that in the United States, federal legislation on the collection of personal data by Fintech companies has not been formed. Only the State of California has an advanced law regulating this area. In this regard, if to compare the GDPR adopted in the EU and America's experience, it is unlikely that the U.S. approach in regulating personal data privacy issues is worth relying on.

Russian Data Legislation Overview

In Russia, detailed regulation, concerning the processing of personal data, is provided by the *Federal Law On Personal Data No. 152-FZ* dated 27 July 2006. Article 3 (3) of the Law defined personal data processing

⁵ California Consumer Privacy Act of 2018. retrieved from: https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

⁶ S.3300—Data Protection Act of 2020, retrieved from: <https://www.congress.gov/bill/116th-congress/senate-bill/3300>.

as any action (operation) or set of actions (operations) performed with or without the use of automation tools with personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, and destruction of personal data. Lawful processing of personal data is allowed in the cases listed in art. Six of the *Law On Personal Data* under the main condition that the data subject has given consent.

Also, there are other laws which regulate specific questions of data processing and transfer. For example, the *Federal Law On Experimental Legal Regimes in the Sphere of Digital Innovations in the Russian Federation* introduces exceptions to the rule of individuals' health data depersonalization for the purpose of implementing artificial intelligence technologies in the sphere of medicine. This Law in other aspects mainly affects telecom operators and Internet companies; therefore, in this chapter, it won't be analyzed.

Article 5 of the *Federal Law On Personal Data* establishes the principles of personal data processing, they are:

- lawful and fair processing of personal data;
- processing of personal data incompatible with the purposes of personal data collection is not allowed;
- restriction to combine databases containing personal data, the processing of which is carried out for purposes incompatible with each other;
- only personal data that meets the purposes of its processing could be processed;
- content and volume of the processed personal data must correspond to the stated purposes of processing;
- data accuracy, sufficiency, and if necessary relevance to a person;
- limited period for storage of personal data, after which the processed personal data shall be deleted or depersonalized.

The listed principles look similar to and don't contradict those which are described by the EU's GDPR. Of course, there are some differences, for example, the principle of restriction to combine databases, but in common, they contain the same ideas. This underlines that it is possible

to elaborate multilaterally acceptable principles for a future framework for the regulation of Fintech activities.

Data Subject Rights

Data Subject Rights Under the EU General Data Protection Regulation

The GDPR established clear rules for interaction between users and companies in the field of Fintech using personal data. This is a tool to combat manipulation and misuse of personal information and is a significant step in protecting personal information on the Internet. The GDPR defines the rights of the subject of personal data in detail. Basic rights of the data subject are:

- right of access by the data subject (Article 15);
- right to rectification (Article 16);
- right to erasure or “the right to be forgotten” (Article 17);
- right to restrict processing (Article 18);
- right to data portability (Article 20);
- right to object (Article 21);
- right to personally influence automated collection and profiling systems (Article 22);
- right to lodge a complaint with a supervisory authority (Article 77);
- right to compensation and liability (Article 82).

Thus, the GDPR provides EU resident citizens with the right to manage personal data: to be aware of the purposes, volumes, and timing of processing, to request access to it or transfer to another processor, as well as the requirement to delete it.

Rights of Subject of Personal Data in Russia

The *Federal Law On Personal Data* in articles 14–17 specifies the rights of the subject of personal data. They include:

- right of access by the data subject (Article 14);
- right to restrict processing (Article 15);
- right to object to automated data processing (Article 16);

- right to lodge a complaint against the actions of a data processor (Article 17).

One more right is ensured in art. 10.3 (1) of the *Law On Information, Information Technologies and Information Protection*—the right to be forgotten. However, the *Federal Law On Personal Data* doesn't contain a legal provision guaranteeing the right to data portability.

Data Laws Application to Foreign Companies

The GDPR Extraterritorial Application

In order to monitor compliance of national policies with the provisions of the GDPR, according to articles 51–59 each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation. For example, in France this function is performed by the *Commission Nationale de l'Informatique et des Libertés*. On December 31, 2021, this public body, based on art. 3 of the GDPR, fined *Google* a total of 150 million euros. This case stresses the importance of the GDPR's features such as the extraterritorial principle of application of its rules for the processing of personal data, as well as extraterritorial liability for violations of the rules for the processing of personal data (art.3).

Russian Concept of Data Localization

One more characteristic feature of the Russian *Law On Personal Data* is that it contains a provision forcing data processors to localize their databases in Russia. The main purpose of the localization requirement is to protect the public interests of the state. According to art. 18 (5) the operator must ensure the recording, systematization, accumulation, storage, processing, and extraction of personal data of Russian citizens using databases located on the territory of the Russian Federation, except for cases specified in the Law. Those who don't want to fulfill the named requirements will be banned from operating in Russia, as has happened to the social network LinkedIn. This rule could be a serious obstacle for foreign Fintech companies, because they must have servers in Russia for processing the personal data of Russian citizens, or make an agreement with a data processing center in Russia.

FINTECH & DATA PROTECTION CHALLENGES

Easy Data Collection

Fintech is mainly based on the analysis of personal information about the client. For the effective functioning of Fintech, personal data about customers and their financial transactions are required. Fintech services strive for inter-product cooperation, which is how they can better satisfy customer requests, i.e., there may be a need to transfer personal data, and sometimes financial assets between different applications. It is collected with the help of the open banking data standard API, which allows third parties to achieve access to banking information (Boot et al, 2021). In this manner, banks provide their customers with the opportunity to use convenient and innovative applications for which information on customer accounts and transactions is transmitted to Fintech companies.

One more source for uncontrolled data extraction is social networks. They contain information about the surnames of network users, their place of work or study, place of residence, habits, marital status, geolocation, etc. It is clear that this data was originally provided to the network during registration by the users themselves. The problem arises when the personal data of the social network users is used by third parties (commercial organizations) for their own purposes which have not received permission for this use of data, neither from users nor from the social networks, and do not pay for the use of this data. In some cases, social networks have sued in attempts to secure client information. Judicial practice in such cases is quite extensive (for example, the *Decision of the Supreme Court of the Russian Federation* of 29.01.2018 No. 305-KG17-21,291). According to the position of the courts, personal data processed by organizations contained in open sources (*VKontakte, Facebook, Instagram, Twitter*) are not publicly available. Accordingly, it is necessary to obtain the consent of the data subject to use this information.

The Question of Consent

The person decides themselves which data can be processed, and can at any moment ask the operator to remove such data from free access. As constituted in art. 4 (11) of the GDPR, and according to art. 9 of the Russian *Law On Personal Data*, the consent shall be freely given, specific, informed, and unambiguous. A particular consent of the person is not required if a customer orders goods or services by filling out a questionnaire on the website in an electronic form containing personal data

information. By submitting their data according to the specified algorithm for filling out the questionnaire, individuals have actually expressed their consent to process their personal data. Hence, according to the Russian legislation, the consent of the subject of personal data is not necessary for it to be processed if it is carried out within the execution of the contract. But it is doubtful that consent is freely given, specific, informed, and unambiguous when a customer uses the default privacy settings of the application or Internet service, especially if there isn't any evidence of attempts to change settings by the user. Herian maintains that users must voluntarily activate and consent to a smartphone's applications data policy and that "the systems will not undermine their privacy by, for example, using collected data for purposes other than contact tracing" (Herian, 2021). If a customer doesn't agree with privacy statements, it will be impossible to use a product.

Of course, sometimes the concept of consent doesn't work. The privacy statements could set forth conditions in a way that a person doesn't have the opportunity to freely express consent or refuse a transfer of personal data to third parties or otherwise influence the provisions of the consent. In this case, a person is forced to give "voluntary" consent, otherwise the service will be unavailable or the application will not function. It is an enormous problem but, for instance, there are cases when courts have proclaimed that the terms of a contract, where a consumer does not have the opportunity to express consent or refuse to process personal data, are illegal⁷.

Users provide access to their data by granting access to it for the application while choosing permission settings. They believe that services provided by developers are safe and secure. There are customers who don't analyze privacy statements while installing applications. Some of them validate all application requirements because they are unclear, long, and written in standardized language texts of privacy statements which are difficult to understand (Dorfleitner et al, 2021). Most users don't ask themselves what data will be collected, by whom and how it will be processed and to whom it will be forwarded, they just believe the advertisement that investments or payments are easy, install the application, and enjoy convenient services. The same is true for different e-commerce

⁷ Decision of the Russian Arbitration Court of the North-Western District, April 2, 2018 No A44-745/2017.

platforms. Even news sites collect information by asking you to accept “cookies.”

Implementation of new techniques for extracting and analyzing large data underlines the necessity for government supervision to avoid fraudulent actions and ensure the rights of citizens to enjoy privacy (Miglionico, 2019). Also, there is a necessity to reduce financial illiteracy of citizens, and to elaborate an approach where Fintech services will notify consumers using clear phraseology about all the consequences concerning data processing. Fintech company clients should know and understand that investing with the help of new technologies is not just easy, but also risky for their privacy.

Cybersecurity

Financial applications are one of the most popular targets for cyber attacks and hacking in order to steal personal information, financial assets, or commit fraudulent transactions on behalf of the client. For this reason, participants of financial transactions need confidence that data security is ensured, and in the Fintech companies' ability to minimize cyber risks and protect against cyber threats.

Of course, Fintechs use technologies for data protection, for example, JWT tokens granting customer authentication, encryption with symmetric and asymmetric algorithms for cloud-based applications and services (Bhardwaj & Goundar, 2019), and other types of encryption and measures for website security, which are also used to address customer cybersecurity concerns. For example, there is a scheme which protects the privacy of the customers with the help of attribute-based access control which means that “only trustable parties are allowed to either partially or fully decrypt their data” (Mehrban et al, 2020).

However, data leaks are still a real threat to ordinary users, banks, and Fintech companies. Data leaks are either disclosure of the bank's customer data by third parties, or data leakage through computer systems and various technical means.

The increasing financial damage from the commitment of cyber attacks, combined with the increasing volume of information data stored in the network infrastructure, necessitates the development of new services to ensure information security and data privacy.

Anonymity & Blockchain

Organizations which collect, record, or store personal information can ensure data privacy with the help of anonymization and pseudoanonymization. The first approach assumes a complete severance of the subject of personal data with his or her digital footprint. Thus, various companies are more interested in the second type of data, since they contain parts of personal data. Nowadays, such a highly valued commodity as customer data can be easily obtained by “inexpensively using artificial intelligence and machine learning” (Baba et al., 2020) whenever an internet user searches a website or purchases goods.

A solution on how to satisfy those customers who value their privacy, don't want to share their personal data, and prefer to keep their anonymity was found with help of blockchain technology. A blockchain is based on a system which uses a distributed ledger, where multiple knots together provide authentication. This approach eliminates the need for intermediaries, clearing and settlement systems, centralized authorities, and third parties as well as ensuring high-security and transparency. Researchers (Walters et al, 2019) note that:

the technology sector may well argue that new technology (distributed ledger technology), such as blockchain, or quantum is likely to be safe as only registered users are able to gain access. Using blockchain as an example, security begins with the network and the management of the nodes. At the private level it appears to be the security of verification within a blockchain system that is most pertinent.

The named features of blockchain make it popular in different industries, including the sphere of finance. On the foundation of blockchain in 2008 a peer-to-peer payment system was launched with a payment unit named Bitcoin (Chauhan et al, 2022), which is the world's first cryptocurrency. The developers of Bitcoin use cryptographic methods to ensure the functioning and protection of the system. Unlike bank accounts and most other payment systems, Bitcoin addresses are not connected to the identity of users at the protocol level. Anyone can create a new randomly generated Bitcoin address at any time without having to provide anyone with personal information. Everyone can transfer Bitcoins from one address to any other without having to disclose any personal information. Bitcoin's transactional information is transmitted by randomly selected nodes of the P2P network. While Bitcoin nodes connect to each

other via IP addresses, the nodes do not know whether the received transaction was created by the node that transmitted the information or just redirected it.

The introduction of Bitcoin accelerated the process for the development of different services, for example, Dark Wallet, Zerocoin, Darkcoin, Shared Coin, etc., which proposed technical solutions, such as mixing of payments, aiming to increase anonymity and to protect personal data. These blockchain features and technical decisions are in contrast with know-your-customer (KYC) and anti-money-laundering (AML) requirements. In successful cases, there would be a system allowing untraceable transactions on the Internet, and of course, impeding the growth of weapons and narcotics black markets, human trafficking, and illegal activities concerning financing of terrorism and money laundering (Foley, Karlsen, & Putniņš, 2019). Moreover, the inability to provide identification and verification of the identity of customers engaged in transactions with cryptocurrencies could undermine a state's banking systems and financial stability (Vučinić, 2020).

Thus, utilizing Fintech services as a tool for anonymous financial transactions is a great threat for central governments which are focused on "data retention, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime" (Vedaschi & Lubello, 2015). Criminal risks from activities with Bitcoin could be reduced only by a well-shaped policy toward the supervision of Bitcoin exchanges, the party's identity disclosure, and globally recognized approaches concerning cryptocurrency exchange of fiat money and goods. At the same time, the importance of self-regulation should not be underestimated. It is technically difficult to control everything in the blockchain industry, therefore, self-regulation and self-control could be a good answer for these challenges.

Regulatory Problems

Fintech generates two main tasks for national regulators. The first one is providing security for storage, transfer, and extraction of private data. The second one is combating anonymity where it could represent a threat to public interests. Considering that the Internet is a global network which could be exploited by Fintech companies to provide services around the world, the topic of how to strive to reconcile these two controversial directions is hard to decide. This regulatory difficulty is due to the fact

that the activity of a Fintech company on data processing could be legitimate in the territorial context of one jurisdiction, but at the same time, be restricted and sanctioned in another country.

Walters, Trakman, & Zeller (2019) note that individuals and entities have an opportunity to easily relocate all around the world in order to minimize the impact of particular laws on themselves. This, in turn exacerbates the data subjects' ability to manage their data flows and secure privacy. Cross-border data flows are an important element of online services (Voigt & Von dem Bussche, 2017), but unfortunately, there are not any worldwide adopted data exchange security standards in the Fintech field (Gozman, & Willcocks, 2019). The existing system of private international law, with its doctrines of choice of applicable law, is unable to overcome challenges associated with the transborder nature of data flows (Svantesson, 2011) and Fintech services (Alfárez & Fernández, 2020).

As is noted (Moura & de Vasconcelos, 2020):

In a globalized world, in which personal data can instantly circulate and be used simultaneously in communications networks that are ubiquitous by nature, these different national and regional approaches are a major source of conflicts of laws. These, in turn, are also the object of divergent solutions, ranging from the application of data protection rules on a purely territorial basis to extra-territorial choice of law regimes, according to which data protection laws may also apply to the processing of personal data undertaken by entities established outside the jurisdiction of the data subject's place of habitual residence.

The private freedoms of data owners are opposed by the public law interests of localization of personal data, including the interests of national security. As Bygrave (2014) notes, data privacy law is a sample of regulatory colonization, and this colonization is not only when the data privacy law is inspiring changes in other legal fields, but also cross-state colonization, where the regulations of one country applies on the territory of another. In recent years some states have begun to support a policy of extraterritorial application of their legislation to data flows and to expand their jurisdictions (Yang, 2021). For example, art. 3 of the GDPR extends the EU's standards externally and applies to the processing of personal data of data subjects who are not in the Union.

Therefore, the presence of the EU's Fintech platforms in the national financial market of a non-EU member state is an example of a foreign law "intervention" in the financial system of the state. Foreign Fintechs may affect certain market segments due to reliance on internationally recognized infrastructure support and change the competitive landscape in a particular country, but not adhere to local regulations. In this context, the question of ownership of personal data and the freedom to dispose of one's personal data is increasingly being raised.

SHAPING LEGAL FRAMEWORK FOR DATA PRIVACY IN THE ERA OF FINTECH PRIVACY

The Need of Internationally Recognized Principles of Data Processing and Law Enforcement

Today, there are three major trends on how to regulate data protection: adoption of specialized legislation covering several areas of the law, constitutionalize rules on data protection, and international harmonization of data protection regimes (Moura & de Vasconcelos, 2020). Not to underrate the value of national legislation, this research demonstrates that because of the transborder character of Fintech, there is a need to harmonize national policies toward personal data protection.

Therefore, it is necessary to develop regulatory principles for managing Fintech businesses based on the synergy of public-private and company-client interests. In order to elaborate a principles-based approach, it is necessary to bring together regulators responsible for different sectors and functions of Fintech as well as international institutions (Arner et al., 2021). Using this approach as a basis, states could introduce a multilateral framework for Fintech and cross-border data processing and storage, as well as dispute resolution.

Besides common principles, an international legal framework should proclaim the basic rights of data subjects, i.e., consumers of Fintech services. They should be based on the idea that data privacy covers public and private law issues (Moura & de Vasconcelos, 2020) and considers public security and the needs of private businesses and individuals.

Of course, special attention is to be paid to the states' right to apply their laws to foreign Fintech companies, including the question of liability. It seems that because of differences in national laws, extraterritorial law enforcement has a controversial nature, while another approach,

data localization, would result in higher costs. Therefore, it is necessary to introduce a new concept of law enforcement, or conclude an international convention establishing a model law standardizing and harmonizing national approaches in cases where Fintech and data privacy are concerned.

In order to prepare the ground for this initiative, the key features of different legal policies should be described, analyzed, and reconsidered. Otherwise, the Fintech industry will suffer legal uncertainty, which inter alia, will restrain development of the industry and innovation. Adoption of data processing and data transferring principles is to be organized jointly with an implementation of their commonly accepted definitions. This step will provide legal certainty, which is a cornerstone to any regulation (Amstad, 2019).

The concept of personal data, including basic principles and definitions, introduced in the GDPR is quite universal, and allows talking about the extension of the GDPR into the sphere of Fintech, which contributes to the best control over customer information collection. It seems reasonable, based on these Regulations, to harmonize the laws of different countries in order to avoid conflicts of laws, especially if it concerns the control of data mining by large multinational IT companies.

Standardization

Fintech companies don't guarantee the availability and clarity of the necessary information about the technologies and related legal, financial and other consequences of utilizing their Apps and services. In fact, when accepting the provisions of a user agreement and giving consent to the processing of their personal data, customers "are often unaware of the amount and the type of information collected about them as well as about how this information can be connected via artificial intelligence technologies to infer their characteristics" (Cortez, 2020), and unable to resist the imposition of rules by Fintech companies. This means that there is a total shift of responsibility toward the individual who gets themselves into an aggressive financial and technological environment. Therefore, the privacy statements should be modified in a way that is in the interest of the customer. To wit, users are granted the right to modify a privacy statement and App data privacy settings, especially in the question of the transfer of personal data to third parties. It is also important that the

privacy statement is written in plain language and contains all the necessary information on how the application and service will use the user's information. In this case, the problem is that there is not any single standard on how to shape a data privacy agreement. The same is true when we are talking about data security. The mitigation of cyber risks and the monitoring of macro-financial risks are among the key issues for cooperation (Chatzara, 2020). Consensus on cybersecurity standards and their interoperability for the entire Fintech market will reduce questions concerning data exchange, and equalize banks which are subject to stringent data privacy requirements with their competitors (Boot et al., 2021).

Standardization in the sphere of Fintech only by means of governmental bodies, even in the frame of a single state, seems to be complicated, but self-regulation could overcome this challenge. Scholars argue that 'for digital finance platforms, regulators could seek to enter into co-regulation agreements with operators that reflect public concerns such as systemic risk, customer protection, market integrity, and national security' (Arner et al., 2021). Thus, governmental bodies, banks, and software developers could build a network for further dialogue and elaboration of a self-regulation policy for the Fintech industry.

Mechanism of Supervision for Bitcoin and Cryptocurrency Exchanges

A combination of public and private keys provides data encryption and anonymity in activities involving cryptocurrencies (Geranio, 2017). It makes governance in the blockchain sphere difficult and stresses significant issues of various types (Vučinić, 2020), including the need for the limitation of data privacy for the public good. The process of cryptocurrency–money exchange could still be supervised and legally regulated. In this regard, Central Banks should adopt the sole general model which will extend the rules of customer authentication, anti-money laundering, etc. on cryptocurrency operations (Alekseenko & Gidigbi, 2021). Also, within the framework of self-regulation and self-control, cryptocurrency exchanges can develop a system allowing the implementation of techniques for user identification. Of course, this step will decrease data privacy, but this sacrifice is not in vain, as it decreases criminal risks.

CONCLUSION

Fintech is transforming the financial services industry, and therefore, requires special regulation or amendments to existing legislation. This chapter illustrates that the main concern relates to the question of the absence of recognized standards for data privacy and gaps in legal regulation of data processing. Despite the fact that many countries are developing a national framework for financial technologies, Fintech as a cross-border technology has revealed many challenges in the financial sector, which can be solved only by the harmonization of data privacy approaches and data processing requirements for standardization in a way which is mutually beneficial for public and private interests.

REFERENCES

- Alekseenko, A. P., & Gidigbi, M. O. (2021). Legal regulation of a cryptocurrency used in Nigeria and Russia: a comparative study. *International Journal of Blockchains and Cryptocurrencies*, 2(2), 187–203.
- Alfárez, F. J. G., & Fernández, S. S. (2020, December). Is private international law tech-proof? Conflict of laws and FinTech: selected issues. In *The Elgar Companion to the Hague Conference on Private International Law*. Edward Elgar Publishing.
- Amstad, M. (2019). Regulating Fintech: Objectives, principles, and practices. *Asian Development Bank Institute Working Paper Series*, 1016.
- Arner, D. W., Buckley, R. P., Charamba, K., Sergeev, A., & Zetzsche, D. A. (2021). BigTech and Platform Finance: Governing FinTech 4.0 for Sustainable Development. Available at SSRN. <https://doi.org/10.2139/ssrn.3915275>
- Azzone G. (2018) Big data and public policies: Opportunities and challenges. *Statistics & Probability Letters*, 136. 116–120.
- Baba, C., Batog, C., Flores, E., Gracia, B., Karpowicz, I., Kopyrski, P., Roaf, J., Shabunina, A., Elkan, R. van & Xu, X. C. (2020), Fintech in Europe: Promises and Threats, *IMF Working Paper* No. 20/241, Available at SSRN: <https://ssrn.com/abstract=3758074> or <https://doi.org/10.2139/ssrn.3758074>
- Bhardwaj, A., & Goundar, S. (2019). A framework to define the relationship between cyber security and cloud performance. *Computer Fraud & Security*, 2019(2), 12–19.
- Boot, A., Hoffmann, P., Laeven, L., & Ratnovski, L. (2021). Fintech: what's old, what's new?. *Journal of financial stability*, 53, 100836. <https://doi.org/10.1016/j.jfs.2020.100836>

- Bygrave, L. A. (2014). *Data Privacy Law: An international Perspective*. Oxford University Press.
- Chatzara V. (2020) *FinTech, InsurTech, and the Regulators*. In: Marano P., Noussia K. (Eds.) *InsurTech: A Legal and Regulatory View. AIDA Europe Research Series on Insurance Law and Regulation*, vol 1. Springer, Cham. https://doi.org/10.1007/978-3-030-27386-6_1
- Chauhan A., Rishabh, Shankar L.N., Mittal P. (2022) *A Deep Dive into Blockchain Consensus Protocols*. In: Zhang YD., Senjyu T., So-In C., Joshi A. (Eds.) *Smart Trends in Computing and Communications*. Lecture Notes in Networks and Systems, vol 286. Springer, Singapore. https://doi.org/10.1007/978-981-16-4016-2_54
- China Fines Alibaba \$2.8 Billion in Landmark Antitrust Case (2021), Retrieved from <https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html>
- Chirita, A. D. (2018). The rise of big data and the loss of privacy. In Bakhom, M., Gallego, B. C., Mackenrodt, M. O., & Surblytė-Namavičienė, G. (Eds.). *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (pp. 153–189). Springer, Berlin, Heidelberg.
- Data Protection Around the World: Future Challenges (2020). Cortez, E. K. (Ed.). *Data Protection Around the World: Privacy Laws in Action* (Vol. 33). Springer Nature.
- Dorfleitner, G., Hornuf, L. & Kreppmeier, J. (2021) Promise Not Fulfilled: FinTech, Data Privacy, and the GDPR, *CESifo Working Paper* No. 9359, Available at SSRN: <https://ssrn.com/abstract=3950094> or <https://doi.org/10.2139/ssrn.3950094>
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, 32(5), 1798–1853.
- Frolova, E. E., Ermakova, E. P., & Protopopova, O. V. (2020, March). Consumer protection of digital financial services in Russia and abroad. In *13th International Scientific and Practical Conference-Artificial Intelligence Anthropogenic Nature Vs. Social Origin* (pp. 76–87). Springer, Cham.
- Gai, K., Qiu, M., & Sun, X. (2018). A survey on FinTech. *Journal of Network and Computer Applications*, 103, 262–273.
- Geranio, M. (2017). Fintech in the exchange industry: Potential for disruption?. *Masaryk University Journal of Law and Technology*, 11(2), 245–266.
- Google dominates search. But the real problem is its monopoly on data (2015), Retrieved from <https://www.theguardian.com/technology/2015/apr/19/google-dominates-search-real-problem-monopoly-data>
- Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research*, 97, 235–256.

- Herian, R. (2021). *Data: New Trajectories in Law* (1st ed.). Routledge. <https://doi.org/10.4324/9781003162001>
- Hernández, E., Öztürk, M., Sittón, I., & Rodríguez, S. (2019, June). Data Protection on Fintech Platforms. In *International Conference on Practical Applications of Agents and Multi-Agent Systems* (pp. 223–233). Springer, Cham.
- Houser, K. A., & Voss, W. G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy. *Rich. JL & Tech.*, 25, 1.
- Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press. Available at: <https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491>.
- Lundqvist, B. (2018). Big data, open data, privacy regulations, intellectual property and competition law in an internet-of-things world: The issue of accessing data. In *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (pp. 191–214). Springer, Berlin, Heidelberg.
- Mehrban S. et al. (2020), Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges, in *IEEE Access*, vol. 8, pp. 23391–23406, <https://doi.org/10.1109/ACCESS.2020.2970430>.
- Miglionico, A. (2019) Artificial intelligence and automation in financial services: the case of Russian banking sector. In *Law and Economics Yearly Review* 8 (1): 125–147.
- Moura V. D. and de Vasconcelos Casimiro S. (2020) in Vicente, D. M., & de Vasconcelos Casimiro, S. (Eds.). *Data Protection in the Internet*. Springer. <https://doi.org/10.1007/978-3-030-28049-9>
- Pittman P. & Levenberg K. (2021) *USA: Data protection Laws and Regulations 2021*. Retrieved from <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>
- Quinn, P. (2021). The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal*, 22(8), 1583–1612.
- Rodríguez, S. (2019, June). Data Protection on Fintech Platforms. In *Highlights of Practical Applications of Survivable Agents and Multi-Agent Systems. The PAAMS Collection: International Workshops of PAAMS 2019, Ávila, Spain, June 26–28, 2019, Proceedings* (Vol. 1047, p. 223). Springer.
- Soloviev, V. I. (2018). Fintech ecosystem and landscape in Russia. *Journal of Reviews on Global Economics*, 7, 377–390.
- Svantesson, D. J. B. (2011). The regulation of cross-border data flows. *International Data Privacy Law*, 1(3), 180–198.
- Sydekum, R. (2018). Can consumers bank on financial services being secure with GDPR?. *Computer Fraud & Security*, 6, 11–13.

- Vedaschi A & Lubello V., (2015) Data Retention and Its Implications for the Fundamental Right to Privacy: a European Perspective, *Tilburg Law Review* 20, 14 <https://doi.org/10.1163/22112596-02001005>
- Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676), 10–5555.
- Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 9(2), 43–66.
- Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature. <https://doi.org/10.1007/978-981-13-8110-2>
- Yang, X. (2021, April). Regulatory Approaches of Cross-border Data Flow in the Big Data Era: China's Choice. In *Journal of Physics: Conference Series*, Vol. 1848, No. 1, p. 012026. IOP Publishing.



Financial Crimes in the Age of the Digital Economy and FinTech

Eva Huang, Xi Nan, and Jun Zhao

INTRODUCTION

FinTech, as an emerging industry, is a significant component of the digital economy, its business model overlaps with the banking business model. The digitalisation of banks themselves means banks also carry on FinTech businesses. In this context, many financial crimes have also been digitalised.

This chapter aims to analyse financial crimes in the age of the digital economy and FinTech, briefly explaining different types of financial crimes, such as money laundering, tax evasion, financial fraud or

E. Huang (✉) · X. Nan · J. Zhao
University of Sydney Business School, Darlington, NSW, Australia
e-mail: eva.huang@sydney.edu.au

X. Nan
e-mail: xi.nan@sydney.edu.au

J. Zhao
e-mail: jzha6973@uni.sydney.edu.au

dishonesty, cybercrime in finance, terrorist financing, bribery, and corruption. More specifically, this chapter provides an illustrative scenario of the detection of financial crimes through the detection of cross-border transaction-based tax evasion on social media platforms.

DEFINITION OF FINANCIAL CRIME

Financial crimes consist of a wide range of activities, from fraud to actively manipulating the stock market or laundering the proceeds of crime. From two perspectives, financial crimes are attractive propositions for both organised and serious crime. Firstly, organised and serious crimes are always looking for exploitable loopholes, and fraud and market manipulation offer attractive opportunities for a quick financial return. Secondly, just as legitimate business needs access to the financial system, so does organised crime. Criminals aim to conceal either the criminal source of their financial flows, or the criminal purposes of their funds.¹

TYPES OF FINANCIAL CRIMES

Financial crime refers to any kind of criminal conduct that relates to money or to financial services or markets, it is commonly considered as covering the following offences:

- a. Financial fraud or dishonesty; or
- b. Cybercrime in finance and cyber security; or
- c. terrorist financing; or
- d. bribery and corruption; or
- e. market abuse and insider trading, etc.
- f. money laundering; or
- g. Tax Evasion.²

¹ David Chaikin (2022), CLAW6031 INTERNATIONAL FINANCIAL CRIME TEXTBOOK, University of Sydney School of Business.

² <https://www.int-comp.org/careers/your-career-in-financial-crime-prevention/what-is-financial-crime/>.

Financial Fraud

Although the elements of fraud are worded differently in different pieces of legislation, their substance commonly include:

- Acting dishonestly;
- The obtaining of property, gaining a financial advantage, or causing a financial disadvantage; and
- In fact, this occurred by a deception.³

Financial fraud is a type of theft that occurs when a person or entity takes or illegally uses money or property with profit-making intent. These crimes commonly involve some form of subterfuge, deceit, or the abuse of a position of trust, which distinguishes them from ordinary theft or robbery. In the modern age, financial frauds can take many forms, including digital forms.⁴

Cybercrime in Finance

Cybercrime in the financial sector is the act of obtaining financial gain through profit-driven criminal activities, including email and internet fraud, identity fraud, ransomware attacks, and attempts to steal financial account, bank card or other digital payment information.⁵ Cybercrime in finance includes acts such as obtaining financial accounts to initiate unauthorised transactions, stealing payment card information, extortion, identity fraud to apply for financial products, and more.⁶

As society increasingly relies on technology, the risk of data leakage increases. Sensitive information such as the identity number, bank account information, and credit card details are now stored in cloud storage devices such as Apple (iCloud),⁷ Amazon (Amazon Web Services),⁸

³ [https://uk.practicallaw.thomsonreuters.com/w-009-8659?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-009-8659?transitionType=Default&contextData=(sc.Default)&firstPage=true).

⁴ <https://www.findlaw.com/criminal/criminal-charges/fraud-financial-crimes.html>.

⁵ <https://gsdec.network/cybersecurity-and-financial-crimes/>.

⁶ Ibid.

⁷ <https://www.icloud.com/>.

⁸ <https://aws.amazon.com/>.

Google Drive,⁹ Dropbox,¹⁰ Baidu Cloud,¹¹ or specialised financial services clouds such as UnionPay Cloud,¹² which may harm an individual's financial health. Financial cybercrime can affect individuals, companies, and industries of all sizes, and can have dramatic consequences.

Terrorist Financing

Terrorist financing is any form of financial support for terrorism or for those who encourage, plan, or participate in terrorism. It usually falls into two categories:

- financing direct costs associated with the perpetration of terrorist acts, such as expenses for travel, explosive materials, weapons, and vehicles,
- funds needed to maintain terrorist organisations, cells, or networks.¹³

The process of terrorist financing generally consists of three stages:

- “Raising funds (such as through donations, self-funding, or criminal activity)
- Transferring funds (to organisations, cells, or networks)
- Use of funds (for example, to buy weapons or bomb-making equipment, to pay insurgents, or to pay for the living expenses for terrorist groups).”¹⁴

Funds are also required to be stored at each stage of the terrorist financing process. Storage can be by stashing cash in a private residence

⁹ https://www.google.com/intl/en_au/drive/.

¹⁰ <https://www.dropbox.com/>.

¹¹ <https://pan.baidu.com/pcloud/home>.

¹² <https://www.unionpayintl.com/>.

¹³ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014>.

¹⁴ Ibid.

or in a cash box, or by depositing funds in a bank account or other financial products. In the digital economy, digital assets or crypto-assets could also be utilised.¹⁵

In all terrorist financing cases, these stages may not be present or clear. To fund larger terrorist organisations, funds may be moved through different layers of the network’s structure—for instance, from an American cell which raised funds, to a governing branch of a terrorist group overseas, and then on to a local cell in a foreign country. Simpler cases may be an American citizen directly funding an overseas insurgent or their domestic activities.

Terrorist financing funds are considered “criminal instruments”, meaning either illicit or legitimate funds are used for criminal purposes. In this way, funds used to finance terrorism are similar to funds used to commit most other crimes (for instance, paying people smugglers). The three-stage process discussed above can also describe the illicit financial flows involved in other types of financial crimes.¹⁶

Bribery and Corruption

Bribery and corruption have historically been considered as a contributing factor to certain types of financial and organised crimes, such as through bribes to law enforcement agencies or undue influence on decision-making. Modern forms of corruption, however, have often been explained as transnational in nature, are more intertwined with financial crime.¹⁷ Both types of crimes have similar drivers, relying on similar mechanisms to divert and launder illicit financial flows, and deprive societies of much-needed financial resources. They threaten not only the social and economic stability of other countries around the globe, but also the rule of law and democracy.¹⁸

¹⁵ https://www.fatf-gafi.org/media/fatf/documents/bulletin/FATF-Booklet_VA.pdf.

¹⁶ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014>.

¹⁷ See https://knowledgehub.transparency.org/assets/uploads/kproducts/2021-Corruption-and-economic-crime_final.pdf; https://www.refinitiv.com/content/dam/market-ing/en_us/documents/reports/true-cost-of-financial-crime-global-focus.pdf; <https://www.austrac.gov.au/sites/default/files/2019-06/sa-brief-peps.pdf>.

¹⁸ https://knowledgehub.transparency.org/assets/uploads/kproducts/2021-Corruption-and-economic-crime_final.pdf.

Transparency in political funding may also ensure that political and electoral campaigns are not tainted by proceeds of corruption and economic crime and could help prevent the capture of state institutions. Certain tools for combating bribery and corruption can be more effectively coordinated because of these common features.¹⁹ For example, a public register of beneficial ownership might prevent the use of shell companies for laundering the proceeds of corruption and financial crimes. In addition, international cooperation is required in the investigation and prosecution of corruption and financial crime schemes and in the recovery of assets. Transparency in political funding also ensures that political and electoral activities are not influenced by the proceeds of bribery and corruption, in order to help prevent the capture of state institutions.²⁰

In November 2021, the OECD Anti-Bribery Convention established legally binding standards to criminalise bribery of foreign public officials in international business transactions and set out a range of measures to bring them into force. It is the first and only international anti-corruption instrument focusing on the “supply side” of the bribery transactions. The 2021 Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions complements the Anti-Bribery Convention with a view to further strengthening and supporting its implementation.²¹

Market Abuse and Insider Trading

The concept of market abuse often includes insider trading, illegal disclosure of inside information, and market manipulation. More specifically, insider trading involves profiting from dealing in securities through the intentional exploitation of confidential information obtained through a privileged relationship or position within the entity.²² Stewart and

¹⁹ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/terrorism-financing-australia-2014>.

²⁰ Ibid.

²¹ <https://www.oecd.org/daf/anti-bribery/2021-oecd-anti-bribery-recommendation.htm>.

²² <https://www.pwc.com/mt/en/services/regulatory-and-financial-crime-consulting/market-abuse-and-insider-dealing.html>.

ImClone's case²³ is a type of market abuse and insider trading example for illustrative purposes.

In December 2001, the U.S. Food and Drug Administration (FDA) announced that it would not approve a new cancer drug called Erbitux made by the company ImClone Pharmaceuticals. With the drug expected to be approved, it represented a major portion of ImClone's future growth plans. As a result, the company's stock price fell rapidly. While many investors suffered losses from the fall, the family and friends of Erbitux CEO Samuel Waksal were not hurt. The U.S. Securities and Exchange Commission later found that before the FDA announced its decision, numerous executives had sold their stock at the direction of Waksal, who had also attempted to sell his own stock.²⁴

In fact, just days before the announcement, U.S. retailer Martha Stewart had sold about 4,000 shares of the company. At this point, the stock was still trading at a high level, with Stewart making nearly \$250,000 on the trade. Over the next few months, the stock plummeted from about \$60 to just over \$10.²⁵

Stewart claimed to have a pre-existing sales order with her broker, but it was later discovered that the broker, Peter Bacanovic, tipped her off that the stock of ImClone was likely going to fall. Stewart eventually resigned as the CEO of her own company, Martha Stewart Living Omnimedia. Waksal was arrested and sentenced to more than seven years in prison and fined \$4.3 million in 2003. In 2004, Stewart and her broker were also convicted of insider trading. Stewart was sentenced to a minimum of five months in prison and a \$30,000 fine.²⁶

Illicit Financial Flows

Different types of financial crimes share one common characteristic, that is, financial crimes are always associated with illicit financial flows. Illicit financial flows refer to the cross-border movement of funds that is illicit in its source (for example, corruption and smuggling), its transfer (for example, tax evasion), or its use (for example, terrorist financing). These financial flows have been a growing global focus over the past

²³ UNITED STATES v. STEWART.

²⁴ <https://www.investopedia.com/articles/stocks/09/insider-trading.asp>.

²⁵ Ibid.

²⁶ Ibid.

two decades, and the International Monetary Fund (IMF) has played a key role in international efforts to combat these opaque and often destabilising capital transfers.²⁷

The IMF has also long been concerned with financial flows that, while not strictly illegal, are linked with tax avoidance caused by aggressive tax planning.²⁸ The issue of illicit financial flows is at the top of the international agenda. Governments around the world are joining forces to fight tax evasion and money laundering, which make up the bulk of illicit financial flows.²⁹

Money Laundering

The Financial Action Task Force (FATF) has defined money laundering as.

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.³⁰

When criminal activities produce substantial profits, involved parties always find ways to control the funds without drawing attention to the underlying activity or the people involved. Criminals do this by obfuscating the sources, altering the form, or moving the funds to places where they are less likely to attract attention.

The Financial Action Taskforce's Role in Anti-Money Laundering & Counter-Terrorist Financing (CTF)

Illicit arms sales, smuggling, and organised crime activities, such as drug trafficking and prostitution rings, can produce huge profits. Embezzlement, insider trading, computer fraud schemes and bribery can also

²⁷ <https://www.imf.org/en/About/Factsheets/Sheets/2018/10/07/imf-and-the-fight-against-illicit-financial-flows>.

²⁸ Ibid.

²⁹ https://www.oecd.org/corruption/Illicit_Financial_Flows_from_Developing_Countries.pdf.

³⁰ <https://www.fatf-gafi.org/faq/moneylaundering/>.

generate large profits and create an incentive to “legitimise” illicit gains through money laundering.

To respond to growing concerns about money laundering and terrorist financing, the Financial Action Task Force (FATF) on money laundering was established by the G-7 Summit in Paris in 1989 to develop a coordinated international response. The FATF currently consists of 37 member jurisdictions and 2 regional organisations, representing most of the world’s major financial centres.³¹ There are 8 FATF-style regional associate members, such as Asia/Pacific Group on Money Laundering (APG), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), and Financial Action Task Force of Latin America (GAFILAT). The United States, Australia, India, and China are members of both FATF and APG.

One of the FATF’s first tasks was to develop a total of 40 recommendations that set out the measures national governments should adopt to implement effective anti-money-laundering programmes.³² The FATF Recommendations cover criminal justice system & law enforcement, financial system & regulation, and international cooperation.

Other than FATF recommendations, FATF Standards also consist of methodologies to assess the effectiveness of the Anti-Money Laundering (AML)/Counter-Terrorist Financing (CTF) systems, and procedures for the Fourth Round of AML/CTF evaluations.³³

Essence and Stages of Money Laundering

Based on FATF’s definition, money laundering is a crime of deception, and it refers to the “process whereby criminals attempt to disguise and legitimate their ill-gotten gains of crime”.³⁴ The essence of money laundering is to disguise the true nature, source, movement, or ownership of property or funds, with the aim to legitimate assets by pretending that property or funds come from a legal source (for example investment), but in reality property or funds come from an illegal source (for example

³¹ <https://www.fatf-gafi.org/about/membersandobservers/>.

³² <https://www.fatf-gafi.org/faq/moneylaundering/>.

³³ Ibid.

³⁴ <https://www.fatf-gafi.org/faq/moneylaundering/>.

drug trafficking).³⁵ In short, there is always an underlying crime where property or funds come from, and the reason for laundering illegal money is to avoid the detection, not to make money.

There are three common stages used to disguise the source of illicit income and make it usable in money laundering activities:

- Placement: Money is introduced into the financial system, commonly by dividing it into various deposits and investments.
- Layering: Money is transferred to generate distance between it and perpetrators.
- Integration: Money is then returned to perpetrators as clean funds or legitimate income.³⁶

Money launderers often adopt methods to avoid detection and conceal the true source of funds. Some of the most commonly used methods are outlined below.

Smurfs

Not in any way related to the children's cartoon, the term "Smurf" is used to describe a money launderer who wants to evade government scrutiny. They hide funds by using placement, layering, and integration stages. Large amounts of funds are deposited into different banks in smaller transactions.³⁷

It is required that financial institutions report large deposits of more than \$10,000 or what they deem suspicious to financial regulators and authorities. By depositing small amounts of funds or smurfing, money launderers can go under the radar and make the funds they deposit appear to be of legitimate origin.³⁸

³⁵ Ibid.

³⁶ David Chaikin (2022), CLAW6031 INTERNATIONAL FINANCIAL CRIME TEXTBOOK, University of Sydney School of Business.

³⁷ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/cuckoo-smurfing#:~:text=Organised%20criminals%20use%20'cuckoo%20smurfing,expecting%20to%20receive%20legitimate%20funds.>

³⁸ [https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp.](https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp)

Mules

A mule is an individual hired by money launderers to help run money laundering schemes. Money mules are similar to drug mules, they may be involved in the scheme, or they may be unknowingly recruited. Those who are hired are often approached by money launderers and often have no knowledge of the scheme. They may be attracted to the promised jobs that pay good rewards. Criminals usually target individuals who are out of the spotlight, including those without criminal records or financially vulnerable.

One of the duties of a mule is to open a bank account and deposit funds in the bank. Money launderers then start making wire transfers and use currency exchanges to move funds around the financial system to evade further detection.³⁹

Shells

Shell or Shell corporations means a company that does not have any business activities or operations, physical operations, assets, or employees. Many shell corporations are legitimate business entities that are used to raise capital, finance the operations of start-ups, or manage mergers and acquisitions.⁴⁰

Other cases may also involve fraudsters making shells who wanted to hide illegal activity and/or evade taxes. Many individuals do this by setting up shell companies in a jurisdiction that guarantee anonymity, allowing them to deposit and transfer funds into different accounts. Shell also allows taxpayers to avoid reporting income and fulfilling their tax obligations.

Legal Analysis of the Crime of Money Laundering

This chapter outlines the crime of money laundering in common law and civil law countries, using Australia and China as examples, respectively.

The Crime of Money Laundering—In Common Law Countries: Australia as an Example

³⁹ <https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp>.

⁴⁰ https://www.fincen.gov/sites/default/files/shared/LLCAssessment_FINAL.pdf.

According to the *Criminal Code Act 1995* (Cth) (the *Act*), a crime consists of “physical elements” and “fault elements (also known as mental elements)”.⁴¹ Proof of the commission of a Commonwealth offence now requires proof of the “physical elements” of the crime associated with the “fault elements” applicable for each physical element. Unless an offence falls into the unusual strict liability offence category, the prosecution must show that both elements exist to prove that a person has committed the crime.⁴²

Physical elements under the *Act* may be either:

- “a. conduct (defined as an act, an omission to perform an act or a state of affairs);
- b. a result of conduct; and
- c. a circumstance in which conduct, or a result of conduct, occurs.”⁴³

Fault elements under the *Act* may be:

- “a. intention;⁴⁴
- b. knowledge;⁴⁵
- c. recklessness;⁴⁶ and
- d. negligence.”⁴⁷

⁴¹ *Criminal Code Act 1995*.

⁴² “Commonwealth Code – Proof of Physical and Mental Elements of An Offence”, *Courts.qld.gov.au* (Webpage, 2017), https://www.courts.qld.gov.au/__data/assets/pdf_file/0004/85468/sd-bb-197-proof-of-mental-and-physical-elements-commonwealth-offences.pdf.

⁴³ *Ibid.*

⁴⁴ Above n44, Section 5.2.

⁴⁵ Above n44, Section 5.3.

⁴⁶ Above n44, Section 5.4.

⁴⁷ Above n44, Section 5.5.

The fault element is also known as *mens rea* in Latin. The literal translation of the term “*mens rea*” is “guilty mind”,⁴⁸ which refers to criminal intent. In criminal trials, establishing the guilty mind of an offender is a necessary element to prove guilt. The prosecution must prove beyond a reasonable doubt that the defendant committed the crime with a culpable state of mind.⁴⁹ According to a famous explanation of the concept by Justice Holmes, “even a dog knows the difference between being stumbled over and being kicked”.⁵⁰

The guilty mind requirement is premised upon the idea that a person must possess a guilty state of mind and be aware of their misconduct; however, the defendant is not required to know that their conduct is illegal to constitute a crime. On the contrary, the defendant must be aware of the facts that make their conduct fit the definition of a crime.

For example, if a person deliberately strikes another person without a legitimate reason (such as self-defence) without that person’s consent, it constitutes an assault. The prohibited conduct is the striking (physical element) and the fault element, or guilty mind, is the intention to hurt/injure/attack/strike. On the other hand, if one person accidentally strikes another person, a criminal offence will not occur since the fault element does not exist.

To use the Australian law on AML/CTF as an example, there are many (19) different money laundering offences in the *Criminal Code Act 1995*.⁵¹ According to Sections 400.3–400.8 of the *Act*, 18 of the 19 offences may be classified by the state of mind of the defendant, and the amount of money involved where the defendant deals with “money or property that is the proceeds of crime or is an instrument of crime”.⁵²

⁴⁸ “Mens Rea - A Defendant’s Mental State - Findlaw”, *Findlaw* (Webpage, 2019), <https://criminal.findlaw.com/criminal-law-basics/mens-rea-a-defendant-s-mental-state.html>.

⁴⁹ “Supreme and District Court Benchbook—Proof of Mental and Physical Elements Commonwealth”, *Courts.qld.gov.au* (Webpage, 2017), https://www.courts.qld.gov.au/_data/assets/pdf_file/0004/85468/sd-bb-197-proof-of-mental-and-physical-elements-commonwealth-offences.pdf.

⁵⁰ “Even A Dog Distinguishes between Being Stumbled over and Being Kicked.”, *WBEZ Chicago* (Webpage, 2018), <https://www.wbez.org/stories/even-a-dog-distinguishes-between-being-stumbled-over-and-being-kicked/cda0cb26-62f2-4ff1-8160-0515760afcb>.

⁵¹ Above n44.

⁵² Above n44.

In other words, to prove the money laundering, prosecution must prove state of mind (fault elements) and conduct of the accused (physical elements). When the defendant believes the money or property is proceeds of crime or intends that money or property will become an instrument of crime, the fault element of intentional money laundering can be proved. If the proceeds reach \$1 million, the defendant will be sentenced to up to 25 years in prison. When the defendant is reckless of the money laundering fact, if the proceeds reach \$1 million, the defendant will be sentenced to up to 12 years in prison. When the defendant is negligent of the money laundering fact, if the proceeds reach \$1 million, the defendant will be sentenced to up to 5 years in prison.⁵³

Section 400.9 covered the scenario that “possession of property reasonably suspected of being proceeds of crime”.⁵⁴

The Crime of Money Laundering—In Civil Law Countries: China as an Example

China has identified money laundering as one type of crime with very specific predicate crimes.

According to Article 191 of the *Criminal Law of the People’s Republic of China*,

“Whoever, while clearly knowing that the funds are proceeds illegally obtained from drug-related crimes or from crimes committed by mafias or smugglers and gains derived therefrom, commits any of the following acts in order to cover up or conceal the source or nature of the funds shall, in addition to being confiscated of the said proceeds and gains, be sentenced to fixed-term imprisonment of not more than five years or criminal detention and shall also, or shall only, be fined not less than five percent but not more than 20 percent of the amount of money laundered; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than five but not more than 10 years and shall also be fined not less than five percent but not more than 20 percent of the amount of money laundered:

- (1) providing fund accounts;
- (2) helping exchange property into cash or any financial negotiable instruments;

⁵³ Above n45.

⁵⁴ Above n45.

- (3) helping transfer capital through transferring accounts or any other form of settlement;
- (4) helping remit funds to any other country; or
- (5) covering up or concealing by any other means the nature or source of the illegally obtained proceeds and the gains derived therefrom.

Where a unit commits any of the crimes mentioned in the preceding paragraph, it shall be fined, and the persons who are directly in charge and the other persons who are directly responsible for the crime shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention.”⁵⁵

In June 2021, the People’s Bank of China released the draft version of amended Anti-Money Laundering (AML) Law for public comment. The Amended AML Law contains significant changes to improve the effectiveness of its legal framework for combating money laundering and terrorist financing and has expanded AML obligations to all individuals and organisations.⁵⁶

Money Laundering in the Digital Age

In the digital age, money launderers always find modern ways of money laundering, putting a new spin on the old crime by utilising the internet to evade detection.

A key factor in money laundering is being closely watched. The use of the Internet makes it easy for money launderers to avoid detection. The rise of online banking institutions, anonymous online payment services, peer-to-peer transfers using mobile phones, and the use of virtual currencies such as Bitcoin and Ethereum have made it increasingly difficult to detect illicit fund transfers.

Some examples are listed below to explain how technology can further help money laundering activities⁵⁷:

⁵⁵《中华人民共和国刑法》 *Criminal Law of the People’s Republic of China* 2017 (Standing Committee of the National People’s Congress). Article 191.

⁵⁶ https://www.garrigues.com/en_GB/new/china-amend-its-anti-money-laundering-law#:~:text=The%20Amended%20AML%20Law%20also,freeze%20or%20transfer%20onshore%20assets.

⁵⁷ [https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp.](https://www.investopedia.com/ask/answers/022015/what-methods-are-used-launder-money.asp)

- The use of proxy servers and anonymizers. These tools make integration nearly impossible to detect, as funds can be transferred or withdrawn with little or no trace of an IP address.
- Funds can be laundered through online auctions and sales, gambling websites, and even virtual gaming sites. Ill-gotten gains are converted into the currency used on these sites, and then transferred back into real, usable, and untraceable clean money.
- Advertise phishing scams targeting victims' bank accounts. Fraudsters defraud victims under the pretext of depositing virtual lottery wins or international legacies. Instead, they put multiple deposits into the account and stipulate that some of the money must be transferred to another account.⁵⁸

Compliance Risks for Banks and FinTech Companies

Illicit financial flows will result in different types of compliance risks to banks and FinTech companies, where they are required to take measures to improve compliance. Enhanced due diligence, suspicious matter reporting, and managing risks of tipping-off offences are three measures to manage compliance risks.⁵⁹

Enhanced Due Diligence

Due diligence is the investigation or exercise of care that a reasonable business or individual would normally expect to take before signing a contract or an agreement with another party or acting with a certain standard of care. Customer due diligence (CDD) is an important and complex area in the world of Financial Crime Compliance (FCC). Customer due diligence is the processes used by financial institutions to collect and evaluate relevant information about customers or potential customers.⁶⁰

Enhanced Due Diligence (EDD) refers to an advanced Know Your Customer (KYC) due diligence process that provides further risk investigation. EDD is designed to handle high-risk clients and large-value

⁵⁸ Ibid.

⁵⁹ David Chaikin (2022), CLAW6031 INTERNATIONAL FINANCIAL CRIME TEXTBOOK, University of Sydney School of Business.

⁶⁰ <https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd#:~:text=In%20the%20world%20of%20Financial,a%20customer%20or%20potential%20customer.>

transactions. Risky customers and transactions pose a greater risk to the financial sector that cannot be detected by CDD procedures. In this case, EDD procedures have been adopted to attempt to create a higher assurance of identity by taking the customer's identity and addressing and assessing the customer's risk category. Additionally, when there is an increased opportunity from money laundering, terrorist financing through the service and product or customer may present a high-risk situation; therefore, these procedures are required to mitigate the increased risk.⁶¹ In the digital age, KYC and EDD can be automated through digital technology.

Some types of higher risk customers are listed:

- “Politically Exposed Persons (PEPs)
- Non-resident customers e.g., foreign students
- Accounts opened by intermediaries e.g., lawyer's trust account
- Holding assets on behalf of other persons e.g., trustees
- Cash-intensive businesses e.g., casinos
- Difficulty in identifying beneficial owner of account e.g., nominee shareholdings
- Complex or unusual ownership structure of customer”⁶²

Suspicious Matter Reports

In Australia, the Australian Transaction Reports and Analysis Centre (AUSTRAC) defines suspicious matter reports (SMR) as,

a report a reporting entity must submit under Anti-Money Laundering and Counter-Terrorism Financing Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law.⁶³

⁶¹ <https://sanctionsscanner.com/knowledge-base/enhanced-due-diligence-edd-123>.

⁶² David Chaikin (2022), CLAW6031 INTERNATIONAL FINANCIAL CRIME TEXTBOOK, University of Sydney School of Business.

⁶³ <https://www.austrac.gov.au/glossary/suspicious-matter-report-smr#:~:text=A%20report%20a%20reporting%20entity,serious%20crimes%20under%20Australian%20law>.

The police rely on financial transaction information to track criminals and criminal activity. The timeliness of suspicious matter reports is critical to protecting Australians from serious crime and terrorism.

It is required to submit an SMR to AUSTRAC:

- within 24 hours if the suspicion is related to terrorism financing
- within 3 business days if the suspicion is related to other matters such as money laundering⁶⁴

The Offence of Tipping-Off

The offence of tipping-off is committed when a person knows or suspects (subjectively) that a protected or authorised disclosure has been made and makes a disclosure to a third party (the client) that is likely to prejudice any investigation which either is or might be conducted.⁶⁵

In Australia, penalties for tipping off can include up to two years in prison and/or a fine of up to 120 penalty units.⁶⁶

In the digital economy, these three compliance risks are more complicated, where digitalisation of the exchange of information, as well as the nature of the Internet, means that there are unexpected consequences arising from automation. These consequences could be social, ethical, or environmental in nature. Little research has been done in relation to these consequences due to the difficulties in detection of relevant crimes and associated risks. The following section illustrates the feasibility of detection through an analysis of the detection of tax evasion as a financial crime.

⁶⁴ <https://www.austrac.gov.au/business/how-comply-guidance-and-resources/reporting/suspicious-matter-reports-smr>.

⁶⁵ https://www.hkicpa.org.hk/-/media/HKICPA-Website/HKICPA/section5_membership/Professional-Representation/AMLB1.pdf.

⁶⁶ <https://www.austrac.gov.au/sites/default/files/2021-06/Quick%20guide%20-%20Tipping%20off.pdf>.

Tax Evasion

Tax evasion refers to the deliberate non-payment of taxes by individuals and entities. Tax evasion often means that taxpayers intentionally misrepresent the true state of their affairs to tax authorities to reduce their tax payables. It also includes false tax declaration, where the income, profits, or gains declared by those tax evaders are lower than the amount earned, or the deductions are over claimed.⁶⁷ Clotfelter's definition of tax evasion has been well-accepted, and he stated that.

Tax evasion can be defined as any criminal activity or any offence of dishonesty punishable by civil penalties that is intended to reduce the taxation incidence, and depends on economic and tax structures, types of income, and social attitudes. The basic theoretical model of tax evasion is a straightforward application of individual choice under uncertainty and the problem an individual faces is whether or not to evade some part of his legal tax liability, given that there is some probability of being caught if he decides to evade.⁶⁸

Based on these concepts of tax evasion, it can be considered that tax evasion usually exists in the following situations: by concealing all or part of the taxable revenue or transactions which have already occurred, such as destroying or concealing an accounting record, preparing false accounting related documents and statements (for example, overstating revenue, failing to record expenses, and misstating assets and liabilities are all ways to commit accounting fraud), not issuing a tax invoice, receipts or tax-related bills, etc., and accompanied by fraudulent declarations, dishonest declarations or omissions of declarations, taxpayers fail to pay or pay less tax than they should have paid.⁶⁹

Tax evasion directly violates taxation and criminal laws, and this violation is mainly reflected in the use of the methods mentioned above to

⁶⁷ "Fraud or Evasion Guideline (Period of Review)", *Ato.gov.au* (Webpage, 2018), [https://www.ato.gov.au/About-ATO/Commitments-and-reporting/In-detail/FOI/Fraud-or-evasion-guideline-\(period-of-review\)/](https://www.ato.gov.au/About-ATO/Commitments-and-reporting/In-detail/FOI/Fraud-or-evasion-guideline-(period-of-review)/).

⁶⁸ Charles Clotfelter, "Tax Evasion and Tax Rates: An Analysis of Individual Returns" (1983) 65(3) *The Review of Economics and Statistics*, 363–365.

⁶⁹ "The Cash and Hidden Economy", *Ato.gov.au* (Webpage, 2019), <https://www.ato.gov.au/general/gen/the-cash-and-hidden-economy/>.

hide the actual taxable amount.⁷⁰ There is no doubt that the use of these methods will make it more difficult for tax authorities to carry out tax administration.

Tax Evasion in the Digital Age

Traditionally, the hidden economy is defined as the economic system in which businesses and individuals do not record or report all their cash income. For tax purposes, traditional hidden economy refers to the economic activity which takes place outside the tax system to avoid tax liabilities. The activities may include cash payments made by consumers which are then not reported as taxable revenue; and cash payments to employees made outside their formal wage structure. These activities are known as the “hidden”, “underground,” “shadow”, “grey”, or “cash” economy. All hidden economy activities have a common feature, that is, they will result in evasion of taxes, leading to governments facing tax revenue loss.

Governments found difficulties in discovering transactions in the hidden economy, and tax evasion arising from hidden economy transactions has been an enduring research topic⁷¹ for scholars of tax administration and tax compliance.

In recent years, the digital economy grew with the development of communications and information technology. Digital economy refers to a series of economic activities that use digital knowledge and information as key factors of production, the modern information network as an important carrier, and information and communication technology as a driving force for efficiency improvement and economic structure optimisation.⁷² As a result of the rapid development of the digital

⁷⁰ “Tax Evasion & Fraud”, *FC Lawyers*, <https://fclawyers.com.au/personal/tax-evasion-fraud/>.

⁷¹ See Matthew Johnston, “How Big is America’s Underground Economy?” *Investopedia* (Webpage, 2019), <https://www.investopedia.com/articles/markets/032916/how-big-underground-economy-america.asp>; Hailin Chen and Friedrich Schneider, “Size and Causes of Shadow Economy in China over 1978–2016: Based on the Currency Demand Method”, *Econ.jku.at* (Webpage, 2018), http://www.econ.jku.at/t3/staff/schneider/papers/Chen_Schneider_2018_Sizeandcausesofshadow.pdf; and Kenneth S Rogoff, *The Curse of Cash: How Large-denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy* (Princeton University Press, 2017).

⁷² See *Mofa.go.jp* (Webpage, 2019), <https://www.mofa.go.jp/files/000185874.pdf>; Rumana Bukht and Richard Heeks, “Defining, Conceptualising and Measuring the Digital

economy, online marketplaces enable consumers to purchase goods globally, and the improvement of consumers' living standards make them no longer satisfied with domestically manufactured products. The volume of cross-border transactions on digital platforms, therefore, continues to grow.⁷³

This chapter uses a detailed Daigou example to illustrate the essence of tax evasion in the digital age, the detection difficulties of such digitalised tax evasion, and a proposed RegTech Tool to achieve detection. For more details, please refer to Eva Huang and Xi Nan, "Transaction-Based Tax Evasion in The Cross-Border Digital Economy: The Case of Daigou Activities on Social Media Platforms" (2020) 26(3) *New Zealand Journal of Taxation Law and Policy*, Lelin Zhang, Xi Nan, Eva Huang, and Sidong Liu "Detecting Transaction-based Tax Evasion Activities on Social Media Platforms Using Multi-modal Deep Neural Networks", accepted to be published on *Digital Image Computing Techniques and Applications Conference Journal*, and Eva Huang and Xi Nan (2021), "Daigou: Cross-Border Digitalised Hidden Economy Transactions Are Now Detectable", *Austaxpolicy: Tax and Transfer Policy Blog*, 6 May 2021.

Daigou Example

Tax administrators around the world are frustrated that they cannot catch cross-border transaction-based tax evasion on digital platforms. Many of these transactions are related to Daigous.

"Daigou" is originally a Chinese term that means three things: a group of people who are buying agents, they buy overseas products outside of China and ship the products to residents in mainland China; the behaviour of acting as buying agents; and an "industry". It now refers broadly to an e-commerce channel between buyers and professional shoppers locating in different countries. Daigou activities can result in criminal offences such as smuggling, tax evasion, and money laundering.

Economy" (Working Paper No.68/Centre for Development Informatics Global Development Institutes, Seed, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431732; and Saudi Arabia, *A Roadmap Toward a Common Framework for Measuring the Digital Economy* (OECD, 2020), <https://www.oecd.org/digital/ieconomy/roadmap-toward-a-common-framework-for-measuring-the-digital-economy.pdf>,5-6.

⁷³ Binglian Liu et al., *Contemporary Logistics in China* (Springer Berlin Heidelberg, 2016).

Daigous have also exploited social media platforms to engage in black-market activities, in effect participating in the digitalised hidden economy. Our research has developed a machine learning strategy that enabled the detection of digitalised hidden economy activities on social media platforms. We explored an example through Instagram. This research will contribute to help address tax evasion arising from these Daigou transactions, which is necessary to detect and eliminate black-market (hidden economy) activities.

How do Daigous conduct transactions? Social e-commerce refers to a business model in which the buying and selling process is completed on social media platforms. This model consists of cross-border and domestic transactions, where sellers take advantage of their extended social networks. Activities include all aspects of e-commerce, from instant messaging to answering customer enquiries to receiving payments via third-party payment methods that are Fintech tools. Here, the social media platform is the primary place to generate business transactions.

There is evidence that Daigou transactions between Australia and China, where Chinese consumers are the final purchasers, are widespread. A 2018 episode of *A Current Affair* addressed the topic of the sizable Daigou industry.⁷⁴ The show revealed that the market size of the global Daigou industry is about AUD\$15 billion. The number of participants in the Daigou industry in Australia is around 200,000 and China is the destination to which most of their purchases are exported.⁷⁵

Daigou and the Hidden Economy

The hidden economy is defined as “those economic activities and the income derived from them that circumvent or otherwise avoid government regulation, taxation or observation.” The predominate platforms on which Daigous engage are social media platforms that are digital payments enabled. Hidden online Daigou transactions share the same characteristics as traditional hidden economy transactions, where merchants prefer to receive anonymous or pseudonymous payments and do not declare the taxable income.

⁷⁴ Michael Vincent, “Like Australia Post on Steroids: Chinese Personal Shoppers Raiding Local Shelves”, *ABC News* (Webpage, 2018), [http://www.abc.net.au/news/2018-04-26/daigou-chinese-personal-shopping-\\$1-billion-industry/9671012](http://www.abc.net.au/news/2018-04-26/daigou-chinese-personal-shopping-$1-billion-industry/9671012).

⁷⁵ *Breaking Borders Exploring the Daigou Opportunity* (Nielsen, 2017), <https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/nielsen-daigou-report-oct17.pdf>.

The rapid development of the Daigou industry may have resulted in serious tax evasion of income tax, and potentially also Goods and Services Tax (GST), in both source and destination countries. For Australia, it has been estimated that “up to \$1 billion in undeclared taxable income may be slipping through the net, leaving a potential tax bill in the hundreds of millions”.

Machine Learning Based Regtech Tool to Achieve Detection

Daigous leave digital footprints in their social media transactions, which enable detection with a suitable data-driven approach. In our recent research paper,⁷⁶ we developed a case study to conduct an experiment on Instagram to search for Daigou transactions. We used #lipstick as the key search word to detect posts which are related to hidden economy activities. We built a design science artefact—a machine learning based Regtech tool for international tax authorities to detect transaction-based tax evasion activities on social media platforms.

To achieve detection, there were three stages in our research:

1. Data mining using Python (a type of high-level programming language);
2. Qualitative manual labelling to develop insights to train the machine;
3. Developing the Regtech tool to detect transaction-based tax evasion activities on Instagram.

To build the dataset, the study employed data trawled from publicly available Instagram posts, including their corresponding poster information. Instagram posts were mined using the hashtag #lipstick in the period from 22 to 26 September 2019.

For each Instagram post, our study collected the username, post timestamp, number of likes, image, post text, and comments. The original post text was included as the first comment due to the way Instagram presents the posts. The study also extracted hashtags from the comments,

⁷⁶ Lelin Zhang, Xi Nan, Eva Huang, and Sidong Liu ‘Detecting Transaction-based Tax Evasion Activities on Social Media Platforms Using Multi-modal Deep Neural Networks’, accepted to be published on *Digital Image Computing Techniques and Applications Conference Journal*.

as these usually form a significant part of the textual information. The study collected a total of 58,660 posts (short-lived and duplicated posts included) and from this data, we produced a dataset of 2,081 randomly sampled unique posts for manual data mining.

Stage Two in our project was the data treatment process to build the training dataset for machine learning purposes. Before labelling, individual posts were examined for the purpose of designing the labelling codes. Nine properties were codified in the form of true or false questions or multiple-choice questions, where the questions can be answered in a form that the machine learning model can understand. This is similar to coding answers to survey questions, but the researcher does not have to ask the questions in the data collection process (Fig. 4.1).

Evidence of Hidden Economy Transactions

Our analysis indicates that 22.21% (464 out of 2081) of the sampled available posts are related to hidden economy transactions and thereby may result in tax evasion (see Fig. 4.2 for an example of the posts). This high proportion suggests that hidden economy transactions on social media platforms have become very common and may lead to significant tax revenue loss. For further labelling results, please refer to our paper.

1. Is the post still available (not being deleted) at time of labelling?
2. Is the post relevant to #lipstick?
3. Judging from the text and image, does the poster have an intention to sell or will the post lead to a potential sale?
4. Judging from the text and image of each post, what is the nature of the poster?
5. Judging from the text and image, is the post related to the hidden economy transactions and thereby resulting in tax evasion?
6. What is the content of the image on the post?
7. What language does the poster write in?
8. Were other contact details left on the post?
9. What are the other contact details left on the post (if any)?

Fig. 4.1 Questions to ask in the data labelling process



(d) A post (<https://www.instagram.com/p/B2snt6tAVsZ/>) relevant to #lipstick, where an unregistered producer is posting advertisement of lipsticks. This post is related to tax evasion activities as the poster is using Instagram to generate unregistered transactions.

Fig. 4.2 A post on Instagram that relates to tax evasion activities

Based on these results, we developed a Regtech tool, which is a multi-modal deep neural network, to automatically detect suspicious posts. The proposed Regtech tool combines comments, hashtags, and image modalities to produce the detection results.

Our model markedly improves the efficiency of detecting and confirming posts that relate to transaction-based tax evasion. Without the detection model, tax officers will need to randomly select the posts, as indicated above. Applying the Regtech tool we develop in our model enables an initial identification of suspicious posts before manual analysis. Tax officers will then manually confirm whether these posts relate to tax evasion.

Figure 4.3 represents the demo results of our Regtech tool, it gives the detection score of an Instagram post to signal its relevance to transaction-based tax evasion activities, considering the comments, hashtags, images, and their combinations within the post. The detection score ranges from 0 to 1, with “1” means the machine regards the post as highly suspicious black-market sales.

Using our model Regtech tool, we can expect to achieve a 72% identification of tax evasion activities based on the algorithmically selected

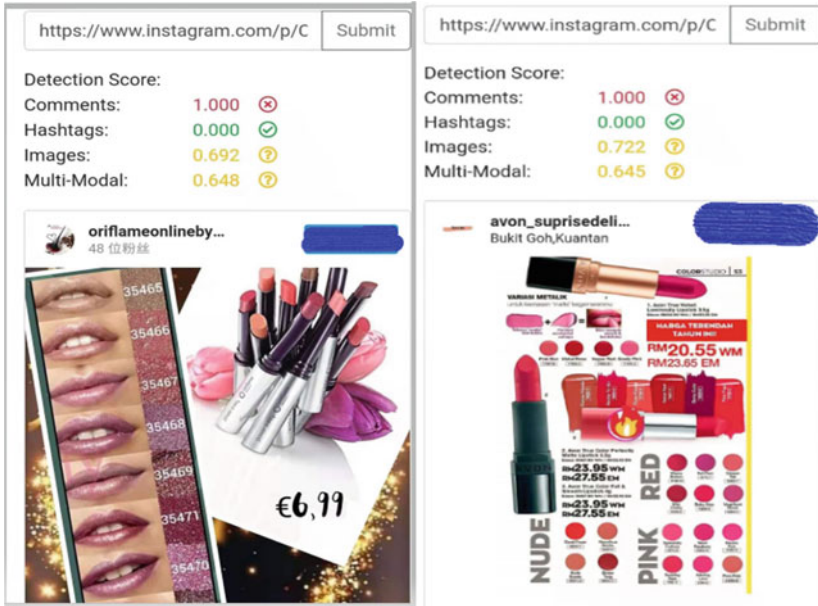


Fig. 4.3 Regtech demo results

suspicious posts. Therefore, with the same amount of effort, the efficiency can be improved by more than 3 times.

CONCLUSION

This chapter explained different types of financial crimes, such as money laundering, tax evasion, financial fraud or dishonesty, cybercrime in finance, terrorist financing, bribery and corruption.

The RegTech tool achieves detection of the financial crime of transaction-based tax evasion on social e-commerce. The financing of these transactions give rise to illicit financial flows, illustrating that similar technology could be adopted to detect illicit financial flows that result from the digitalised version of other international crimes, such as money laundering or terrorist financing. Global regulators are urged to pay attention to adopting digital technologies to assist in the detection of financial

crimes in the digital economy, but care should be taken to consider their unexpected ethical, social, and environmental consequences.

Dr Eva Huang received her PhD from the University of Sydney Business School and she is a lecturer at the University of Sydney Business School. Her research interests include Tax Administration in the Digital Age and Regulation on Alternative Finance. She has published papers in Peer Reviewed Journals, such as New Zealand Journal of Taxation Law and Policy, eJournal of Tax Research, etc.

Dr Xi Nan received her PhD from the University of Sydney Business School. Her research interests include Tax Administration in the Digital Age and Regulating E-commerce Transactions. She has published papers in Peer Reviewed Journals, such as New Zealand Journal of Taxation Law and Policy.

Jun Zhao is a PhD student from the University of Sydney Business School. His research interests include Management Accounting in the Digital Age and Regulating E-commerce Transactions.



Regulatory Innovation in FinTech

Hung-Yi Chen

INTRODUCTION

The financial technology (FinTech) industry has grown rapidly over the last 10 years. On the one hand, the penetration of the internet and widespread adoption of smartphones have made it possible for people to complete transactions easily using mobile applications. On the other, it has been driven by the huge demand for financial services from under-banked or unbanked groups. For example, Ant Group, a subsidiary of Alibaba, has been working in the field of small loans for many years to help SMEs using its e-commerce platform. Moreover, they also leverage the data on user behavior to offer consumer loans in order to encourage online shopping. In addition to the rise of FinTech business models mentioned above, the digital transformation of banks in developed countries and the booming of digital finance in developing ones, such as

H.-Y. Chen (✉)
Meta Intelligence, Kaohsiung, Taiwan
e-mail: hungyi@meta-intelligence.tech

M-Pesa in Africa, are also important factors¹ that have been driving the rapid growth of the industry. However, we will not neglect the relevant risks that accompany the emergence of this new industry. For instance, the Chinese online lending industry, once the largest in the world, has been associated with Ponzi schemes in the past few years that have resulted in millions of investors losing their funds. In the case of Ezubao, the number of victims was hundreds of thousands of people and the amount of money involved topped 500 million RMB. We have also seen numerous hacking incidents in the cryptocurrency exchange industry in Japan. Accordingly, the market mechanism itself is not sufficient to protect consumers. In order to pursue the sustainable development of this new industry, this chapter aims to review the existing theories and academic discussion, as well as to explore potentially better options for FinTech governance.

INTRODUCTION TO FINTECH GOVERNANCE THEORIES

How should the fintech industry be governed? Some scholars have² sought to categorize the attitude of global regulators towards FinTech, including: (1) doing nothing; (2) cautious permissiveness through flexibility and forbearance; (3) restricted experimentation; and (4) regulatory development. First, “doing nothing” refers³ to the practice of the financial regulatory authorities in China prior to 2015. At that time, the FinTech industry was still in its early stages. In order to accelerate the innovation and adoption of financial technologies, regulators tended to wait and see instead of stifling this new industry. Secondly, “cautious permissiveness through flexibility and forbearance” entails offering a friendly regulatory environment under the existing legal framework, such as no-action letters or restricted licenses, so as to provide a certain degree of flexibility for the industry’s development. Furthermore, the “restricted experimentation” refers to the *regulatory sandbox* mechanism. Finally, regulatory development consists of following the legislative process to draft the bills that regulate the industry.

¹ Douglas W. Arner et al., *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 *Northwestern Journal of International Law and Business* 371, 377–80 (2017).

² Dirk A. Zetsche et al., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 *Fordham Journal of Corporate and Financial Law* 31, 35 (2017).

³ *Ibid.* at 44.

With respect to legislative objectives, there are three core dimensions of financial regulation, which include: financial innovation, market integrity, and rule simplicity. It has been pointed out that these three concepts are difficult to achieve⁴ at the same time, at least from the perspective of U.S. financial regulation history. The same study further noted that FinTech has the following three key characteristics: (1) use of a large amount of new data as the basis for FinTech products; (2) use of artificial intelligence and machine learning as the core technology; and (3) the involvement of many non-financial companies, which also leads to the possibility of information asymmetries between regulators and FinTech companies. Due to the increasing complexity of business models, this will also make it difficult to implement the concept⁵ of financial regulation through the simple and clear rules outlined above.

Instead of rules-based regulatory regimes, principles-based ones will be considered,⁶ which provide a greater degree of flexibility. In some jurisdictions, there is controversy⁷ as to whether there should be regulation first and then innovation, or innovation first and then regulation. Another discussion is based on the regulatory pendulum, which points out that the economic depression caused by the Financial Crisis certainly made recent financial regulation stricter. On the one hand, the public expects strict regulation to protect its investors; on the other, regulators also hope to avoid any financial risks via strict regulation and to reduce the risks of public pressure.

Lastly, the recent emergence of the TechFin industry has been widely discussed. This marks a new global trend⁸ in non-financial companies involved in financial businesses, especially in the technology, e-commerce,

⁴ Yesha Yadav & Chris Brummer, *Fintech and the Innovation Trilemma*, 107 Georgetown Law Journal 235, 262–64 (2019).

⁵ Ibid. at 264–66.

⁶ Chris Brummer & Daniel Gorfine, *FinTech: Building a 21st-Century Regulator's Toolkit*, 5 Milken Institute 6–7 (2014), https://milkeninstitute.org/sites/default/files/reports-pdf/3.14-FinTech-Reg-Toolkit-NEW_2.pdf.

⁷ “Outside of the financial sector context, debates regarding the best approaches to address innovation—particularly technological innovation—typically center around questions of whether to regulate in advance of innovation or whether to allow innovation to develop and then, if necessary, regulate post development.” Zetsche et al., *supra* note 2, at 50.

⁸ Dirk A. Zetsche et al., *From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance*, 4–5 (Eur. Banking Inst., Working Paper No. 6, 2017), <https://ssrn.com/abstract=2959925>.

or telecom sectors. For example, China's Alibaba's Ant Group offers a variety of financial services, such as Alipay, and the U.S. Facebook has in recent years invested in Libra coins, which are available in most countries of the world. The main advantage of these companies is that they have a large number of users and their data for credit assessment, which can then be used for financial business development.⁹ This also makes the existing laws, which are primarily tailored for financial companies, not especially applicable for TechFin ones.

THE POTENTIAL OF PUBLIC AND PRIVATE GOVERNANCE FOR FINTECH

It was noted above that most discussion thus far has focused on how the public sector should regulate FinTech, but there has been a lack of discourse on how the private sector could contribute to FinTech governance. With the increasing complexity of contemporary society, it is doubtful whether a top-down regulatory model can perform optimally, e.g., the public-sector-oriented supervision approaches in most jurisdictions across various industry sectors.

With the recent establishment of the Innovation Office and Regulatory Sandbox, it is apparent that the orientation of regulators has shifted from pure supervision to governance. Instead of the supervision mindset, how to lead the development of FinTech and be competitive at the global level is an important objective that regulators take into consideration. In addition, the study suggests that industry self-regulation (self-governance)¹⁰ should be considered to provide better forms of governance, as in the establishment of industry associations and the implementation of self-regulation rules¹¹ through the reputation mechanism.

This chapter reviews the FinTech regulations from selected jurisdictions and observes that the regulatory framework falls into four distinct categories: (1) supervision-oriented approaches driven by public sectors; (2) collaboration-oriented approaches driven by public sectors; (3) supervision-oriented approaches driven by private sectors; and (4) collaboration-oriented approaches driven by private sectors. The chapter

⁹ Ibid. at 9.

¹⁰ Yadav & Brummer, *supra* note 4, at 297.

¹¹ Ibid. at 304.

also aims to provide concrete examples that cross three major FinTech markets, namely, China, the United States, and UK and to conclude the best practices or early lessons learned. It also highlights the benefits and challenges presented by each regulatory approach.

Supervision-Oriented Approaches Driven by Public Sectors: The U.S. Jumpstart Our Business Startups (JOBS) Act

The U.S. JOBS Act was one of the first regulatory response to the emergence of the FinTech industry, especially regarding equity-based crowdfunding. The background of the JOBS Act was that the Financial Crisis of 2008, which caused a global economic depression and rising unemployment rates. In order to remedy the issue of unemployment, the U.S. authorities encouraged the public to start their own companies as a means of creating job opportunities. At the time, crowdfunding was becoming popular around the world, and many people were using it as a channel to raise the funding they needed to put their ideas into practice with financial support from the public. Accordingly, lawmakers sought to amend regulation to make crowdfunding a legal way for new businesses to raise funds from the public, as well as to create a better capital market.

In order to ensure that the risks were controllable, the JOBS Act limited the annual fundraising amount of each fundraiser and required them to comply with disclosure obligations. In addition, it also sets an annual cap on the total amount of investment of each general investor to secure funds, given that equity-based crowdfunding is risky. However, it is worth noting that although the Act was first announced in 2012, it did not take effect in the United States until 2015, with three years needed for the entire legislative process entailed. Of course, it is necessary to plan well when drafting the law. However, this is obviously time-consuming and could not keep pace with the rapid development of technology.

In addition to the problem of time expenditure addressed above, more importantly, the fast-changing business models of FinTech firms also present huge challenges to regulators. For example, initially, the peer-to-peer lending industry simply matched borrowers and lenders as its chief business model. In order to enhance the confidence of lenders in online loans, online lending platforms prepared certain amounts of funding and

guarantees to lenders that they could receive the principal on time.¹² The risks of the original model against the later one differ.

Therefore, there are two major disadvantages of “supervision-oriented approaches driven by public sectors,” namely, that the legislative process is time-consuming and business models change rapidly. It takes too much time for new regulation, which cannot keep pace with development driven by technology. The rapid change in business models is also another factor that presents huge challenges. In the case of China’s peer-to-peer lending industry, the regulatory authorities took a “do nothing” approach so as to not stifle the initial emergence of financial technologies. They also drafted a bill for peer-to-peer lending. As previously noted, there were many problematic peer-to-peer lending platforms in China, some of which were even involved in the Ponzi scheme. Eventually, in 2020, regulators in China decided to crack down on the entire industry. Based on the above case, it can be seen that the legislative process is unable to keep pace with the speed of the development of the FinTech industry. It reflects that the disadvantages of taking a traditional approach, such as new regulation or amending the law in order to harness the innovation.

After the introduction of the JOBS Act in the United States, financial regulators around the world conducted a legal transplantation in an effort to build alternative channels of fundraising and encourage the founding of startups. However, it is worth noting that not every country has been successful. In Japan, equity-based crowdfunding was legalized through a legal amendment in 2015. However, by 2018, there had still been no applications submitted to become a platform providing equity-based crowdfunding services.¹³ Another example is Taiwan, where there are several equity-based crowdfunding platforms, but their total market scale is only around 393,000 USD.¹⁴ These cases reflect the necessity for

¹² “The P2P sector offers a good example of how regulation needs to proceed carefully when creating rules for an industry. industry demands may represent nothing more than a snapshot in time of their difficulties and may fail to address the evolving nature of their business as it grows in terms of market size and risk.” Douglas W. Arner et al., *The Evolution of FinTech: A New Post-crisis Paradigm*, 47 *Georgetown Journal of International Law* 1271, 37–38 (2016).

¹³ “However, in the years following the amendment equity-based crowdfunding has been virtually non-existent in Japan.” T. Ziegler et al., *The 3rd Asia Pacific Region Alternative Finance Industry Report* 81 (2018).

¹⁴ “For example, even though three of six private platforms have been issued equity-based crowdfunding licenses and commenced operations in 2015, only 2 startups appear to

further legal amendments in both jurisdictions. However, as noted above, the amendment process takes time and the business model will keep developing and changing in parallel. Accordingly, “supervision-oriented approaches driven by public sectors” will not be the only approach and may not be the best one for FinTech governance.

*Collaboration-Oriented Approaches Driven by Public Sectors:
Regulatory Sandboxes and Innovation Offices*

As discussed above, the legislative processes required to facilitate “supervision-oriented approaches driven by public sectors” take a long time. They are thus unable to keep pace with the rapid development of financial technologies. In order to accelerate and encourage the development of FinTech, the Financial Conduct Authority in the UK introduced a “regulatory sandbox” system, which provides a new regulatory mechanism. Specifically, the financial regulator offers financial technology start-ups the opportunity to test their business models for a certain period under certain conditions before relevant regulation is formally established. Instead of fully licensed business, the annual transactional amounts and user groups are restricted to mitigate potential risks. For instance, a company applying to enter the regulatory sandbox is allowed to start its operations for “professional investors” within “a year” and not exceed the transactional amount of “\$1 million annually.”

In this way, FinTech companies can apply for entry into the regulatory sandbox in compliance with regulatory requirements and adjust their business models through real operations to further development. For financial regulators, the regulatory sandbox can also help them understand the potential risks associated with emerging business models and make timely regulatory responses to companies utilizing the sandbox. To this extent, the regulatory sandbox can encourage innovation by allowing applicants to test their business models and ensure consumer protection by certain restrictions. This would be helpful for a country seeking to accelerate and boost the development of FinTech.

The regulatory sandbox focuses more on a collaboration-oriented approach between the regulator and regulated companies. Although we

have successfully raised 12 million TWD (around US\$393,000) on the licensed platforms in operation by February 2017.” Cambridge Judge Business School, *Cultivating Growth: The 2nd Asia Pacific Region Alternative Finance Industry Report 68* (2017).

acknowledge the advantages of regulatory sandboxes, a previous study¹⁵ pointed out that in order to ensure that FinTech companies successfully pass the experiment, they have the capacity to take on a larger user base. In a regulatory sandbox, business models are tested with restrictions on the number of transactions and their size. It is not the same as the market scale and its associated real-world risks. Specifically, success in the sandbox may only occur in the experimental environment. From this perspective, this study argues that the regulatory sandbox still provides the best balance between promoting innovation and consumer protection. The concept of a regulatory sandbox could overcome the issues of “Too Small to Care,” “Too Large to Ignore,” and “Too Big to Fail.” It offers a mechanism for regulators to work with FinTech companies and determine better solutions.

With respect to legal transplantation, more than 50 countries around the world have adopted the regulatory sandbox model; however, it is worth noting that only a few have successfully fostered innovation. The main reasons are two-fold, which include: (1) the organizational structure does not need to be adjusted accordingly; and (2) a lack of human resources.

First, in terms of organizational structure, the regulatory sandbox could be categorized as a singular framework or a multifaceted one. The one introduced by the FCA in the UK and adopted by most jurisdictions falls into the former, whereas Thailand and Hong Kong deployed the latter. In Thailand, the Central Bank, Securities Exchange Commission, and Office of Insurance Commission all have regulatory sandboxes. FinTech companies can apply to their respective authorities according to the type of business proposed. In practice, however, the business models of FinTech are often associated with diversified fields, which might fall within the scope of multiple regulatory authorities. In this case, it is not clear to the applicant which regulatory sandbox ought to be chosen. Moreover, the cross-organizational collaboration of regulatory sandboxes is ambiguous. Hong Kong had a similar problem at first, but the regulator changed to a single regulatory sandbox¹⁶ and the number of applications significantly increased.

¹⁵ Yadav & Brummer, *supra* note 4, at 296.

¹⁶ “Hong Kong has experienced the benefits of improved regulatory coordination. Previously, the Monetary Authority, the Securities and Futures Commission, and the Insurance Authority had the benefit of improved regulatory coordination. Futures Commission,

Second, it is also important to note that the UK's regulatory sandbox system assigns an expert to assist companies subject to it. To this extent, if a country simply conducts legal transplantation of a sandbox system without considering the required human resources, the regulatory sandbox cannot operate optimally. This is also in line with a study that pointed out the importance of the change in the functions of the supervisory authority; that is, the financial authority should make corresponding adjustments in response to the digital transformation, such as through the establishment of new organizations or positions to accelerate digital development.¹⁷

Comparative studies across jurisdictions have indicated that China itself is a huge regulatory sandbox¹⁸; however, this paper argues that the “do nothing” approach taken by the Chinese regulatory authorities from 2015 is not equivalent to the regulatory sandbox model as discussed above. The main difference is that the regulatory sandbox referred to is specifically intended to test FinTech business models in a restricted environment, such as in the presence of limitations on transaction amounts, investors, and experimental period. Furthermore, the regulator is to actively work with the applicants of a regulatory sandbox and together contribute to FinTech development and better governance. This is quite different from the “do nothing” approach.

In addition to the regulatory sandbox, the *innovation office* set up by the UK's Financial Conduct Authority (FCA) has been introduced¹⁹ in

and the Insurance Authority had independent regulatory sandboxes, which made it difficult to test products that spanned jurisdictions.” UNSGSA FinTech Working Group, *Early Lessons on Regulatory Innovation to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes and RegTech* 32 (2019).

¹⁷ 臧正運 [Zhengyun Tsang], 金融科技法制與監理變革的形塑力量與關鍵趨勢 [The Shaping Forces and Key Trends of Legal and Regulatory Changes in Fintech], 236 萬國法律 2, 7 (2021).

¹⁸ “In practice, this meant that China's need for regulatory sandboxes was limited, as China itself represented a sandbox on a national level.” Zetzsche et al., *supra* note 2, at 50.

¹⁹ “Starting in 2015 (to our knowledge, with the Luxembourg Commission de Surveillance du Secteur Financier (CSSF), the United Kingdom's Financial Conduct Authority (U.K. FCA), and the Australian Securities and Investments Commission (ASIC) functioning as first movers), communication between regulators and FinTechs has increasingly been institutionalized through the development of innovation departments within. Since 2015, institutional access points have been established in over twenty jurisdictions.” *Ibid.* at 39–40.

more than 20 countries around the world since 2015. The innovation office aims to establish a communication mechanism between regulators and FinTech companies. The names are different among jurisdictions; for example, Japan's Financial Services Agency has set up a FinTech Support Desk, Singapore's Financial Supervisory Authority has set up a FinTech Office, and the South Korean government has established a FinTech Center. All are designed to further strengthen communication between regulators and FinTech companies and to help companies understand how to apply for the necessary licenses²⁰ and comply with the regulations. It should be noted that the Innovation Office changes top-down supervision into horizontal collaboration with regulated businesses and helps to unify the multiple windows in the financial authority, making internal resources more effectively operated and improving external communication with prospective financial companies. Overall, it could help FinTech companies start their businesses as soon as possible and boost FinTech development in a country.

Supervision-Oriented Approaches Driven by Private Sectors: The Japan Cryptocurrencies Exchange and Peer-to-Peer Finance Association in the UK, Credit Ratings Agencies on Peer-to-Peer Lending in China

The U.S. JOBS Act, the Regulatory Sandbox, and the Innovation Office, are all driven by public sectors. However, with the increasing complexity of modern society and rapid changes in technology, it is doubtful whether the government's capacity remains sufficient to carry on. According to a recent report,²¹ 67% of U.S. federal statutes have never been updated and 17% have only been updated once. Another study also pointed out that unlike the ICT industry in the past, which was normally led by a single company²² or a few companies, the digital economy is facing a huge number of new companies and startups bringing innovation to the

²⁰ Péter Fáykiss, Dániel Papp, Péter Sajtos & Ágnes Törös, *Regulatory Tools to Encourage FinTech Innovations: The Innovation Hub and Regulatory Sandbox in International Practice*, Financial and Economic Review 43, 53–54 (2018).

²¹ Jason Lewris et al., *Using Advanced Analytics to Drive Regulatory Reform*, Deloitte, 6, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-using-advanced-analytics-to-drive-regulatory-reform.pdf>.

²² Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 Jurimetrics 79, 83–84 (2020).

industry around the world. Regulators are often unable to keep up with the industry's rapid development. The problems of "legislative dysfunctionality" and "agency resource constraints" are especially apparent due to the complexity of the digital world.²³ Therefore, it is necessary to explore the feasibility and necessity of governance driven by private sectors.

In Japan, the cryptocurrencies exchange industry was not regulated by the government at first. However, market players decided to form an industry association and set up self-regulatory rules in order to maintain the industry's reputation. Later, Japan established relevant laws and regulations. However, the Japanese cryptocurrency exchange industry association still plays an important role, and even those who wish to apply for a license must be nominated by the industry association, which shows its role in governance. In addition, in the UK peer-to-peer lending industry, there was a similar industry association that played a self-regulatory role before the UK FCA intervened. However, with the implementation of the relevant regulations for a couple of years, the industry association no longer exists, which differs from the practice of Japan's cryptocurrencies exchange industry.

In addition to the industry associations in Japan and the UK, the credit ratings agencies on peer-to-peer lending in China is another example of observing how the market works without regulation from the financial authorities. As noted earlier, the peer-to-peer lending industry in China has caused the public to be distrustful of the industry due to factors such as Ponzi schemes. In order to help investors better understand the qualities among various peer-to-peer lending platforms in the market, credit ratings agencies, such as Wangdaizhijia, Wangdaitianyan, and Rong360, publish the scores of peer-to-peer lending platforms, which could serve as references to help investors choose loan products corresponding to the risks they can afford.

The research indicated that self-regulatory rules can be used as a tool²⁴ to fill in regulatory gaps and improve the quality of regulation. Industry associations can also serve as good communication channels between

²³ Ibid. at 86.

²⁴ "Private self-regulation can be especially helpful in filling gaps and informing the quality of public regulatory oversight." Brummer & Yadav, *supra* note 4, at 304–5.

regulators and the FinTech industry²⁵; for example, the Canadian Financial Authority was in discussions with R3, a blockchain association comprised of more than 80 financial companies, to decide whether to adopt blockchain technology into the financial system.

It should also be noted that those outsourced business of financial institutions,²⁶ especially that many financial institutions are currently adopting cloud services provided by large technology companies. However, how should financial regulators manage issues such as information security presented by cloud service providers instead of financial institutions? Specifically, ever more financial institutions rely on cloud platforms such as Google or Amazon, but we have also seen that these cloud platforms have had network problems lasting hours or days in the past few years. Who should take responsibility for transaction losses incurred in such cases²⁷—financial institutions or cloud service providers? This reflects the fact that governance driven by public sectors might not be sufficient for the increasingly complex society created by new technologies. Therefore, it is urgent and necessary to further discuss how to leverage market reputation mechanisms, the self-regulations of industry associations, or credit ratings agencies to facilitate co-governance via public–private collaboration.

How to truly implement regulations driven by private sectors remains a challenge. Unlike public sectors, private sector actors have no power to compel implementation. Furthermore, for industry associations, the market coverage of members, membership criteria, neutrality of the rules, and the compliant system ensure that the self-regulatory rules set by the association meet the industry’s expectations and avoid it gaining a potential monopoly, all of which constitute approaches to pursuing better governance driven by private sectors. In addition, doubts are often raised about credit ratings agencies, such as whether they can perform their duties fairly. On the one hand, they charge service fees from the rated companies; on the other, they provide ratings services. How to be transparent and avoid those public concerns is highly critical for the further evolution of the governance power of private sectors.

²⁵ Ibid. at 305.

²⁶ Tsang, *supra* note 17.

²⁷ Elaine Ou, *Can’t Stream Netflix? The Cloud May Be to Blame*, Bloomberg (March 2, 2017), <https://www.bloomberg.com/opinion/articles/2017-03-02/can-t-stream-netflix-the-cloud-may-be-to-blame>.

Collaboration-Oriented Approaches Driven by Private Sectors: Plug and Play Abu Dhabi, Global FinTech Hackcelerator Singapore, Taiwan FinTechSpace

Several regulators have launched FinTech accelerators, which are usually operated by a semi-government organization. Accelerators typically provide or facilitate mentoring, workspaces, consultations with industry experts (including on regulation), networking opportunities, and access to funding.²⁸ For instance, Plug and Play Abu Dhabi, supported by the Abu Dhabi Investment Office, aims to foster corporate innovation and the integration of start-ups in businesses. Others, such as the Global FinTech Hackcelerator organized by MAS, allow regulators to work with firms to solve industry problem statements. The common characteristics of these accelerators are linked with regulators. Another example, FinTechSpace in Taiwan, is a financial technology incubator supported by the FSC, a financial regulator in Taiwan, and is operated by the Institute for Information Industry to provide counseling to FinTech start-ups in Taiwan and generally boost FinTech. It provides a full range of services,²⁹ from venture capital, to advisory services, legal advice, building platforms to connect banks with startups, as well as FinTech exhibitions. The Taiwan FinTechSpace also provides a mechanism of communication between start-ups through a coworking space, which is helpful for the formation of an industry self-regulatory atmosphere and encourages startups to participate in public hearings to express their opinions and helps these incubated companies cooperate³⁰ with banks or large corporations. Incubators and accelerators run by a semi-government organization is an exemplary format of how a public sector can work together with the private for the better development and governance of the industry. There are currently eight comparable projects initiated by regulatory bodies around the world.

²⁸ “Accelerators typically provide or facilitate mentoring, work spaces, Accelerators typically provide or facilitate mentoring, work spaces, consultations with industry experts (including on regulation), networking opportunities, and access to funding.” UNSGSA, *supra* note 16, at 19.

²⁹ 羅至善 [Luo Zhi-Shan], 從新創培育經驗看金融監理的數位轉型 [*The Digital Transformation of Financial Supervision from the Experience of New Venture Cultivation*], 236 萬國法律 11 (2021).

³⁰ Nadim Bardawil, *Fintech and the Accelerator Culture*, 37 International Financial Law Review 101, 102 (2018).

Summary

In this paper, we built a simple framework to map out four regulatory approaches for harnessing the potential of financial disruption, namely: (1) supervision-oriented approaches driven by public sectors; (2) collaboration-oriented approaches driven by public sectors; (3) supervision-oriented approaches driven by private sectors; and (4) collaboration-oriented approaches driven by private sectors. We summarize the above discussion in Table 5.1.

First, we consider the JOBS Act in the United States as an example to observe how financial regulators respond to innovative business models through legislation. From the above case, we can see that it takes too much time for the legislative process and it is difficult to catch up with the evolution of changing technologies and business models. In response, policymakers around the world are creating “regulatory sandboxes” to foster innovation in the financial sector while staying alert to emerging risks. One key objective of sandboxes is to facilitate startups’ access to capital. The UK Financial Conduct Authority pioneered the world’s first regulatory sandbox in 2015. To date, more than 50 countries have adopted sandboxes. This study also analyzed how private sector regulatory governance can complement regulatory gaps or fill out the gap of

Table 5.1 FinTech governance matrix

	<i>Collaboration-oriented approach</i>	<i>Supervision-oriented approach</i>
Public sectors	Some jurisdictions have established innovation offices and regulatory sandboxes as a first step in their regulatory innovation journeys Flexibility and one-stop services The limitation of small-scale experiments <i>Examples: Innovative offices, regulatory sandboxes</i>	The common approach for regulators responding to financial disruption via amendments or new regulations Legitimacy Take too much time and is not agile <i>Examples: JOBS Act</i>
Private sectors	A number of regulators have also launched FinTech accelerators Efficiency of communications Still in the early stages <i>Examples: Government-linked accelerators</i>	Self-regulations are adopted by FinTech sectors across countries Supplements to regulations Concerns of fairness <i>Examples: Industry association, credit ratings agencies</i>

Source The Author

insufficient regulatory capacity. For instance, the industry association of P2P lending in the UK, P2PFA, made up a fundamental part of regulating the P2P lending industry before relevant regulation was issued by the UK authorities. It is somewhat similar for the cryptocurrencies exchange industry in Japan. Lastly, noting the global financial regulatory trend, we can also observe that financial regulators have moved away from their solely regulatory role to promote the development of the industry by means of incubators, helping FinTech companies accelerate their development.

CONCLUSIONS

This paper first analyzed the development of the FinTech industry and associated risks, and then reviewed the academic discussions around FinTech governance. It was determined that most studies primarily focus on public sector regulation, with less attention paid to how private sectors can contribute to better governance. Over the past decade, private sector governance or co-governance also substantially influenced FinTech development. This paper aimed to provide case studies through various selected jurisdictions and analyze the strengths and weaknesses of the public and private sector regulatory mechanisms in the hope that this could provide another perspective on FinTech governance. The five key points conveyed in this paper are as follows:

1. **The increase in the number of market players:** Compared to the financial industry, which in the past was mostly dominated by large enterprises, ever more FinTech innovations are initiated by startups. Regulators are therefore facing the challenge of how to deal with the rapidly growing number of FinTech products launched by a huge variety of market players.
2. **The complexity of business activities:** FinTech now encompasses payments, lending, fundraising, insurance, and robotic advisors. In some cases, a single FinTech product could cover a variety of business areas. Accordingly, the increasing levels of innovation and the complexity of changing business activities makes it more complex than ever.
3. **From strict supervision to agile governance:** In the past, regulation placed more emphasis on strict rules to mitigate the risks. It also aimed to implement regulation that was universal for the entire

industry. In modern society, however, business patterns are changing rapidly and regulation alone may not be the solution. Regulatory actors should consider pursuing better governance through public and private sector cooperation or regulation. This would be helpful in mitigating the insufficient capacity of relevant authorities in the digital world.

4. **From risk-prevention to eco-system building:** In the era of globalization, a regulator should not only prevent domestic risks but also consider its competitiveness in its region and the world. As is apparent in the cases of Abu Dhabi, Singapore, and Taiwan, regulators are actively building eco-systems to boost FinTech development instead of engaging in strict supervision.
5. **From supervision driven by government to co-governance:** This paper analyzes current FinTech governance from the perspective of public–private collaboration. Each model has its own advantages and disadvantages. These depend on the practices and needs of a jurisdiction. This study wishes to offer regulators a blueprint for FinTech governance.

The study provides a matrix to map out four types of regulatory approaches based on case studies across jurisdictions, spanning various mechanisms, which includes regulation, innovation offices, regulatory sandboxes, industry associations, credit ratings agencies, and government-linked accelerators. How these different mechanisms operate in theory and practice is the subject of this comparative analysis. Such a comparative view is essential to a better understanding of the strengths and weaknesses of the various mechanisms and their practical implementation. It aims to unpick the complexity of how to harness the potential of FinTech. This paper is aimed not only at scholars but also at the central banks and securities and exchange commissions themselves, seeking to assist them in revising their rules, as well as at states and organizations developing future legal mechanisms or better approaches to governance.

LITERATURE

- Adam Thierer, *Soft Law in U.S. ICT Sectors: Four Case Studies*, 61 *Jurimetrics* 79 (2020).
- Cambridge Judge Business School, *Cultivating Growth: The 2nd Asia Pacific Region Alternative Finance Industry Report* (2017).

- Chris Brummer & Daniel Gorfine, *FinTech: Building a 21st-Century Regulator's Toolkit*, 5 Milken Institute (2014), https://milkeninstitute.org/sites/default/files/reports-pdf/3.14-FinTech-Reg-Toolkit-NEW_2.pdf.
- Dirk A. Zetsche et al., *From Fintech to Techfin: The Regulatory Challenges of Data-Driven Finance* (Eur. Banking Inst., Working Paper No. 6, 2017), <https://ssrn.com/abstract=2959925>.
- Dirk A. Zetsche et al., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 *Fordham Journal of Corporate and Financial Law* 31 (2017).
- Douglas W. Arner et al., *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 *Northwestern Journal of International Law and Business* 371 (2017).
- Douglas W. Arner et al., *The Evolution of FinTech: A New Post-crisis Paradigm*, 47 *Georgetown Journal of International Law* 1271 (2016).
- Elaine Ou, *Can't Stream Netflix? The Cloud May Be to Blame*, Bloomberg (March 2, 2017), <https://www.bloomberg.com/opinion/articles/2017-03-02/can-t-stream-netflix-the-cloud-may-be-to-blame>.
- Jason Lewris et al., *Using Advanced Analytics to Drive Regulatory Reform*, Deloitte, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-using-advanced-analytics-to-drive-regulatory-reform.pdf>.
- Nadim Bardawil, *Fintech and the Accelerator Culture*, 37 *International Financial Law Review* 101 (2018).
- Péter Fáykiss, Dániel Papp, Péter Sajtós & Ágnes Törös, *Regulatory Tools to Encourage FinTech Innovations: The Innovation Hub and Regulatory Sandbox in International Practice*, *Financial and Economic Review* 43 (2018).
- T. Ziegler et al., *The 3rd Asia Pacific Region Alternative Finance Industry Report* (2018).
- UNSGSA FinTech Working Group, *Early Lessons on Regulatory Innovation to Enable Inclusive FinTech: Innovation Offices, Regulatory Sandboxes and RegTech* (2019).
- Yesha Yadav & Chris Brummer, *Fintech and the Innovation Trilemma*, 107 *Georgetown Law Journal* 235 (2019).
- 羅至善 [Luo Zhi-Shan], 從新創培育經驗看金融監理的數位轉型 [The Digital Transformation of Financial Supervision from the Experience of New Venture Cultivation], 236 *萬國法律* 11 (2021).
- 臧正運 [Zhengyun Tsang], 金融科技法制與監理變革的形塑力量與關鍵趨勢 [The Shaping Forces and Key Trends of Legal and Regulatory Changes in Fintech], 236 *萬國法律* 2 (2021).



Digital Assets and Central Bank Digital Currency in ASEAN

Pawee Jenweeranon

INTRODUCTION

Digital assets have been utilized as fundraising tools and means of trade in several Southeast Asian nations. These operations are being carried out outside of any legal framework, causing considerable worry among governments and regulatory agencies in many countries, who see them as posing serious threats to national financial stability and retail investors. However, apart from regulators and public concerns, governments and regulators in ASEAN also recognize the potentials of ICOs, cryptocurrency and DLT technology in various ways, such as the recognition of their potential for enhancing financial inclusion for start-ups as expressed by the Thai Securities and Exchange Commission (SEC), which is the main regulator for supervising such activity.¹

¹ “SEC Thailand’s Viewpoint on ICO”, Securities and Exchange Commission of Thailand, accessed July 30, 2019, <https://www.sec.or.th/EN/Pages/FinTech/ICO.aspx>.

P. Jenweeranon (✉)
Thammasat University, Bangkok, Thailand
e-mail: paweejen@tu.ac.th

In recent years, many countries, such as Singapore, Malaysia and Thailand, have increased the number of digital token sales as a means of fundraising. In 2018, successful ICO projects in many countries spurred the regulators to regulate these activities in order to prevent fraudulent behaviour and scams. To demonstrate this increasing trend, the blockchain start-up TenX successfully raised close to USD 80 million through a token sale in Singapore.² Also, in Thailand, there is an ICO project called JFinCoin ICO launched by the J Ventures company, which raised funds through digital token offerings in January 2018.

Consequently, this has led to the use of regulatory approaches among ASEAN countries to prevent possible risks and to derive benefits from this technology at the same time with bespoke regulatory solutions. For example, the Royal Decree on Digital Asset Businesses, which was enacted in Thailand, expressed the guideline (A Guide to Digital Token Offerings) that has been issued by the financial authority of Singapore and the Capital Market and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 as well as the Guidelines on Digital Assets of the Securities Commission Malaysia (SC).³

In general, the problems of capital shortage facing small- and medium-sized enterprises (SMEs) in many countries led to the proposal of a regulatory framework for alternative financing instruments outside the traditional banking sector in national and regional legal regimes. Apart from the efforts of many countries to improve the legal and institutional framework for access to secured credit, financial technology or *FinTech* is considered to be the solution. This is also because of industry backgrounds concerning the percentage of internet users, mobile phone users and other related factors.

To reflect the significance and constraints of digital assets in general, to exemplify this, tokenization will allow for the creation of a new financial system and will undergo widespread adoption; however, regulation often stands as an obstacle. To date, there have been a number of problematic legal issues potentially arising from asset tokenization. These include the lack of clarity of the relevant regulatory frameworks, the lack of

² Marcus Chow, Jolie Giouw, “MAS clarifies position on the offer/issue of digital tokens in Singapore”, accessed July 30, 2019, <https://www.twobirds.com/en/news/articles/2017/singapore/mas-clarifies-position-on-the-offer-issue-of-digital-tokens-in-singapore>.

³ Guidelines on Digital Assets, <https://www.sc.com.my/api/documentms/download.ashx?id=dabaa83c-c2e8-40c3-9d8f-1ce3cabe598a>.

co-ordinated activity between regulators as well as problematic issues pertaining to the unclear legal rights and obligations of token issuers and token holders. Because of this, the advantages of tokenization are potentially undermined unless regulators put in place a regulatory framework which can appropriately balance risk prevention and market stimulation, creating adequate asset support tokenization for SME financing. A regulatory framework as well as a policy toolkit are needed to adequately address the legal, regulatory challenges and potential risks of asset tokenization.

In a broader sense, to be more specific, this chapter aims at exploring current regulatory frameworks in ASEAN countries related to digital assets in a broad sense.

From the aforementioned statement, digital assets can be used as alternative fundraising channels for businesses. Accordingly, to understand the challenges in financial inclusion in ASEAN is necessary to understand countries' efforts to support the use of digital assets in general.

Financial Inclusion and Digital Finance

In recent years, financial inclusion has been a significant issue in Asia-Pacific⁴ and other regions of the world. According to a publication from the International Monetary Fund (IMF), financial inclusion is associated with economic growth in developing countries.⁵ In the case of financial inclusion and the use of technology, countries in Asia-pacific have also made great progress to enhance financial inclusion through their use of technology⁶; for instance, the adoption of digital financial services including mobile banking and mobile money, as well as instant payment schemes.

⁴ Sarwat Jahan, Jayendu De, Fazurin Jamaludin, Piyaporn Sodsriwiboon and Cormac Sullivan,

The Financial Inclusion Landscape in the Asia-Pacific Region: A Dozen Key Findings, IMF Working Papers, <https://www.imf.org/en/Publications/WP/Issues/2019/04/19/The-Financial-Inclusion-Landscape-in-the-Asia-Pacific-Region-A-Dozen-Key-Findings-46713>.

⁵ *Financial Inclusion in Asia-Pacific*, Asia and Pacific Department, International Monetary Fund, Department Papers Policy Papers, <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2018/09/18/Financial-Inclusion-in-Asia-Pacific-46115>, p. 5.

⁶ *Ibid.*, 5.

In the ASEAN region, banking penetration remains low in many jurisdictions, with only some 47% of ASEAN citizens having a bank account. The huge gap among ASEAN countries can be seen with the 40% of the Philippines population that has a bank account⁷ compared to Malaysia's 80% account-holding statistic.⁸

It is worth noting that there have been many attempts, both international and domestic, to address the financial exclusion problem. To this extent, the promotion of financial inclusion in the ASEAN region was mandated in the Chair's statement of the 19th ASEAN Summit in Bali in 2011. Also, during the summit, ASEAN Ministers were tasked with exploring new initiatives to address the problem. Accelerating financial inclusion in the Southeast Asian region with digital finance has been proposed as the main solution by the Asian Development Bank (ADB); a report published by the ADB further emphasized that collaboration between different stakeholders such as regulators, public policymaking institutions and supply-side participants is needed. Digital finance is expected to increase financial inclusion.⁹ It also has the potential to boost GDP by 2%–3% in Indonesia and the Philippines, and 6% in Cambodia.¹⁰

To be more specific, in order to grow financial inclusion in the region, three primary foundations must be taken into account to enable the spread of digital financial services (DFS). These include government and private sector commitment to the development of DFS, a good ICT infrastructure, as well as an appropriate legal and regulatory framework.¹¹ From a legal and regulatory perspective, according to the ADB publication,¹² regulatory frameworks for DFS can be categorized into many types

⁷ Irawan Hadi Payitno, "2017 Financial Inclusion in Indonesia Reaches 63 Percent", *netralnews*, January 5, 2018, <http://www.en.netralnews.com/news/business/read/17080/2017..financial.inclusion.in.indonesia.reac>.

⁸ Ibid.

⁹ "Accelerating Financial Inclusion in South-east Asia with Digital Finance", Asian Development Bank, accessed July 30, 2020, <https://www.adb.org/sites/default/files/publication/222061/financial-inclusion-se-asia.pdf>.

¹⁰ Ibid, 4.

¹¹ "Advancing Digital Financial Inclusion in ASEAN, Policy and Regulatory Enablers", World Bank Group, accessed July 30, 2020, <http://documents.worldbank.org/curated/en/856241551375164922/pdf/134953-WorldBankASEANDigitalFinancialInclusioninASEANpublicationJan.pdf>, pp.12.

¹² Ibid., pp. 37–45.

of specific regulatory frameworks; for instance, regulatory frameworks for payment services and providers, e-money service providers, online lending service platforms, equity-based crowdfunding platforms and as a banking agent initiative.¹³

The benefits of enhancing financial inclusion, especially SME financial inclusion, include helping increase economic growth at both the domestic and regional levels. This is also due to the fact that SMEs play a key role with respect to job creation and financial stability.¹⁴

Apart from the above-mentioned statements, which state the potentials of digital finance in enhancing financial inclusion, it should be noted that, in particular, digital financial services through mobile phone technology has become one of the preference tools to address the current financial exclusion challenges, especially in developing countries. To this, E-money and mobile money can be seen as one of the primary ways in increasing access to finance in a number of countries such as various African nations.

However, generally, even digital finance is widely accepted as an instrument for financial inclusion. Key risks from the use of digital finance can reflect the need for a regulation and a supervisory approach. Risks might have occurred due to the lack of knowledge and awareness in financial services and products. To this, financial literacy and financial education have the potential to act as supportive tools to prevent possible risks.

To enable businesses to offer new financial products and services, we need a regulatory framework to mitigate potential risks and to support market players who offer innovative products and services. This is also to promote fair competition in the market, which can deliver benefits for consumers through lower prices, greater choices, and improved services. This includes laws and regulations for digital assets and its related activities that could have a role in encouraging greater financial inclusion in many ways.

¹³ Ibid., pp. 37–45.

¹⁴ *Financial Inclusion of Small and Medium-Sized Enterprises in the Middle East and Central Asia*, Department Papers/ Policy Papers, International Monetary Fund (IMF), <https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/02/11/Financial-Inclusion-of-Small-and-Medium-Sized-Enterprises-in-the-Middle-East-and-Central-Asia-46335>, pp. 5–11.

DIGITAL ASSETS REGULATIONS IN SELECTED ASEAN COUNTRIES

This section aims to explore legislative and regulatory efforts in ASEAN countries to reflect different regulatory approaches being used by regulators or policymakers. In this regard, digital asset regulations are a broad term that reflects all relevant regulations concerning cryptocurrencies, digital tokens, CBDCs, underlying technologies and related activities.

Indonesia

Indonesia does not recognize virtual currency as a non-cash payment method on the grounds that it is its own currency and not the Indonesian Rupiah. Bank Indonesia Regulation No.18/40/PBI/2016 concerning the Implementation of Payment Transaction Processes specifically prohibits the use of virtual currency in the payment transaction process.

This regulation defines virtual currency as digital money issued by parties other than a monetary authority and obtained through mining, purchase or reward transfer, for example Bitcoin, BlackCoin, Dash, Dogecoin, Litecoin, Namecoin, Nxt, Peercoin, Primecoin, Ripple and Ven. Virtual Currency is not recognized as a valid means of payment and is hence prohibited in Indonesia.

Such was declared by Bank Indonesia in a press release dated February 6, 2014 entitled “Pernyataan Bank Indonesia Terkait Bitcoin dan Virtual Currency Lainnya”, which can be translated as “Statement of the Bank Indonesia in relation to Bitcoin and other Virtual Currencies”. The statement expresses Bank Indonesia’s position that Bitcoin and other virtual currencies are neither real currencies nor acceptable payment methods in Indonesia. The general public is advised to exercise caution while dealing with Bitcoin and other virtual currencies. Any risk associated with Bitcoin ownership/use is borne solely by the owner/user of this virtual currency.

Although virtual currency may be used as a form of payment in Indonesia as stated above, virtual currency trading is not banned. Instead, the Commodity Futures Trading Regulatory Agency (Badan Pengawas Perdagangan Berjangka Komoditi) recently passed Regulation No.5 of 2019 concerning Technical Provisions on the Operation of Crypto Assets Market in Futures Exchange, which allows virtual currencies to be legally traded as commodities. Moreover, the regulation defines relevant terms

such as crypto-asset exchange, crypto-asset clearing agencies, crypto-asset storage providers, as well as crypto-asset traders and clients. To this, the rule provides greater regulatory certainty and reflects the development of the regulatory framework concerning digital asset businesses.

Lao

Cryptoassets, like other FinTech products, are still in their development in Laos. Most financial transactions are still performed in cash¹⁵ in the country, and few people are conversant with technology. The BOL, the country's monetary authority, is very concerned about these instruments and has issued a warning about the risks of cryptocurrencies. There are no data on the number of local citizens who trade or deal with cryptocurrencies (or crypto assets in a broader sense).

While cash transactions are still preferred in the country among local citizens, it was reported in 2018 that certain businesses have started accepting cryptocurrencies as payment for products and services, as well as promoting cryptocurrency investing and trading.¹⁶ One IT services company even accepted donations in Bitcoin, Ethereum and ZeCash for the victims of the July 2018 dam-disaster flooding in Southern Laos.¹⁷

The first cryptocurrency exchange Laos, Vientiane Exchange Money, opened at the beginning of July 2018. This exchange offered the option to exchange Bitcoin with other currencies and claimed to possess the latest technology that will allow it to provide customers with the fastest transactions for all currencies it offers, even featuring an ATM machine for transactions.¹⁸

Similar to most countries across the globe, cryptocurrencies, on the other hand, are not recognized as legal tender in the country. The

¹⁵ Alex Kong, "The State of FinTech in Laos," yostartups, accessed July 30, 2019, <https://yostartups.com/the-state-of-fintech-in-laos/>.

¹⁶ "Bank of Laos Warns Public Against Use of Cryptocurrencies," *Laotian Times*, August 31, 2018, <https://laotiantimes.com/2018/08/31/bank-laos-warns-cryptocurrencies/>.

¹⁷ "Cryptocurrency Donate for Flooding in Southern Laos," Lao IT Dev, accessed July 30, 2019, <https://laoitdev.com/crypto-donation/>.

¹⁸ "First Certified Crypto Exchange In Laos Launches: Vientiane Exchange Money," *J&C Services*, June 13, 2018, <http://jclao.com/first-certified-crypto-exchange-in-laos-lau-nches-vientiane-exchange-money/>; "Laos Opens its First Certified Crypto Exchange," *CryptoCoin News*, June 19, 2018, <https://www.youtube.com/watch?v=CK1s3FTU03Y>.

Payment System Law restricts payment instruments other than cash to limited types of payment instruments.¹⁹ The terms “crypto assets”, “digital tokens”, and “distributed ledger technology” are also not defined in any existing laws and regulations.

Notably, shortly after the launch of the first cryptocurrency exchange in Vientiane, the BOL has issued a Notice on August 29, 2018 warning the public against the use of cryptocurrencies, citing Bitcoin, Ethereum and Litecoin as examples. It reminded the public that cryptocurrencies are not real currencies and should not be used for payments under the Law on Payment System. The BOL exhorts the Lao people to make an in-depth study prior to investing or purchasing these products. It warns of the significant risk attached, such as the potential for use in money laundering or the funding of terrorist activities, and also cautioned traders on the currency’s severe price volatility and potential to be offered as payment for fraudulent activities.²⁰ While the BOL’s Notice does not directly outlaw cryptocurrencies, it has stifled their active growth and adoption in the nation.

Interestingly, prior to the issuance of this Notice, a team of foreigners in Laos launched Bananacoin, which markets itself as the first environmentally friendly plantation in Laos with a utility token based on Ethereum that is backed by the market value of 1 kg of banana. Bananacoin is actually a combination of cryptocurrency and crowdfunding, with the team behind the project hoping to use the investment gained from the tokens to expand the land cultivated for bananas.²¹ The initial coin offering (ICO) has already ended, with 6,812,551 million tokens sold.²² However, it is not clear if this company holds any authorization from the BOL for holding of the ICO.

A crypto mining operator, Syan Technologies Limited of Hong Kong, was also reported to be in talks with the Lao Government for the set-up of a cryptocurrency mining facility on the banks of the Mekong river in

¹⁹ Article 14, Law on Payment System No. 32/NA (dated 7 November 2017).

²⁰ Notice No. 314/BOL on the Use and Exchange of Cryptocurrency (dated 29 August 2018).

²¹ “Whitepaper Bananacoin: Expansion of banana production in Laos with the help of crowdfunding,” bananacoin, accessed July 30, 2019, https://bananacoin.io/?utm_source=icobench.

²² Ibid.

November 2017,²³ but there has been no update on this potential project and the website of the said company does not appear to be active.

The Government does not appear to be veering away from its negative outlook on cryptocurrencies. With this outlook, coupled with the current state of FinTech development in Laos, cryptocurrency market growth in the country is expected to be slow and will continue to lag other nations in Southeast Asia. Lao authorities will have to recognize the potential of cryptocurrencies and the distributed ledger technology to develop policies and implement regulations that would foster the growth of cryptocurrencies while continuing to protect the public against the potential risks of this new technology.

Malaysia

Fundamentally, the Government of Malaysia realizes the potential of digital assets and blockchain technologies in various industries. In fact, the Finance Minister, Lim Guan Eng, noted that: “In particular, we believe digital assets have a role to play as an alternative fundraising avenue for entrepreneurs and new businesses, and an alternate asset class for investors”.²⁴ At the beginning of 2019, the SC issued the framework for crypto exchanges, which states that the new framework will fall under the purview of its Guidelines on Recognized Markets. In accordance with the same guideline, there is the amendment of a section to introduce new requirements for crypto exchanges. Specifically, under the regulation²⁵ all Digital Asset Exchange (DAX) Operators must be locally incorporated and have a minimum paid-up capital of RM 5 million. A DAX Operator

²³ “Syan Mining Project latest: deal struck with Laos PDR government and location for forthcoming cryptocurrency mining facility identified,” *Open Development Mekong*, October 30, 2017, <https://opendevopmentmekong.net/announcements/syan-mining-project-latest-deal-struck-with-laos-pdr-government-and-location-for-forthcoming-crypto-currency-mining-facility-identified/#!/story=post-7601904&loc=20.0171109,103.378253,7>; “Syan Technologies in talks with Laos PDR government to deploy hydroelectric-powered cryptocurrency mining facility,” *Digital Journal*, 2017, <http://www.digitaljournal.com/pr/3512518>.

²⁴ “Law on Digital Currency Effective Tuesday, Says Guan Eng”, *The Star Online*, January 14, 2019, <https://www.thestar.com.my/business/business-news/2019/01/14/law-on-digital-currency-effective-tuesday-says-guan-eng/>.

²⁵ *Ibid*.

is prohibited from providing financial assistance both in direct and indirect forms to investors, including its officers and employees, to investor trade in Digital Assets on its platform. A DAX Operator shall gain the approval from the SC of the trading of the digital asset before facilitating such trading. The requirements further state that an internal audit function must be established by a DAX Operator in order to design, execute, and maintain an internal audit framework that is suitable for the company's business and operations. In addition, there is also a requirement concerning which currencies are allowed to be used and invested on its platforms.

Anyone interested in starting a digital asset platform was needed to apply to the SC to be registered as a recognized market operator by March 1, 2019, under the new rules. Anyone who conducts unlicensed initial coin offerings (ICOs) or digital asset exchanges risks a 10-year jail term and an RM 10 million punishment, according to the new rules. Consequently, the guidelines for ICOs were released in March 2019.

Singapore

Back in 2017, according to the MAS, the use of virtual currencies is not prevalent in Singapore, with just around 20 merchants accepting Bitcoins at the moment.²⁶ Furthermore, the usage of virtual currencies (or “digital tokens”) as a form of payment in the financial sector is limited, and crypto-asset trading is mostly used for speculative investment reasons. Financial institutions, on the other hand, acknowledge that the digital token market is gaining traction.

This ecosystem, which includes “trading platforms, brokers, and wallet providers”,²⁷ may be outside the purview of authorities. While there is no specific legislation to oversee crypto-asset operations in Singapore at the

²⁶ “Reply to Parliamentary Question on the prevalence use of cryptocurrency in Singapore and measures to regulate cryptocurrency and Initial Coin Offerings,” Monetary Authority of Singapore, accessed October 3, 2017, <https://www.mas.gov.sg/news/parliamentary-replies/2017/prevalence-use-of-cryptocurrency>.

²⁷ “Emerging digital token ecosystem draws regulators’ eye,” November 29, 2018, *Straits Times*, <https://www.straitstimes.com/business/emerging-digital-token-ecosystem-draws-regulators-eye>.

moment, many existing laws may be applicable. Furthermore, the formation of organizations like the Token Economy Association (“TEA”)²⁸ demonstrates MAS’ commitment to the growth of this new sector. TEA also can be seen as a self-regulatory organization.

The regulatory body in charge of this sector, MAS, has adopted a cautious approach to cryptocurrencies.²⁹ The primary motivations of Singaporean authorities’ response to crypto-asset operations have been to provide consumer protection, maintain financial stability and unleash technological innovation. The role of “digital tokens” has developed beyond that of a virtual currency, according to MAS, and may now reflect ownership or a security interest in an issuer’s assets or property, as well as a debt owing by an issuer. The Commercial Affairs Department is also responsible for rule enforcement and consumer protection (CAD). Unless exempted, issuers and intermediaries of digital tokens would be subject to licensing requirements under the Securities and Futures Act (“SFA”) and the Financial Advisers Act (“FAA”), as well as anti-money laundering and counter-terrorist financing regulations.³⁰

In 2018, the TEA,³¹ an industry-sponsored self-regulatory organization, was established with the mission of monitoring digital tokens like as bitcoin and developing effective methods to govern the sector. The TEA is presently collaborating with the Association of Crypto-Currency Enterprises and Start-ups Singapore to develop a code of conduct that will include anti-money laundering, counter-terrorism funding and due diligence processes (for identity authentication).³²

²⁸ See Token Economy Association, <http://teasingapore.org/about-us/>.

²⁹ “MAS cautions against investments in cryptocurrencies,” *Monetary Authority of Singapore*, December 19, 2017, <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-cautions-against-investments-in-cryptocurrencies.aspx>.

³⁰ “A Guide to Digital Token Offerings,” Monetary Authority of Singapore, accessed October 15, 2021, <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf>.

³¹ “MAS cautions against investments in cryptocurrencies,” *Monetary Authority of Singapore*, Dec 19, 2017, <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-cautions-against-investments-in-cryptocurrencies.aspx>.

³² *Ibid.*

In addition, regarding blockchain technology, the managing director of MAS stated that the technology has great potential for making trade finance safer and more efficient, and praised DBS Bank, Standard Chartered Bank, HSBC and Bank of America for their accomplishments.³³ Project Ubin and the Global Trade Connectivity Network are two initiatives that MAS has pursued in the last year with the goal of using blockchain and Digital Ledger Technology (“DLT”).

To be more specific, in terms of relevant regulatory framework, the varied features of digital assets, from security to non-security tokens, lead to complexities from a regulatory standpoint. A token’s legal status depends on its main function or the type of token being considered; accordingly, the tokens’ categories are helpful for capturing the complexities of digital assets and to guiding effective regulatory responses. In other words, the complexity of the structure of digital assets has led to concerns from regulators and all relevant stakeholders, such as consumer risk and money laundering concerns. It is necessary to understand the core concepts and features of the main types of crypto assets in order to understand the regulatory and supervisory implications.

As a result, for example, if the crypto assets or digital assets has the attributes of a capital market product. The Securities and Futures Act shall be applied to the case. According to the Act, capital market products include securities, units in a collective investment scheme (CIS), over the counter (OTC) derivatives, etc. However, if the crypto assets has the attributes of a commodity, the Commodity Trading Act³⁴ is the key legislation.

It should be noted that different entities have different approaches to the labelling of different categories of crypto assets; however, most entities share the common consideration that the categorization of crypto assets shall rely on their main functions and features. From the hybrid features of a number of tokens in the market, the classification of such crypto assets is not always as straightforward as has been proposed by the

³³ “Singapore FinTech Journey 2.0 – Remarks by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Singapore FinTech Festival on 14 November 2017”, Monetary Authority of Singapore, accessed October 20, 2021, <http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2017/Singapore-FinTech-Journey-2.aspx>.

³⁴ See The Commodity Trading Act, <https://sso.agc.gov.sg/Act/CTA1992>.

research team at the Cambridge Centre for Alternative Finance, University of Cambridge.³⁵ This is similar to what was addressed in the report by the International Monetary Fund (IMF), which noted that “the definition is far from globally uniform...”.

Thailand

Digital assets have been used as fundraising instruments and mediums of exchange in Thailand without laws or regulations to regulate these activities. This led to concerns from the Thai government authorities as well as key regulators about the potential impact of the activities on national financial stability and public risk.

The Thai SEC published a statement on ICO in September 2016 that highlighted many of the concerns regarding ICO abuse, public dangers and cyber security-related problems; nevertheless, the Thai SEC said that ICO has the potential to be an alternate method of financing, particularly for digital start-ups. As a result, the Thai Securities and Exchange Commission was contemplating a suitable regulatory strategy for ICO operations.

The Thai SEC is the main authority supervising and considering all matters relating to digital asset businesses, including both digital currency- and ICO-related activities.

To address concerns about the potential risks of using digital assets, the Royal Decree on the Digital Asset Businesses B.E.2561 (2018) was enacted to regulate the offering of digital assets and the undertaking of digital asset businesses, which were categorized into three main types: (i) Digital Asset Exchanges; (ii) Digital Asset Brokers; and (iii) Digital Asset Dealers.³⁶ In addition, further to considering the Royal Decree, business operators shall comply with the rules, conditions and procedures specified in the notification of the Thai SEC, as well as the notification of the Ministry of Finance of Thailand concerning sufficient sources of capital and other requirements. For instance, the required paid-up registered capital for the ICO portal operator is 5 million Thai Baht. In addition, for key definitions that capture the scope of law application, digital assets

³⁵ “Legal and Regulatory Considerations for Digital Assets,” Cambridge Centre for Alternative Finance, accessed March 30, 2021, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>.

³⁶ See Section 3 of the Royal Decree on the Digital Asset Businesses B.E.2561 (2018).

under the Royal Decree can fall within the scope of cryptocurrencies or digital tokens.³⁷

In summary, the Royal Decree, along with the subordinate legislation, provides a licence requirement for restricted activities related to digital assets.

Regarding the legal status of digital assets, in Thailand, in accordance with the Currency Act B.E.2501, Section 6 of the Act stipulates that Thai currency consists of coins and notes. Furthermore, Section 7 of the Act adds that the official unit of currency is “Bath”. Thus, this Act limited the definition of “currency” under the Thai legal system to two forms, comprising coins and notes. The Act became effective in 1958. Around 60 years ago, at the time of its enactment, there were still limitations in terms of the available form of money circulating in the market. In addition, Section 9 of the Act prohibits any person from performing certain activities in relation to money without authorization, with exceptions granted by the Ministry of Finance. To conclude, the Act does not recognize virtual currency as Thai currency, and therefore it cannot be regarded as a legal tender under Thai laws.

However, although virtual currency is not a legal tender under the Currency Act of Thailand, for both parties, an obligation can be extinguished if the creditor accepts a virtual currency for payment transactions instead of the official one.

Crypto Baht—Project Inthanon Initiative

Project Inthanon is the recent initiative launched by the Bank of Thailand in collaboration with commercial banks; it is a wholesale digital currency issued with the purpose of facilitating interbank settlements.

“These efforts should pave way for faster and cheaper transaction and validation due to less intermediation processes needed compared to the current systems”, stated by Dr. Veerathai Santiprabhob, Governor of the Bank of Thailand in his “Thai Economy: The Current State and the Way Forward” speech.³⁸ This can also reflect the attempt of the Bank of Thailand to exploring new technologies such as Blockchain to improve its operation.

³⁷ See Section 3 of the Royal Decree on the Digital Asset Businesses B.E.2561 (2018).

³⁸ “Thai Economy: The Current State and the Way Forward, Key Note Address by Dr. Veerathai Santiprabhob”, the Bank for International Settlements, accessed July 30, 2019, <https://www.bis.org/review/r180606g.pdf>.

Vietnam

In accordance with Decision No. 1255/QĐ-TTg,³⁹ dated August 21, 2017, the Deputy Prime Minister appointed the Ministry of Justice to lead and coordinate with the SBV in completing the legislative framework on the administration of virtual assets, digital currencies and virtual money. Despite experts' warnings about its hazards and the absence of a management structure, Bitcoin gained substantial market interest in Vietnam. The Ministry of Justice is currently evaluating existing regulations in Vietnam regarding the administration of virtual assets and currencies.

As such, there have been some mixed opinions with regard to the management of virtual currencies, especially Bitcoin or Litecoin. Previously, on October 30, 2017, the SBV stated that virtual currencies are not a lawful means of payment, and that therefore, "from January 1, 2018, the act of issuing, providing and using illegal means of payment (including Bitcoin and other similar virtual currency) may be subject to prosecution in accordance with the provision of Article 206 of the Penal Code 2015", as conveyed in the SBV's statement released on October 28, 2017. However, illegal transactions using Bitcoin continue.⁴⁰

In the past, there was discussion surrounding new legislation that would pave the way for a wider economic upheaval that would attempt to tax Bitcoin as a digital asset in the foreseeable future, but cryptocurrencies have yet to be declared an asset or currency. The central bank invoked *Article 4.6 of Decree 101 of 2012 on non-cash payment*; however, current laws have not yet specified whether Bitcoin is a currency or a commodity or payment instrument, which means that Bitcoin trading services are not recognized as payment processing services, and therefore the new decree does not apply to crypto exchanges and traders. As stated by Deputy Prime Minister Vuong Dinh Hue, most cryptocurrency transactions are now related to investment or speculation, not as a medium for

³⁹ Decision no. 1255/QĐ-TTg (dated August 21, 2017), <https://thuvienphapluat.vn/van-ban/EN/Thuong-mai/Decision-1255-QĐ-TTg-scheme-completion-legal-framework-management-virtual-assets-digital/362201/tieng-anh.aspx>.

⁴⁰ "Vietnamese Government pushes legal framework in dealing with Bitcoin", *Hanoi Times*, January 7, 2018, <http://www.hanoitimes.vn/science-tech/2018/01/81e0bff2/vietnamese-government-pushes-legal-framework-in-dealing-with-bitcoin/>.

trade or paying for services.⁴¹ As a result, the Vietnamese government will continue to research and keep up with the latest advancements in cryptocurrencies. The Ministry of Justice has also surveyed the development of cryptocurrencies in Vietnam and abroad in order to analyse the pros and cons of the examined trends. This analysis will form the basis for further consideration by the Vietnamese government.

ASEAN GENERAL OVERVIEW OF LEGISLATIVE EFFORTS ON DIGITAL ASSET BUSINESS REGULATIONS

To summarize, Southeast Asian central banks have taken a cautious stance on the rise of virtual currencies in terms of their potential risks to the public. Also, there are no laws and regulations in any countries designed to regulate cryptocurrencies themselves; however, there are laws, regulations and guidelines in many countries issued to regulate the activity that surrounds virtual currencies, as well as digital tokens. To this extent, cryptocurrencies are not recognized by the laws of any countries in Southeast Asia as legal tender. However, cryptocurrencies exchange platforms, as well as platforms to facilitate ICO activity, are permitted in some countries through the newly issued regulations/guidelines, along with the securities laws.

To be more specific, different countries have different ways to regulate ICO and cryptocurrency exchanges. To this extent, the main approaches can be identified—the first applies ICO/cryptocurrency-related activity to the existing securities Law. This can be seen in Singapore, where there are currently no bespoke regulations to supervise crypto-asset-related activities, although several existing regulations may apply. The second is applying newly issued laws/regulations to these activities.

However, these two approaches are generally similar in terms of the requirements set for both cryptocurrency exchanges and ICO platforms. For example, under the Royal Decree on Digital Asset Businesses of Thailand, the Royal Decree sets out requirements for an operating licence the platforms must obtain to legally conduct their activities if digital tokens/cryptocurrencies fall within the scope of the outlined restrictions (security token). This is similar to what is prescribed in the Securities

⁴¹ Thanh Le, “No Legalizing Bitcoin, Vietnam Says”, *VNExpress*, June 29, 2018, <https://e.vnexpress.net/news/business/no-legalizing-bitcoin-vietnam-says-3770123.html>.

Law of Singapore (the Securities and Future Act (SFA)) for the requirement with regard to capital market products (Section 2(1) of the SFA)⁴² and the CMS licence. To this extent, with regard to the regulatory approach to ICOs/cryptocurrency exchanges in Singapore, the Securities and Future Act (SFA) is the governing law to be considered along with a guideline issued by MAS. To be more specific, MAS expressed that if digital tokens traded on any digital token exchange platforms are securities, future contracts or other types of capital market products under Section 2(1) of the SFA, the exchanges must receive authorization from MAS before acting as platforms to accommodate such activity.⁴³

However, there are also differences under Thai and Singapore regulations. This can refer to the sixth case study given in the Guide to Digital Token Offerings issued by MAS, that a virtual currency exchange platform that wishes to allow users to exchange virtual currencies to fiat currencies is currently not regulated by MAS.⁴⁴

In Malaysia, the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 came into force on January 15, 2019. This order set an authorization requirement for digital asset platform operators. In particular, the Malaysia SC requires a digital asset platform to apply to the SC to be registered/authorized under the revised guidelines. However, with regard to ICOs, MS stated that the guidelines for ICOs will be issued by the end of Q1 of 2019.⁴⁵

At present, other ASEAN countries, namely Brunei, Indonesia, Laos, Myanmar and Vietnam, still have no laws and regulations specifically designed to regulate either cryptocurrency exchange platforms or platforms for ICO-related activity; however, regulators in these countries may apply existing relevant regulations in such cases. Of these countries, there are also attempts to find proper regulatory approaches to address this

⁴² The Securities and Future Act (Chapter 289), <https://sso.agc.gov.sg/Act/SFA2001>.

⁴³ The Securities and Future Act (Chapter 289), <https://sso.agc.gov.sg/Act/SFA2001>.

⁴⁴ A Guide to Digital Token Offerings, <http://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov.pdf>.

⁴⁵ “Media Statement on Implementation of Digital Assets Prescription Order”, *Securities Commission of Malaysia*, January 17, 2019, <https://www.sc.com.my/news/media-releases-and-announcements/media-statement-on-implementation-of-digital-assets-prescription-order>.

development of technology; for instance, in Vietnam, the Ministry of Justice is reviewing existing laws on the management of virtual assets and currencies in the country.

To summarize, cryptocurrencies are not recognized by the law of any Southeast Asian countries as legal tender. However, cryptocurrency exchange platforms, as well as platforms to facilitate ICO activity, are permitted in some countries through the newly issued regulations/guidelines and/or the Securities Law.

CONCLUSION

Digital technology diffusion requires sufficient infrastructure, a thriving entrepreneurial ecosystem, and a favourable legal and regulatory framework. Many countries in ASEAN have put in place a fundamental digital infrastructure to support their digital economy. The presence of digital entrepreneurs can encourage the adoption of digital technologies by driving down costs and raising quality, reinforcing market demand (for example, via intelligent automation, cloud technology, or software as a service), and putting pressure on incumbents to keep up. The digital innovation ecosystem in emerging or less-developed nations, on the other hand, is still small in contrast, with just a few local and international digital solution companies compared to the size of the countries' economies. For instance, compared to its regional counterparts, Thailand exhibits relative underdevelopment in five complex B2B sectors, indicating considerable potential. Mobility tech, big data and analytics, health tech, digital media and entertainment tech are some industries. There are several explanations for Thailand's limited funding flow into these industries.

Regarding regulatory constraints, overall, for ASEAN member states, lacking regulatory support and over-regulation problems are two of the main issues that regulators should take into account when regulating FinTech businesses. Lessons learned from different jurisdictions reflect these two problems in various FinTech companies. Many of Southeast Asian countries have an innovation-stifling environment with high regulatory compliance costs, poor de-facto enforcement, and a vicious cycle of heavy regulation due to their view of excessive risks in the digital ecosystem.

While regulators in Southeast Asian countries are receptive to emerging financial services technologies, poor infrastructure has undoubtedly obstructed them in supporting FinTech in practice.

In addition, for regulators in Southeast Asia that have put effort into addressing such technology developments, the regulatory environment in some countries is still not sufficient to support this. For instance, the Know Your Customer (KYC) regulations in many countries are still limited to face-to-face identity verification, which does not correspond to FinTech business models. The different standard of data protection is another concern for regulators due to some categories of FinTech businesses being necessary to deal with the cross-border transfer of data, which creates difficulty for such businesses if the standard of data protection between two (or more) countries is not the same. This also reflects regulatory harmonization challenges at the regional level.

On the other hand, it is also possible for a country that issued bespoke regulations to over-regulate FinTech businesses if they cannot set the optimal balance between market simulation and risk management.

To conclude, regarding digital assets (and central bank digital currencies (CBDCs) which is a part of digital assets) regulations, one of the most significant issues confronting domestic regulatory approaches on digital assets is that various authorities have differing attitudes on the usage of cryptocurrencies. These conflicting positions, as well as a lack of communication among various organizations, may pose challenges in the usage and oversight of cryptocurrencies.

For example, several countries have their own legislation for ICOs; nonetheless, it remains difficult for authorities to give clear-cut guidance and/or subordinate regulations, such as the criteria for distinguishing utility and security tokens.

Furthermore, additional difficult legal concerns for which there is yet no legislative backing, such as the validity of so-called “smart contracts” and law enforcement or the seizure of cryptocurrencies, may develop as a result of aspects of digital assets and DLT.



Cryptocurrency, Stablecoins, and Blockchain

Pawee Jenweeranon

INTRODUCTION

The varied features of digital assets, from security to non-security tokens, lead to complexities from a regulatory standpoint. A token's legal status depends on its main function or the type of token being considered; accordingly, the tokens' categories are helpful for capturing the complexities of digital assets and to guiding effective regulatory responses. In other words, the complexity of the structure of digital assets has led to concerns from regulators and all relevant stakeholders, such as consumer risk and money laundering concerns.

The main focus of this chapter is to differentiate “crypto assets” from “digital assets” in the blockchain ecosystem. With respect to this, for the reason that there are many terms that are used interchangeably, it should be emphasized that this chapter analyses “crypto assets” as a subset of “digital assets”; “digital assets have a broader definition than “crypto assets”, “digital tokens”, “private digital tokens”, or “cryptocurrencies”.

P. Jenweeranon (✉)
Thammasat University, Bangkok, Thailand
e-mail: paweejen@tu.ac.th

This chapter aims to catalogue the main types of crypto assets in the market as is necessary for the regulatory analysis that follows in later chapters. This is because the analysis in the subsequent chapters aims to identify regulatory gaps. Hence, it is important to understand the arrangements of such assets, which could otherwise fall outside the scope of existing legal and regulatory frameworks. For example, in order to understand the characteristics of crypto assets referencing one fiat currency, it is necessary to differentiate this type of crypto asset from electronic money and to correspondingly propose sound regulatory responses. Accordingly, the chapter classifies types of digital assets according to their functions, features, creation, and initial distribution.

In general, all related terms, from digital assets, to crypto assets, to cryptocurrencies, have been differentially defined from one country to another. Moreover, in some states, the existing taxonomies of these terms have failed to fully capture the terms' relevant features.¹ It is therefore necessary to differentiate the scope of all of these terms, as this will be helpful for capturing the proper regulatory responses. In addition to this, regulations, government documents, and working papers, as well as research/industry reports that describe these terms will be discussed.

To exemplify this, the relevant terms are defined in the Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, in particular, in which “crypto-asset” is broadly defined as a digital representation of value or rights that utilizes distributed ledger technology or similar.² This is similar to the Cambridge Centre for Alternative Finance, which draws a clear distinction between two key terms, namely digital assets and crypto assets. In particular, the novel characteristics of crypto assets make them differ from digital ones. These distinct characteristics include the non-necessity

¹ “Legal and Regulatory Considerations for Digital Assets,” Cambridge Centre for Alternative Finance, accessed June 30, 2021, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>.

² Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>, p. 17.

of a formal issuer and the incentive model derived from its underlying distributed ledger technology.³

The Financial Conduct Authority (FCA) of the UK also specified in their guidance on crypto assets that there is no universal definition for the term; however, the FCA considered crypto assets to be “a cryptographically secured digital representation of value or contractual rights”. The definitions can reflect the similar ways of interpretation of the term crypto assets, in that all the interpretations highlighted the use of cryptographic techniques. Furthermore, apart from the common way of interpretation, it should be noted that some propose that the term crypto assets should be defined as widely as possible. This is to cover all types of crypto assets in the market.⁴

The emergence of the crypto asset concept led to widespread discussions of regulatory support mechanisms. This is because its characteristics can be complex and different from regulated substances within the scope of existing regulatory frameworks. Accordingly, this chapter aims to explore the different features of the main types of crypto assets or blockchain-based digital assets in the market. The chapter does not cover all types of digital objects or assets, such as in-game objects. Additionally, it should be noted that this chapter does not cover the so-called Central Bank Digital Currencies (CBDCs). The Bank of International Settlement also states that CBDCs differ from crypto assets in general,⁵ whereas others might consider CBDCs a type of crypto asset or price-stable forms thereof.⁶

To briefly summarize, many countries still lack a clear regulatory basis for certain types of crypto assets due to their complicated structure. To supplement, according to existing regulatory frameworks, crypto assets

³ “Legal and Regulatory Considerations for Digital Assets,” Cambridge Centre for Alternative Finance, accessed June 30, 2021, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>.

⁴ Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>, p. 17.

⁵ “Statement on Crypto Assets,” Bank of International Settlement, accessed June 30, 2021, https://www.bis.org/publ/bcbs_nl21.htm.

⁶ “EC Consultation Paper: An EU Framework for Markets in Crypto Assets,” BARCLAYS, accessed June 30, 2021, <https://home.barclays/content/dam/home-barclays/documents/citizenship/ESG/EC-CP-EU-Framework-for-Markets-in-Crypto-assets.pdf>.

may not be possible to consider as fiat money.⁷ This is because existing legislation remains narrow with respect to the definition of state currency, as well as some crypto assets having an unstable price or value. With respect to this, crypto assets may fall within the terminology of property referring to the legal statement proposed by the UK Jurisdiction Taskforce of Lawtech⁸; however, a regulatory basis continues to lack in many other countries.

GENERAL DEFINITION: INTERNATIONAL AND DOMESTIC DIALOGUES

As noted earlier, there are many approaches to classifying the types of crypto assets in the market. The general classification should be financial and non-financial asset-type crypto assets. To this, as per the general definitions provided, crypto assets constitute an umbrella term that includes various kinds of sub-categories. To better understand the outline of crypto asset classifications, this thesis explores the ways in which crypto assets are categorized by international organizations. This is because standard-setting by these may be helpful in identifying the most suitable structure within the scope of this study.

The European Commission classifies crypto assets into three main types—utility tokens, asset-referenced tokens, and E-money tokens. The European Commission also differentiates different types of crypto assets in its Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets and amending Directive (EU) 2019/1937 (MiCA).⁹ However, the European Banking

⁷ “Report with Advice for the European Commission on Crypto-assets,” European Banking Authority, accessed June 30, 2021, <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5cd880684/EBA%20Report%20on%20crypto%20assets.pdf>, p. 12.

⁸ “Legal Statement on Cryptoassets and Smart Contract,” The LawTech Delivery Panel, accessed June 30, 2021, https://35z8e83mlih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf.

⁹ “Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937 (MiCA),” European Commission, accessed June 30, 2021, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/200924-presentation-proposal-crypto-assets-markets_en.pdf.

Authority (EBA) provides a taxonomy of crypto assets that includes payment/exchange/currency tokens, investment tokens, and utility tokens.¹⁰ It is interesting to note that the European Central Bank developed the so-called crypto cube to identify different classes of crypto assets. The crypto cube assessment focuses on certain criteria, such as the existence/absence of the issuer, the decentralization/centralization of responsibilities and what underpins the value of such assets.¹¹

The International Organization of Securities Commissions (IOSO) cited three main types of crypto assets, namely security, utility and payment/exchange/currency tokens. However, the IOSO emphasizes that a case-by-case assessment is needed. This reflects the fact that a clear distinction for various types of digital tokens may need to come with the assessment guidelines, as it could be difficult to ascertain consistency when exercising discretion.¹²

On the other hand, private sector actors may consider classes of crypto assets differently than those given by international entities. The types can be identified as payment tokens (such as cryptocurrencies), financial asset tokens, and consumer tokens.¹³

It should be noted that different entities have different approaches to the labelling of different categories of crypto assets; however, most entities share the common consideration that the categorization of crypto assets shall rely on their main functions and features. From the hybrid features of a number of tokens in the market, the classification of such crypto assets is not always as straightforward as has been proposed by the research team

¹⁰ “Report with Advice for the European Commission on Crypto-assets,” European Banking Authority, accessed June 30, 2021, <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf>, p. 12.

¹¹ Dirk Bullmann, Jonas Klemm, and Andrea Pinna, *In Search for Stability in Crypto-assets: Are Stablecoins the Solution?*, Occasional Paper Series, European Central Bank, accessed June 30, 2021, <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230-d57946be3b.en.pdf?321f6bf14960e6f604725be5a466957b>, p. 9.

¹² “Investor Education on Crypto-Assets,” The International Organization of Securities Commissions, accessed June 30, 2021, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD668.pdf>.

¹³ “Cryptocurrencies and Tokens,” ING, accessed June 30, 2021, https://www.ecb.europa.eu/paym/groups/pdf/fxcg/2018/20180906/Item_2a_-_Cryptocurrencies_and_tokens.pdf.

at the CCAF.¹⁴ This is similar to what was addressed in the report by the International Monetary Fund (IMF), which noted that “the definition is far from globally uniform...”.

To exemplify this, the complexation of crypto asset characteristics can be seen in the arrangement of the so-called stablecoins, which are a subtype of crypto asset. In particular, a stablecoin is a type of crypto asset that features some stabilization mechanisms. However, the term stablecoin lacks a universal definition.¹⁵

According to the publication of the European Central Bank (ECB), stablecoins can be classified into fiat-backed stablecoins (tokenized funds). Tether, which is the oldest and most utilized stablecoin, represents this type. The second type is collateralized stablecoins, or collaterally backed stablecoins that differ from tokenized funds or fiat-backed stablecoins, as this type of stablecoin is backed by assets. There are also other types of stablecoins that will be discussed herein, such as off-chain collateralized stablecoins, on-chain collateralized stablecoins, and algorithmic stablecoins.

At the domestic level, in terms of crypto asset classification, many countries prioritize the assets’ main characteristics and economic purpose as their main considerations. For instance, FINMA classifies crypto assets into three main types—payment, utility, and asset tokens.¹⁶ However, it also identifies the existence of hybrid tokens.¹⁷

It is necessary to understand the core concepts and features of the main types of crypto assets in order to understand the regulatory and supervisory implications. This study aims to propose an accommodative framework that potentially fills existing regulatory gaps. The framework should be helpful in supporting asset tokenization in relevant industries.

¹⁴ “Legal and Regulatory Considerations for Digital Assets,” Cambridge Centre for Alternative Finance, accessed June 30, 2021, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>.

¹⁵ Dirk Bullmann, Jonas Klemm, and Andrea Pinna, *In Search for Stability in Crypto-assets: Are Stablecoins the Solution?*, Occasional Paper Series, European Central Bank, accessed June 30, 2021, <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230-d57946be3b.en.pdf?321f6bf14960e6f604725be5a466957b>, p. 9.

¹⁶ “Development in FinTech,” FINMA, accessed June 30, 2021, <https://www.finma.ch/en/documentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/>.

¹⁷ *Ibid.*

Accordingly, it is important to analyse samples of crypto assets in the market in order to understand their arrangements.

BASIC CHARACTERISTICS OF CRYPTO ASSETS

Tokens are the general term for value units in a blockchain system. There were about 11,000 distinctive kinds of tokens by the end of 2021.¹⁸ Conceptually, this segment classifies crypto assets in the market into specific types—security, utility, payment/currency, and hybrid tokens. Accordingly, the selection of tokens in this section is based on different features of each token that represent different arrangements. This part does not cover all possible types of crypto assets in the market; however, the analysis of certain types of tokens would help illuminate the complex arrangements of crypto assets that lead to regulatory concerns.

To this, this section adds the basic principle of key factors, including money, currency, and securities in brief. The outline constitutes a framework for analysing the arrangements of selected crypto assets or tokens that could be helpful for regulatory analysis in the following chapters. This section will further address general explanations of the various categories of tokens.

Money/Currency Characteristics

A currency typically performs, or should fulfil, three fundamental functions, known as primary monetary functions in the terminology of monetary theory¹⁹: (1) The medium of exchange function: A currency is a means of exchange that facilitates the exchange of goods and services. (2) Store of value function: A currency acts as a store of value, allowing its worth to be preserved for an indefinite length of time. (3) Unit of account function: A currency is a unit of account that may be used to represent the value of a product or service.

Additionally, it is possible to derive additional characteristics of currencies based on the three primary monetary functions, which are referred to as secondary monetary functions. On the one hand, these define the

¹⁸ CoinMarketCap, available at <https://coinmarketcap.com/>.

¹⁹ Ali, Barrdear, Clews, and Southgate, “Innovations in Payment Technologies and the Emergence of Digital Currencies” (2014) 54(3) *Bank of England Quarterly Bulletin*, 276 (278).

features of a currency in greater depth, but they are also essential to the basic monetary functions to be fulfilled. Furthermore, supplementary monetary functions offer a more accurate assessment of crypto assets in terms of the currency question.

For instance, to this, it is beneficial in the short run and essential in the long term for a currency to be simple to handle and highly transportable for it to have utility as a method of payment. This is especially true for transactions involving significant sums of money or a large number of currencies. Ease of handling and transportability are particularly important for transactions that take place across great distances.

Another prerequisite—at least on a local or regional level—is widespread currency adoption in business and, more broadly, amongst the public. Only if a significant number of places accept the currency in return for products, services, or debt settlement will it eventually fulfil its role as a means of payment. A (positive) network externality or network effect is a term used in economics to describe this occurrence.²⁰ The greater the advantage for all network members, the larger the (currency) network. Only when a sufficient number of network participants are present²¹—in the case of a currency, the number of people and businesses who accept it—does the currency meet the above-mentioned criteria for acting as a means of exchange and payment.

Furthermore, in order to fulfil the store-of-value purpose, a currency must exhibit price stability in addition to physical or digital storage and durability criteria. The value of the currency should therefore only vary to a limited degree over time, with minor inflationary (reduction in value and therefore a decrease in buying power) or deflationary (increase in value and thus an increase in purchasing power) tendencies. The population's belief that a currency's future buying power will be essentially the same as today's lies at the heart of the store-of-value function. Confidence in a currency may rapidly deteriorate if the store-of-value function is not met, as is the case in periods of hyperinflation. As a result, the other two

²⁰ Oz Shy, *The Economics of Network Industries* (2001), 3 (187 et seq.); Michael L. Katz and Carl Shapiro, "Technology Adoption in the Presence of Network Externalities" (1986) 94(4) *Journal of Political Economy*, 822 (823 et seq.).

²¹ The critical network size for this can be considerable; see Oz Shy, *The Economics of Network Industries* (2001), 104, 113.

monetary functions—medium of exchange and unit of account—will be only partially fulfilled.

Price stability, on the other hand, is not only essential for the store-of-value function but also plays a crucial role in the performance of the unit of account function. Indeed, if the currency’s price volatility necessitates regular price changes in order to guarantee an accurate representation of value, displaying the pricing of goods and services in units of this currency only makes limited sense. It is also debatable whether displaying pricing in this currency is helpful if it is not commonly used and only has limited acceptability.

A currency’s fungibility is a crucial condition for performing the value-measuring function, in addition to characteristics such as high acceptability and price stability. In this sense, fungibility refers to the characteristic that any physical or digital unit of a currency has the same nominal value as any other unit of the same currency. This means that variations in individual currency units, such as age or past owners, have no effect on their value. A fungible form of money, in other words, is memoryless. If a money is not fungible, it requires a lot more work to utilize it as a unit of account. In order to estimate the value of a given set of currency units, for example, one must not only count the quantity of the currency units provided but also identify the additional value-determining dimensions and account for these appropriately. A currency whose fungibility cannot be guaranteed is only appropriate to a limited degree for use as a unit of account or for assessing the value of other things, as this entails significant search and transaction costs.

Additionally, it should be worth considering that, as of today, many currencies have no or just a very low underlying (material) value that differs significantly from their nominal one. As a result, a fiat currency’s value is solely determined by the advantages generated by the monetary functions specified above. To put it another way, a currency must not have an intrinsic value in undertaking monetary functions.

Security Characteristics

To determine whether such crypto assets shall be regarded as securities or not, this section explores some common features of securities by referring to some selected countries’ regulatory frameworks. The question of whether the crypto asset constitutes a “security” under those regulations is a critical one.

To exemplify this, this section briefly analyses US federal securities laws. An “investment contract”, as well as other instruments such as stocks, bonds, and transferable shares, are all considered “securities”. A crypto asset should be examined to determine whether it contains the features of any product that satisfies the federal securities laws’ definition of a “security”. The *Howey* decision and subsequent case law of the United States Supreme Court have determined that an “investment contract” arises when money is invested in a joint business with a reasonable expectation of benefit accruing from the efforts of others.²²

Moreover, the SEC released a “Framework for ‘Investment Contract’ Analysis of Digital Assets” on April 3, 2019, in an effort to offer clarification.²³ This approach is encouraging, as it demonstrates that the Securities and Exchange Commission is prepared to exclude some blockchain-based digital assets from being regarded as securities. Although the advice is an improvement over the abysmal uncertainty that currently exists in this area, it is no replacement for unambiguous law and court decisions. According to the above-mentioned framework, the key question when applying the *Howey* test to a digital/crypto asset is whether the buyer has a reasonable expectation of profit (or other financial rewards) arising from the labour of others. Participating in dividends or other means of achieving asset appreciation, such as selling at a profit in the secondary market, may be expected to provide a return to a buyer.²⁴ The “economic reality”²⁵ of the transaction, as well as “what character the instrument is given in commerce by the terms of the offer, the plan of distribution, and the economic inducements held out to the prospect”, are all relevant to this investigation.²⁶ As a result, the analysis is objective, focusing on the transaction itself and how the digital/crypto asset is offered and

²² SEC v. W.J. *Howey* Co., 328 U.S. 293 (1946) (“*Howey*”).

²³ “Framework for “Investment Contract” Analysis of Digital Assets,” U.S. Securities and Exchange Commission, accessed June 30, 2021, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_cdnref9.

²⁴ *Ibid.*

²⁵ SEC v. W.J. *Howey* Co., 328 U.S. 293 (1946) (“*Howey*”).

²⁶ SEC v. CM Joiner Leasing Corp, 320 U.S. 344 (1943) at 352–53.

sold.²⁷ To this, relevant laws and regulations will be discussed herein in the subsequent chapters.

It is worth pointing out that “reasonable expectation of profits” is a key characteristic of “securities” subjected to the Howey test.²⁸ In the case of crypto assets, when assessing one, it is important to evaluate if there is a realistic expectation of profit. Profits may include, for example, capital appreciation from the growth of the original investment or commercial operation, as well as a share of profits from the use of buyers’ money.²⁹ The Howey test does not regard price appreciation resulting simply from external market factors (such as general inflationary trends or the economy) that affect the supply and demand for an underlying product to be “profit”. This is significant in assessing security characteristics of such crypto assets in the market. The security characteristics may link to tokens that can be used for investment purposes (investment tokens).

Property Characteristics

Conceptually, the phrase “digital asset” encompasses a broader spectrum of electronic, and therefore more intangible, assets than conventional conceptions of property. Furthermore, with respect to the definition proposed by the Bank of International Settlement (BIS), crypto assets are private digital assets that rely on cryptography and distributed ledgers or comparable technologies to function. To this, crypto assets are digital assets that appear in an intangible form.

As a result, in particular, in the case of digital/crypto assets, there are distinct legal concerns to take into account. Even if the token does not reflect rights in a physical asset or rights against a counterparty, it is generally believed that the token may be regarded as an object of property rights in the case of crypto assets. Although many legal systems regard some rights (i.e., rights in rem) as objects of property rights, they may not fully recognize intangible elements as constituting appropriate objects

²⁷ “SEC Framework for “Investment Contract” Analysis of Digital Assets (2019),” *Harvard Law Review*, accessed June 30, 2021, <https://harvardlawreview.org/2019/06/sec-framework-for-investment-contract-analysis-of-digital-assets-2019/>.

²⁸ “Framework for “Investment Contract” Analysis of Digital Assets,” U.S. Securities and Exchange Commission, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn5.

²⁹ *United Housing Foundation, Inc. v. Forman*, 421 U.S.837 (1945) at 852.

across all property rights. This can be seen in the civil and commercial laws of many jurisdictions. In this context, ownership is an especially difficult issue. This is known as the “property issue” and it comes down to whether or not any particular legal system can incorporate “digital commodities”. The author will address all relevant legal and regulatory unclarity in the chapter containing the legal and regulatory analysis.³⁰

The issue is somewhat simpler in the case of digital assets, as many legal systems regard certain rights as intangible objects of property rights (i.e., *res incorporales*). However, as many of these legal systems concentrate on the paper representation of the *res incorporales*, the property issue persists: paper certificate offer a physical, moveable *res* that is a suitable object of property rights. In order to make the pre-DLT system of dematerialized business shares function, certain systems require a (paper) worldwide certificate in a vault. When the paper is removed, the property issue arises for all digital assets in such systems.³¹

Drawing on money/currency, security, and property characteristics, to summarize, it is necessary to understand these characteristics in order to appropriately categorize different types of tokens in the market. Conceptually, money is an economic unit that functions as a means of payment, a unit of account, and a store of value, whereas securities are a negotiable financial instrument that represents financial value in the form of treasury bills, bonds, shares, debentures, or any other instruments specified by securities laws.³² However, it is not easy to provide clarity in determining which digital/crypto assets are legal tender, money, securities, or utilities. The following comprise the main types of tokens based on their respective objective functions.

GENERAL TYPES OF CRYPTO ASSETS

In order to apply all of the above characteristics to particular types of crypto assets or tokens, this section further specifies the categorization of crypto assets as follows:

³⁰ “Legal and Regulatory Considerations for Digital Assets,” Cambridge Centre for Alternative Finance, accessed June 30, 2021, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf>.

³¹ *Ibid.*

³² “Handbook on Securities Statistics,” International Monetary Fund, accessed June 30, 2021, <https://www.imf.org/external/np/sta/wgsd/pdf/hss.pdf>.

Private Tokens/Coins

Payment Tokens

To this, further to the currency characteristics as mentioned earlier, the primary purpose of currency tokens (also known as payment tokens) is to be used as a mode of payment. A central authority may issue these. Currency tokens, on the other hand, are often built on a separate, decentralized blockchain that does not feature a central counterparty. They do not have any inherent value.³³ Currency tokens, on the other hand, are exchanged at a particular price because other market actors assign a monetary value to the tokens based on the limited amount of tokens encoded in the code and the blockchain's anti-counterfeiting security features.³⁴

Securities Tokens

An investment token may provide the opportunity to benefit from the issuer's future profits, the right to receive fixed payments, or voting rights.³⁵ It is usually not sufficient for a token to be classed as an investment token if its investment component entirely depends on expected gains on the secondary market (that is, the possibility of selling the token for a greater price than that for which it was purchased). Aside from that, virtually every token would be considered an investment token.

Investment tokens may also be linked to a company's shares, in which case they are referred to as equity tokens. As a result, a company's shares may be transferred to a third party that will keep them safe. Ownership of the token in this configuration entails a "claim" against the custodial third party for "surrender" of the share and "assignment" of any rights arising from it. Alternatively, business shares may be directly tokenized; that is, the company's stock may be stored and sold on the blockchain. The feasibility of this strategy is a function of national corporate laws.

A debt token is defined as an investment token that represents the right of the token holder to periodic fixed or variable payments and is

³³ Phillipp Maume and Mathias Fromberger, "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws" (2019) 19 *Chicago Journal of International Law*, 548 (582).

³⁴ Iris M. Barsan, "Legal Challenges of Initial Coin Offerings (ICO)" (2017) 3 *Revue Trimestrielle de Droit Financier*, 54 (57).

³⁵ Phillipp Maume and Mathias Fromberger, "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws" (2019) 19 *Chicago Journal of International Law*, 548 (559).

structured similarly to a bond. It is also known as a security token and refers to tokens that are compliant with securities laws.

Utility Tokens

Utility tokens represent a claim or entitlement to a certain level of performance by the issuer. As a result, they resemble a digital coupon. The holder of a utility token may exchange it for the product or service associated with the token with the issuing business. This category of goods and services includes, for example, the supply of storage space,³⁶ restaurant meals, and the usage of promotional services.³⁷ The architecture of a utility token is entirely determined by the token's issuer. Secondary market trades are also possible using utility tokens. However, their tradability and potential profit expectations have no bearing on their categorization as utility tokens.

The issuer may re-issue a utility token if a token holder redeems it. Alternatively, he or she may burn something. The token is permanently removed from the blockchain as a result of this action and its status as a unit of value is thus permanently lost.

In other words, utility tokens are a type of digital voucher that may be used to purchase products or services.³⁸ They also represent the issuer and purchaser's rights and responsibilities. The issuer guarantees the buyer a future service, which may be stated in a white paper or in the terms of service. As a result, the conventional paper voucher is classified as a "carrier instrument" or "bearer token" under section 807 BGB.³⁹ Gift cards that are charged electronically are likewise subject to this judgement.⁴⁰ When redeeming the token, the issuer promises a service or the delivery of commodities. In the case of tokens, however, owing to the absence of a certificate, the transfer of this value is more complicated. Although the (voucher) data is stored on gift cards, tangibility is achieved.⁴¹ Tokens,

³⁶ See e.g. the Filecoin, <https://filecoin.io/>.

³⁷ See e.g. the Friendz Token, <https://www.friendz.io/>.

³⁸ Cf. Hacker/Thomale, loc. cit., p. 14; cf. also Weitnauer, BKR 2018, 231, 232.

³⁹ Cf. Knöfel, in WM 2017, 833, 836.

⁴⁰ Cf. Knöfel, in WM 2017, 833, 836.

⁴¹ Cf. Engelhardt/Klein, MMR 2014, 355, 357.

on the other hand, are intangible. As a result, tokens have no legal status and only serve to symbolize the underlying rights.⁴²

Filecoin is one example of a utility token. The project team was able to generate \$257 million via token sales. The decentralized cloud storage platform for Filecoin is also accessible to token-holders. In other words, Filecoin constitutes a decentralized data storage marketplace, protocol, and cryptocurrency that is making the internet safer and more efficient.⁴³

Asset-Backed Tokens

Apart from the types of tokens mentioned above, there is a category of token that significantly relates to asset tokenization due to its characteristics. In the market, there are tokens that are directly connected to a real asset—amongst the many token types. Asset-backed tokens are a subset class and tokenization is the process of connecting a real item to a virtual token. The holder of an asset-backed token has the right to recover the connected item from the entity holding it on a regular basis by “redeeming” the token.⁴⁴ Custodianship is often performed by the token issuer. One actual item is sometimes connected to a specific number of tokens. Works of art or real estate, for example, may be tokenized in this manner. An equity token is one that is tied to a company’s stock. Such a token may also be linked to precious metals or other valued items. The low volatility of asset-backed currency tokens makes them especially suited as a method of value storage. The issue with asset-backed coins is that they are seldom guaranteed to have adequate coverage.

Privacy Coins

Privacy coins are a type of cryptocurrency that enables private and anonymous blockchain transactions to be conducted by concealing the origins and destinations thereof. In order to avoid chain analysis, the methods

⁴² “ICO: Legal Classification of Tokens: Part 4—Utility Token,” Bird&Bird, accessed June 30, 2021, <https://www.twobirds.com/en/news/articles/2019/global/ico-legal-classification-of-tokens-utility-token>.

⁴³ See <https://filecoin.io/>.

⁴⁴ See Usman W. Chohan, “Tethering Cryptocurrencies to Fiat Currencies without Transparency: A Case Study,” ResearchGate, accessed June 30, 2021, https://www.researchgate.net/publication/323761289_Tethering_Cryptocurrencies_to_Fiat_Currencies_Without_Transparency_A_Case_Study.

employed include concealing a user's actual wallet balance and address and mixing numerous transactions with one another.

In the spirit of openness, Bitcoin and other non-private blockchains enable anyone to see public addresses and transactions on their networks, making it very easy to trace a user's deposits and withdrawals. Privacy coins, on the other hand, encompass two distinct aspects: anonymity and untraceability. Anonymity conceals the identity of the person making the transaction, whereas untraceability makes it almost impossible for other parties to follow the trail of transactions using services like blockchain analysis.⁴⁵ This research explores the two main types of privacy coins below.

Governance Tokens

Developers build governance tokens to enable token-holders to help influence the future of a system. Governance token-holders have the ability to influence project choices, such as submitting and voting on new feature ideas, as well as altering the governance structure itself.

In many instances, smart contracts instantly apply the modifications made, reviewed, and voted on via on-chain governance that is accessible through governance tokens. In other instances, the project's maintenance staff is charged with implementing the modifications or recruiting someone to do so. Proponents of governance token-based systems argue that they provide user control, which is consistent with the original cryptocurrency goals of decentralization and democracy. Decentralized autonomous organizations (DAOs) allow users to direct the evolution of their systems.

Maker (MKR) is a well-known example of a governance token. Its holders may vote on decisions relating to the decentralized finance (DeFi) system, which the decentralized stablecoin DAI utilizes. MKR holders, for example, may vote to alter the complex economic laws that govern decentralized lending, allowing DAI to maintain its price stability. MKR holders were also voting on whether the protocol's debt limit should be increased at the time the content of this paper was published.

According to the Coingecko website, top governance coins can be delineated by market capitalization. These include Uniswap, PancakeSwap, Aave, Amp, Maker, etc.

⁴⁵ "What Are Privacy Coins?," coinmarketcap, accessed June 30, 2021, <https://coinmarketcap.com/alexandria/article/what-are-privacy-coins>.

Stablecoins

Conceptually, stable coins are designed to decrease the significant price fluctuation seen in Bitcoin and other crypto assets, as this volatility is considered the primary barrier to their broad adoption and use as payment methods. The US Dollar Tether is the most well-known example of a stable coin (USDT). The stable coin is a type of asset-backed token. Such currency tokens are known as stable coins. The Tether token, for example, is pegged to the US dollar. As a result, its exchange rate fluctuates minimally around the dollar.

The European Central Bank defines stablecoins as “...digital units of value designed to minimize fluctuations in their prices against a reference currencies or basket of currencies...”; this statement reflects the fact that stablecoins are primarily intended to prevent volatile price fluctuations. However, stablecoins are a broad term that could encompass various arrangements. To this, types of references can include fiat currencies, physical gold, and other types of assets.⁴⁶

Given its characteristics, many countries realized the benefits of stablecoins and aimed to put in place proper regulatory instruments to support their utilization while mitigating potential risks. Stablecoins are a type of digital asset that is intended to be accepted as a method of payment for online transactions (“ecommerce”), peer-to-peer and micro-payments, and a variety of other possible future uses. They also have the potential to be used as a digital monetary instrument in DLT applications, such as programmable money or smart contracts.⁴⁷

For instance, according to a publication by the G7 Working Group on Stablecoins, they could contribute to the development of an international payment system. Given their characteristics and underlying technology, stablecoins can offer faster, less expensive payment options.⁴⁸

However, although stablecoins offer a variety of benefits, there are also challenges and risks that should be considered in developing their

⁴⁶ “The Two Side of the (Stable)coin,” European Central Bank, accessed June 30, 2021, <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp201104~7908460f0d.en.html>.

⁴⁷ Douglas Arner, Raphael Auer, and Jon Frost, *Stablecoins: Risks, Potential and Regulation*, BIS Working Paper No 905, Bank of International Settlement, <https://www.bis.org/publ/work905.pdf>, pp. 2–3.

⁴⁸ *Investigating the Impact of Global Stablecoins*, G7 Working Group on Stablecoins, Bank of International Settlement, <https://www.bis.org/cpmi/publ/d187.pdf>, p. 1.

ecosystem. These can include the lack of clarity of a regulatory framework in relation to the legal status of stablecoins. In this regard, a proper legal foundation for stablecoin arrangements is required.

It is vital to understand the main functions, features, and common types of stablecoins to analyse the most suitable regulatory framework to apply in their case. The most common types of stablecoins are fiat-collateralized, crypto-collateralized, and non-collateralized varieties.⁴⁹ To be more specific, stablecoins can be categorized into three main types depending on the underlying collateralized assets. This feature of stablecoins was developed to stabilize their price, as it tied in with the value of the underlying assets, as noted earlier.

In relation to asset tokenization, according to Jeremy Allaire, CEO and creator of Circle Internet Financial, stablecoins will play a significant role in the tokenizing of assets—converting assets in the form of tokens into a blockchain. He conveyed this at the World Economic Forum in Davos, Switzerland, on Tuesday (21/01) at the session “From tokenized assets to a tokenized economy⁵⁰”.

Hybrid Tokens

As tokens may have a wide range of characteristics and purposes, hybrid forms emerge. In these instances, the categorization must be made on the basis of the actual characteristics of the individual token while remaining within the bounds of the applicable legal rule. Furthermore, it is important to note that there are other tokens that cannot be classified into any of the aforementioned categories.

Sovereignty Tokens/Coins

Central Bank Digital Currencies (CBDC)

According to the associated Bank of International Settlement (BIS) publication, changes in payments, banking, and technology, as well as the disruption accelerated by Covid-19, have attracted attention at the CBDC. It is interesting to note that key statistics produced by the BIS

⁴⁹ “What Are Stablecoins,” CBINSIGHTS, accessed June 30, 2021, <https://www.cbinsights.com/research/report/what-are-stablecoins/>.

⁵⁰ “Stablecoins Will Play a Key Role in Asset Tokenization,” panoramaprypto, accessed June 30, 2021, <https://panoramaprypto.com/stablecoins-will-play-a-key-role-in-asset-tokenization/>.

reflect the interests of the CBDC. As per its name, central bank digital currencies are an electronic form of central bank money or a digital banknote. Accordingly, a digital banknote can be used by individuals in any transactions (so-called retail CBDC) or amongst financial institutions for interbank transfers (so-called wholesale CBDC).

In terms of features, CBDC can be categorized into different groups of other crypto assets in the market. With respect to this, a snapshot of a taxonomy of crypto assets developed by the European Parliament reflects the difference between CBDCs and other private crypto assets.⁵¹

Additionally, in a statement, the Bank of England noted that, in principle, the Bank supplies real money in the form of banknotes that may be used to make payments by both individuals and companies. Electronic money is also available, although it can only be utilized by banks and certain financial organizations. Electronic money issued by the Bank of England would thus be accessible to all families and companies through a Central Bank Digital Currency. Anyone would then be able to make electronic payments in central bank money, which would be allowed by this.⁵² CBDC has the potential to expand payment options and the Bank's ability to keep pricing and the entire UK financial system stable. However, it may also present difficulties that must be carefully handled. As a result, we are studying CBDC and enlisting the help of experts both within and outside the Bank. Our CBDC Discussion Paper for 2020 describes our primary research topics, and our summary of replies to the Discussion Paper summarizes the input we received.⁵³

Moreover, the Bank of International Settlement states that some 50 central banks have previously published ideas or prototypes for central bank digital currencies (CBDCs). Meanwhile, the media reports that around 80% of central banks are seeking use cases for central bank

⁵¹ "Crypto-assets: Key Development, Regulatory Concerns and Responses," European Parliament, accessed June 30, 2021, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU\(2020\)648779_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf), p. 23.

⁵² "Central Bank Digital Currencies," Bank of England, accessed June 30, 2021, <https://www.bankofengland.co.uk/research/digital-currencies>.

⁵³ *Ibid.*

digital currencies (CBDCs), with 40% already putting proof-of-concept programmes in place.⁵⁴

However, the CBDC is not a major subject of this research. This is because the study focuses on private types of crypto assets, particularly those considered investment instruments. It is significant to understand the difference between central bank and non-central bank money: CBDCs differ from private crypto assets in that central bank money is provided as a public good.⁵⁵ However, CBDC will potentially take a leading role in enhancing the financial infrastructure, for instance, in supporting multi-currency cross-border payments.

ANALYSIS OF SOME SELECTED TOKENS IN THE MARKET

Drawing on the previously-presented insights, this section aims to explain different categories of crypto assets in the market. However, due to the fact that there are many types thereof, this section will exemplify some key types of crypto assets that attracted public attention and can be used to represent different structures of such assets.

Bitcoin

Bitcoin (BTC) is a type of cryptocurrency that has gained substantial public attention in recent years. With respect to its characteristics, Bitcoin could be considered a financial asset type or currency. In practice, however, Bitcoin has the features of an investment instrument rather than a means of payment, as it is volatile in price. To specify its initial features as presented in its white paper,⁵⁶ Satoshi Nakamoto aimed to use this type of crypto currency to cut out the need for relevant intermediaries or financial institutions in the payment process.

⁵⁴ “About 80% of Central Banks Are Exploring CBDC Use Cases, Bison Trails Report Says,” coindesk, accessed June 30, 2021, <https://www.coindesk.com/about-80-of-central-banks-are-exploring-cbdc-use-cases-bison-trail-report-says>.

⁵⁵ Erik Feyen, Jon Frost, Harish Natarajan, and Tara Ricem, *What Does Digital Money Mean for Emerging Market and Developing Economies?*, Working Paper, Bank of International Settlement, accessed October 31, 2021, <https://www.bis.org/publ/work973.htm>.

⁵⁶ “Bitcoin: A Peer-to-peer Electronic Cash System,” Bitcoin, accessed June 30, 2021, <https://bitcoin.org/bitcoin.pdf>.

As per a general taxonomy of crypto assets – financial and non-financial assets, in the white paper, Bitcoin is described as “a purely peer-to-peer version of electronic cash”.⁵⁷ Accordingly, it is more likely to initially be designed to be a currency that falls under the scope of financial assets. However, if we compare Bitcoin to national currencies, differences are apparent, such as its decentralized nature. This decentralization also means that Bitcoin does not rely on the control of a Central Bank. Because of this, and as Bitcoin is not produced by a Central Bank, no country considers Bitcoin a legal tender under existing legislation. Other differences include a fixed supply of Bitcoin (21,000,000 units).

Currency is traditionally created by a country’s government. For example, the United States Treasury, via the United States Mint and the Bureau of Engraving and Printing, creates the coins and notes that its citizens use in their daily lives.⁵⁸ The US’ central bank, the Federal Reserve, then distributes money via the banking system. This money is fiat money, which means that its value is not guaranteed by gold or any other commodity.⁵⁹ Rather, its worth is derived from the fact that it is widely accepted as a form of payment. In other words, the way individuals utilize dollar notes and coins in the economy makes them valuable as money.

As previously stated, in an economy, money has three purposes: it acts as a medium of exchange, a store of value and a unit of account. Money must be accepted in exchange for goods and services in order to constitute an efficient medium of trade. Bitcoin may be used to buy and sell a limited number of things. Although the number of businesses accepting Bitcoin as payment has increased, these transactions still make up a small proportion of the overall economy. Furthermore, although Bitcoin was designed as a peer-to-peer payment system, many Bitcoin transactions between consumers and businesses are facilitated by “middlemen” who

⁵⁷ “Defining Bitcoin: Money, Currency or Store of Value,” cointelegraph, accessed June 30, 2021, <https://cointelegraph.com/news/defining-bitcoin-money-currency-or-store-of-value>.

⁵⁸ “Bitcoin, Money or Financial Investment,” Economic Research, Federal Reserve Bank of St. Louis, accessed June 30, 2021, <https://research.stlouisfed.org/publications/page1-econ/2018/03/01/bitcoin-money-or-financial-investment>.

⁵⁹ Ibid.

arrange the transactions by exchanging Bitcoin for traditional currencies.⁶⁰ A transaction may be time- and resource-consuming; on average, it takes 78 minutes to confirm a transaction (but it may take considerably longer) and it costs \$28 to complete one.⁶¹ Furthermore, individuals want a means of payment that retains its value over time (as compared with services or a basket of goods). Bitcoin's value, on the other hand, has fluctuated over time.

In other words, it requires broad adoption in order to fulfil its role as a medium of exchange and therefore as a method of payment. As a result, it should not only be provided as a payment option by (online) shops and businesses, but should also be utilized by the general public to pay for purchases. However, there are currently a few businesses across the globe that accept Bitcoin as a form of payment. It should be emphasized though that consumers only utilize it to a limited degree.⁶² The reasons for this are many, and include the typically complex management of Bitcoin transactions, amongst others. In addition, the comparatively high transaction fees for micro-payments and medium-sized transaction amounts, as well as the—in comparison to other payment methods—lengthy time it takes for a transaction to be verified on the blockchain all make it cumbersome to use Bitcoin for daily transactions.

The stability of a money's value is much more significant, as it can thus act as a store of value. The value of Bitcoin has risen considerably in recent years. When prices are increasing, variable prices may not seem to be a danger to a money's store-of-value function; nevertheless, when prices are dropping, people are reminded that stable value is an essential feature of any medium of value storage. According to economist Robert

⁶⁰ David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal*, Working Paper 19747, National Bureau of Economic Research, accessed June 30, 2021, <http://www.nber.org/papers/w19747.pdf>, p. 6.

⁶¹ “Big Transaction Fees Are a Problem for Bitcoin—But There Could Be a Solution,” CNBC, accessed June 30, 2021, <https://www.cnbc.com/2017/12/19/big-transactions-fees-are-a-problem-for-bitcoin.html>.

⁶² Athey, Parashkevov, Sarukkai, and Xia, *Bitcoin Pricing, Adoption, and Usage: Theory and Evidence*, Working Paper No.17-033, Stanford Institute for Economic Policy Research (SIEPR), accessed June 30, 2021, https://siepr.stanford.edu/sites/default/files/publications/17-033_1.pdf.

Shiller, this volatility jeopardizes Bitcoin's reputation as a store of value and is a key barrier to its adoption as a currency.⁶³

Due to hacker attacks, thefts, and other security issues, the store-of-value function has been weakened.⁶⁴ For example, hackers took down Mt. Gox, the biggest Bitcoin exchange, in 2014, and 850,000 Bitcoins (worth \$14 billion at \$17,000 apiece) were stolen at the time.⁶⁵ Hackers stole \$70 million in Bitcoin on December 7, 2017.⁶⁶ Bitcoin owners are unable to keep Bitcoins as a deposit in a bank; instead, they must store them in a digital wallet, and such digital deposits are not protected by the government in the same way that deposits at banks and credit unions are.

By definition, the blockchain technology that underpins Bitcoin and many other crypto assets is a digital memory, with a storage function that is especially effective owing to its decentralized nature. As a result, crypto tokens in general and Bitcoin in particular ultimately meet the required storage and durability criteria. In contrast to, or in conjunction with, traditional (fiat) currencies, the key question is whether crypto assets can maintain their value over longer periods of time.

Money is also used as a unit of account, or a standard for valuing products and services. Retailers must periodically recalculate their Bitcoin pricing, as Bitcoin values drastically change while the market is open and from day to day, which is likely to mislead both buyers and sellers. Furthermore, the price of Bitcoin swings on exchanges, and Bitcoin often trades at various values on multiple exchanges, making pricing choices for sellers even more difficult.⁶⁷

⁶³ "What is Bitcoin Worth? Don't Even Ask," *New York Times*, accessed June 30, 2021, <https://www.nytimes.com/2017/12/15/business/bitcoin-investing.html>.

⁶⁴ David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal*, Working Paper 19747, National Bureau of Economic Research, accessed June 30, 2021, <http://www.nber.org/papers/w19747.pdf>.

⁶⁵ "A Brief History of Bitcoin Hacks and Frauds," *Ars Technica*, accessed June 30, 2021, <https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/>.

⁶⁶ Rishi Iyengar, "More Than \$70 Million Stolen in Bitcoin Hack," *CNN Tech*, December 8, 2017, <http://money.cnn.com/2017/12/07/technology/nicehash-bitcoin-theft-hacking/index.html>.

⁶⁷ David Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal*, Working Paper 19747, National Bureau of Economic Research, accessed June 30, 2021, <http://www.nber.org/papers/w19747.pdf>.

Should we treat Bitcoin as a property? In an effort to answer these questions, there have been discussions on these issues in recent years (citation needed). To exemplify this, the Internal Revenue Services (IRS) of the US ruled that those virtual currencies should be treated as property for tax purposes.⁶⁸ In particular, the IRS provides that virtual currency functions like real currency; however, it does not have legal tender status. However, the clarification makes utilizing bitcoin as a currency more problematic. For anyone who transacts in digital currencies will be subject to the same record-keeping obligations and taxes as those who transact in stocks and other financial instruments.⁶⁹

Ethereum

Ethereum cryptocurrency (ETH) is a type of cryptocurrency. It is a digital currency that can be used on the internet, and is comparable to Bitcoin. Like other cryptocurrencies, one may transmit ETH without using a third-party service such as a bank. It is the same as giving over cash in person, except that it can be done with anybody, anywhere, at any time. ETH is a decentralized and global cryptocurrency. This is because it is built on Ethereum, which provides anyone, regardless of background or location, with open access to digital money and other services.⁷⁰

ETH has been widely used as an investment instrument like other types of cryptocurrencies in the market. In this regard, analysing its fundamental features or characteristics in terms of the above characteristics and types of tokens will not differ from the case of BTC, as previously discussed. Specifically, in many respects, ETH and BTC are similar: both are decentralized digital currencies that are exchanged on internet exchanges and held in different kinds of cryptocurrency wallets. This section considers ETH, as it is the second-largest cryptocurrency by market capitalization. However, it should be noted that the fundamental

⁶⁸ “IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply,” IRS, accessed June 30, 2021, <https://www.irs.gov/newsroom/irs-virtual-currency-guidance>.

⁶⁹ “Bitcoin to Be Treated as Property Instead of Currency by IRS,” *The Guardian*, accessed June 30, 2021, <https://www.theguardian.com/technology/2014/mar/25/bitcoin-property-currency-irs-rules>.

⁷⁰ See <https://ethereum.org/en/eth/>.

goal of ether is to make the Ethereum a smart contract and decentralized application (dapp) platform that is easier to use and commercialize. This differs from the case of BTC, which was initially designed to be an alternative to national currencies.

Monero

According to the Coindesk website, Monero is a cryptocurrency that focuses on anonymity and was launched in 2014. It was forked from Bytecoin by a user known as “Thankful for today” on the Bitcointalk forum, and was subsequently maintained by the decentralized development community. Monero is fungible, which means that participation in past transactions has no effect on the value of any given currency, since the entire transaction history is unknown. Monero enables privacy and prevents coins from being spent more than once by using senders’ unique ring signatures, secret recipient addresses, and Ring Confidential Transactions.⁷¹ According to its white paper, the most significant features of this digital money are “privacy and anonymity⁷²”.

In other words, all transaction data are obscured, despite the fact that it is a public and decentralized ledger. With Bitcoin, by contrast, all transaction information, user addresses, and wallet balances are made public and accessible.

Zcash

According to its website, Zcash is a digital money that protects user privacy and is based on sound science. People may trade quickly and securely using it for a minimal charge. Shielded Zcash keeps transactions private while enabling users to selectively disclose address and transaction information for auditing or regulatory compliance purposes.⁷³

In this, Monero and Zcash can be regarded as privacy coins. It should be pointed out that privacy coins differ from other types of cryptocurrencies or crypto assets, as they are designed to be anonymous and

⁷¹ “Monero,” coindesk, accessed June 30, 2021, <https://www.coindesk.com/price/monero/>.

⁷² “Crypto Note V 2.0,” Bytecoin, accessed June 30, 2021, <https://bytecoin.org/old/whitepaper.pdf>, p. 1.

⁷³ “How It Works,” Zcash, accessed June 30, 2021, <https://z.cash/technology/>.

untraceable. However, it is worth pointing that to consider Monero and Zcash as currencies, their values are set by demand and supply. Again, similar to the case of other cryptocurrencies such as Bitcoin, this is a key barrier to its use as a currency in accordance with the main functions of money (a medium of exchange, a unit of account, and a store of value). To conclude, these features may not affect their legal status as a currency according to three main aforementioned attributes; however, these may embody the anonymity that this form of money provides.

Uniswap (UNI)

According to its website, UNI is a tradable asset that functions similarly to most other ERC20 tokens, with the exception that it is more powerful as a voting mechanism. The owner must first go through the delegation procedure before using it as a vote. Delegating UNI ties one's tokens' voting power to an address that may then be used to vote. This address can be private or that of a trustworthy third party a user thinks will vote in Uniswap Governance's best interests.⁷⁴

Could a governance token be classified as a security? To begin with, tokens are rarely utilized for public fundraising in today's designs to avoid being regarded as securities. Ordinary users acquire these tokens by locking up money, providing liquidity, or recommending users on the public side and they are typically given away for free. Ordinary users do not obtain tokens via direct cash purchases, according to its general design. However, DeFi projects almost always have an initial investor. Based on the original investor's contribution, a portion of the token is distributed to subsequent investors. Such a token purchase mechanism satisfies Howey's definition of investment. Additionally, despite the fact that regular users acquire these tokens in a non-monetary manner, all users have a clear expectation of appreciation, which is consistent with the Howey Test's definition of profit expectations. Furthermore, although the use of DeFi does not require human participation or manual day-to-day operation, these systems are created by specialized teams. Certain issuers' papers state that some tokens can be saved for future workers, and that the construction team would receive tokens in instalments. The Howey Test concept of regular business is obviously met by such a business team.

⁷⁴ "Beginners Guide to Voting," Uniswaps Docs, accessed March 30, 2021, <https://docs.uniswap.org/protocol/concepts/governance/guide-to-voting>.

It is also worth noting that governance tokens come with specific benefits. Protocols may charge their users a fee. Such fees are then collected and a governance vote may determine whether a part of the fees should be distributed to token-holders, similarly to how dividends are distributed in stocks. As was previously stated, token owners have the right to vote on the protocol's future. Most projects, for example, permit token-holders to vote on smart contract code modifications, as well as treasury management. Considerations for governance token qualifications as securities will be discussed in detail in the following chapters.

Non-Fungible Tokens

The public's interest in Non-fungible Tokens (NFTs) was piqued in February 2021 when a piece of video art sold for 6.6 million USD, and it was piqued again in March when a collage of digital art created by the same artist (who goes by the moniker Beeple) sold for 69 million USD. Both transactions had one thing in common: the buyer did not attain any real goods; instead, he received a crypto asset known as an NFT.

NFTs are one-of-a-kind; unlike money, they are not “fungible” or interchangeable. An NFT attests to the asset's ownership and may therefore be seen as a virtual certificate of authenticity. NFTs are now traded in digital markets using cryptocurrency as a payment method and the Ethereum blockchain as the preferred decentralized ledger.⁷⁵

These features imbue them with a plethora of options. With the assistance of smart contracts and metadata, the usage of NFTs on a blockchain ensures ownership and provenance in an unbreakable way. Transparency in ownership and transactions also eliminates issues that may arise in non-virtual markets, such as art, jewellery, and real estate. NFTs may furthermore eliminate the need for dealers and other types of intermediaries, enabling buyers and sellers to retain a greater portion of the transaction's value. NFTs are also programmable and transferable, allowing a piece of material to be enhanced or connected to other material by third parties after being uploaded to the blockchain. By integrating it with additional material from the musical act, an NFT representing a

⁷⁵ “Update on Digital Assets: NFTs, DeFi, Cryptos, CBDCs,” DBS, accessed June 30, 2021, https://www.dbs.com.sg/corporate/aics/templatedata/article/generic/data/en/GR/042021/210405_insights_digital_currencies.xml.

backstage pass at a performance, for example, may be made more valuable or collectable.⁷⁶

NFTs are also being used to trade a broad variety of virtual goods, from NBA virtual trading cards to memes and tweets on the internet. The token may be displayed on monitors or added to a virtual gallery once it has been bought. There are hundreds of billions of dollars' worth of yearly transactions in music, video games, and art that could be tokenized, providing content-creators with greater power and value. An NFT's royalty may also potentially revert to the inventor each time it is sold.⁷⁷

Tether

According to the Tether white paper,⁷⁸ Tether (known to all as USDT) is a unit (or multiple units) of a fiat-pegged cryptocurrency issued by Tether Limited. It should be noted that Tether Limited formerly incorrectly stated that each token was backed by one US dollar.⁷⁹ In principle, each Tether unit, according to the company, is fully backed by USD reserves. Tether supply would be determined by investor demand in this system, with supply rising when investors deposit USD with Tether Inc and decreasing when investors recover dollar deposits, thus removing Tether from circulation. Conceptually, Tether differs from Bitcoin in terms of having a more stable value. More importantly, by volume, in 2019 USDT overtook Bitcoin as the most widely traded cryptocurrency.⁸⁰

With respect to its characteristics, Tethers serve to provide liquidity and are a well-known token that may be used to facilitate transactions between other cryptocurrencies.

It should be noted that there is also the so-called "Tether Gold" that was developed by the same operator. As its name implies, Tether

⁷⁶ Ibid.

⁷⁷ Ibid.

⁷⁸ See <https://tether.to/>.

⁷⁹ "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York.," Letitia James NY Attorney General, accessed June 30, 2021, <https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinex-illegal>.

⁸⁰ "Digital Cash as Legal Tender," Forbes, accessed June 30, 2021, <https://www.forbes.com/sites/davidbirch/2021/01/04/digital-cash-as-legal-tender/?sh=1d00f6049a1>.

Gold is defined as a digital token that is backed by physical gold. In the white paper, Tether Gold was described as an option for investors who could be interested in investing in physical gold with lower costs. There are differences between Tether and Tether Gold, such as the referenced assets.⁸¹

Given the stable value of Tether, it is necessary to further consider its legal status as a currency. As previously noted, the stability of money is significantly important, as it serves as a store of value. In general, however, it should be noted that the stable value of stablecoins depends heavily on the type of such a stablecoin—they are presently classified as either national fiat currency-backed, or cryptocurrency-backed, based on the underlying collateral.

Some may argue that Tether's false statement regarding its reserves⁸² could potentially affect its currency status. However, as previously noted, a currency does not need to have an intrinsic value for undertaking monetary functions.

Regarding its security characteristics, in the case of Tether, although it is a type of cryptocurrency that is utilized by crypto investors who wish to escape the high volatility of other cryptocurrencies while maintaining their value within the crypto market, Tether can be used as an investment instrument because, unlike other cryptocurrencies in the market, it has a high level of transparency and a low price fluctuation. In this regard, it would be interesting to consider whether Tether should constitute a security in light of its characteristics. To assess its security features, it is necessary to understand investors' reasonable expectation as being a "reasonable expectation of profits" to be a key characteristic of "securities".

The later chapters will explore different regulatory implications based on the different characteristics of these crypt assets. In this regard, the chapters will address key concerns from regulators concerning the fact that stablecoins may be susceptible to a bank run if a significant number of investors hurry to redeem them, forcing sponsors to liquidate assets at

⁸¹ "Tether Gold—A Digital Token Backed by Physical Gold," Tether Gold, accessed June 30, 2021, <https://gold.tether.to/Tether%20Gold%20Whitepaper.pdf>.

⁸² Matt Robinson, "Tether's Latest Black Eye Is CFTC Fine for Lying About Reserves," Bloomberg, October 15, 2021, <https://www.bloomberg.com/news/articles/2021-10-15/tether-bitfinex-to-pay-fines-totaling-42-5-million-cftc-says>.

fire-sale prices and placing strain on the financial system. This concern led to a proposal and discussion regarding more stringent rules.

STEEM Tokens

Conceptually, the STEEM blockchain saves information in an immutable blockchain record and pays users in digital tokens called STEEM in exchange for their efforts. The Steem blockchain creates fresh STEEM coins every day and adds these to a community’s “rewards pool”. Users are subsequently rewarded with tokens in exchange for their efforts, which are determined by the number of votes their material receives. Users with greater “STEEM Power” in their accounts are then able to choose how a larger portion of the rewards pool is allocated.⁸³

REGULATORY CHALLENGES

ASEAN Countries

Digital assets can be used in a variety of ways. To be more specific, this depends on their main intended function or the type of token being considered. For example, digital assets can be used as financial instruments for businesses in the form of alternative fundraising channels. Accordingly, regulatory constraint is one of the key challenges for regulators in the use of digital assets as a tool to boost financial inclusion in certain jurisdictions. To date, there have been a number of legal problems that may arise from the use of digital assets. These problems include a lack of clarity in key regulatory frameworks, a lack of coordination amongst authorities, information asymmetry, and issues relating to the ambiguous legal rights and responsibilities of token issuers and token holders. Consequently, unless authorities put in place a suitable regulatory framework, the benefits of digital assets may be undermined.

Specifically, it is worth noting that regulators in most ASEAN countries are receptive to the changes. There are laws, regulations and guidance that have been issued by regulators in order to support fast-growing innovation while preventing potential risks. It is important to highlight that regulatory responses regarding crypto assets can generally be

⁸³ “SteemitFAQ,” steemit, accessed June 30, 2021, https://steemit.com/faq.html#What_is_Steemit_com.

categorized into three main types of regulatory responses: existing regulation; retrofitted regulation; and bespoke regulation.⁸⁴ Most regulations in ASEAN countries mainly regulated related activities and businesses concerning digital assets.

In essence, regulators have to date focused on regulations for crypto asset businesses, whose activities include initial coin offerings (ICOs). However, the legal status of certain types of digital tokens remains unclear, and are not properly regulated by regulations in a number of ASEAN countries.

It is worth noting that to understand digital token categorization, it is important for regulators and all stakeholders to implement laws and/or regulations for such digital assets. This is also because digital assets can be categorized into a variety of types, hence the differences that may fall within the scope of different laws and/or regulations. More precisely, a token's legal treatment may depend on its main function or the type of token being considered. The tokens' categorizations are helpful for capturing the complexities of crypto assets and in informing regulatory responses in this rapidly evolving domain.

More specifically, digital tokens and cryptocurrencies can be considered types of digital assets. The types of digital assets primarily depend on the assets' functions and features. This can be explained by reference to the functions and features of traditional financial instruments or financial assets, such as securities. For example, the security characteristics of security (digital) tokens shall be considered in order to properly assess the security of such tokens. However, there are other types of tokens, including payment and utility tokens, which may fall within the scope of a different regulatory framework. Furthermore, there are emerging new types of digital assets such as "Libra coin" which was initially proposed as "a simple global currency...", it is obvious that the coin is aimed to be used as a means of payment. This type of digital asset could be regarded as a so-called stable coin. Also, there are a number of hybrid-type (digital) tokens that could be difficult to group as any particular type of tokens, and accordingly it is difficult for regulators to appropriately regulate such

⁸⁴ "Global Cryptoasset Regulatory Landscape Study, Cambridge Centre for Alternative Finance, University of Cambridge," Cambridge Centre for Alternative Finance, accessed March 30, 2020, https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf, p. 41.

tokens as well as related businesses and intermediaries. This can reflect the regulatory challenges for regulators in ASEAN in ensuring laws and regulations keep pace with the complexity of digital assets' arrangement. In other words, to contemplate a regulatory framework for digital assets, there are a number of laws, regulations, and guidances that should be taken into account as it is vital to understand the main functions, features, and the common types of digital assets in order to analyse the most suitable regulatory framework.

Regarding the regulatory challenges, as mentioned earlier, there is regulatory uncertainty in a number of countries in Southeast Asia. For example, in Indonesia, even there are new rules (Regulation No.5/2019) allowing crypto assets to be traded as commodities on future exchanges in the country; however, the regulation excludes initial coin offerings from the scope of the regulation. This can reflect the regulatory uncertainty as the regulation was not designed to support digital asset activities at full scale. In addition, there is no regulation or guideline that was specifically designed to ascertain the legal status of digital assets, including private tokens. For instance, to consider whether such tokens are securities or not.

Furthermore, to exemplify the regulatory challenges, it is notable that the types of digital asset businesses under existing Thai laws and regulations are still limited and do not cover all possible types of digital asset businesses in the market. At present, under the Emergency Decree on Digital Asset Businesses, the types of digital asset businesses are limited to three main types, namely exchange, brokerage, and dealer businesses. In addition, the exemptions under the Notifications issued by the Thai SEC are still limited and may need to be retrofitted in response to emerging technologies. This can be seen as an insufficient standard to ensure consumer protection.

For ICOs, there are bespoke regulations in Thailand as well as some other countries for regulating ICO-related activities; however, it is still challenging for regulators to provide clear-cut guidelines and/or subordinate regulations, such as the criteria to differentiate utility and security tokens.

With regard to stable coins, it is noted that within the Thai legal and regulatory framework, stable coins may not be granted the status as a legal tender or currency. However, stable coins are a type of digital asset that was defined in the Emergency Decree on Digital Asset Businesses. However, at present, it is worth noting that the Thai Securities and

Exchange Commission does not allow Libra to be traded as trading pairs. In connection with the Notification KorTor11/2561, Thai SEC tends to exempt businesses offering services in relation to the purchase or sale of fiat-collateralized stable coins from the requirements specified in the Emergency Decree. However, to date, the Thai SEC has only exempted businesses offering services in relation to the purchase or sale of Thai baht-collateralized stable coins. Therefore, in the case of Libra, regulatory unclarity in Thailand may possibly impede its adoption and development in the market.

There are also concerns associated with foreign business restrictions and taxation: Under the Royal Decree and mandate of the Ministry of Finance, businesses engaged in the digital asset trade must be registered as companies in Thailand. This restriction can potentially obstruct foreign entities/investors from entering the Thai market as digital asset-related businesses. This can also limit consumer choices. Moreover, it is not consistent with the initiatives launched by the Thai government to attract foreign investment in this area, as noted in a BOI announcement in 2014.⁸⁵

Regarding the implementation of regulations on capital gains tax, under Thai laws, the Ministry of Finance issued ministerial regulations to impose a 15% withholding tax on capital gains and benefits from digital assets. This 15% tax rate could make the digital asset market in Thailand less attractive for both Thai and foreign traders. Furthermore, there are still many difficulties in terms of tax calculation.

In addition, with regards to the coordinated mechanisms, one of the most significant difficulties confronting domestic regulatory perspectives on the digital asset industry is that various authorities have differing views on the usage of cryptocurrencies. These contradictory positions and a lack of cooperation amongst various authorities may pose a difficulty in the usage and monitoring of cryptocurrencies.

Furthermore, additional complicated legal problems, such as the validity of so-called “smart contracts” and law enforcement, or the seizure of cryptocurrencies, may emerge as a result of characteristics of digital assets and DLT.

⁸⁵ The Announcement of the Board of Investment No. Sor. 1/2559 Re: Additional Amendments of Eligible Activities for Investment Promotion In accordance with the BOI Announcement No. 2/2557, http://www.boi.go.th/upload/content/Announcemnt_Sor1-2559_90752.pdf.

In summary, there is regulatory unclarity concerning digital assets which can potentially impede the utilization of digital assets at full scale.

Other Frontier Markets

Hong Kong SAR

In terms of the regulatory framework, Hong Kong's fundamental legislation, in general, is based on free market principles, which are critical for the country's continued status as an international financial centre. Regulatory responses to FinTech development, in this perspective, are part of policy innovation targeted at market facilitation and other related activities.

The legal status of crypto assets may differ depending on the primary use or kind of crypto asset in question. Crypto asset classifications are useful for expressing the intricacies of this asset class as well as directing regulatory actions. The laws and regulations governing crypto assets in Hong Kong are catalogued, compared, and evaluated in this chapter. A thorough examination of the complex characteristics and functionalities of crypto assets is required for this purpose, as is a grasp of the dangers and regulatory consequences.

The SFC, Hong Kong's territorial regulator, is in charge of crypto assets. In theory, crypto assets or digital tokens are regulated by the SFC, since some forms of crypto assets or digital tokens may be classified as "securities" or "futures contracts" under the Securities and Futures Ordinance owing to their features (SFO). It is important to note that the SFC is the primary regulatory and supervisory body for crypto asset activity. The SFC, statements, and a position paper released by the institution are also important controlling rules.

Certain types of crypto assets were regulated by existing securities regulatory perimeters prior to the SFC's statement on the regulatory framework for virtual asset portfolio managers, fund distributors, and trading platform operators, which was designed to prevent the risks associated with virtual asset investment. Before issuing the above-mentioned statement, as well as a position paper in 2019, the SFC issued circulars to clarify its regulatory stances, including a statement on initial coin offerings (ICOs), a circular to licensed corporations and registered institutions on Bitcoin futures contracts, and a circular to licensed corporations and

registered institutions on cryptocurrency-related investment products in 2017.⁸⁶

Furthermore, the ICO statement⁸⁷ underlines that a digital token may be considered a security under Hong Kong's current regulatory framework. Furthermore, the ICO's digital tokens may constitute a share, a debenture, or an interest in a collective investment scheme (CIS) based on their characteristics and what the tokens represent, according to the ICO's statement on ICOs. To provide an example, if a digital token represents an ownership stake in a company, it will be treated as a share. The tokens should be treated as a debenture if they are used to recognize a debt or obligation. Furthermore, tokens might be seen to have an interest in a CIS if they offer token holders with a portion of the project's earnings. To conclude, the rights linked to such digital tokens must be considered in order to establish which form of financial instrument they are. It should be emphasized that under Hong Kong securities legislation, all potential forms of financial instruments are deemed "securities".

In Hong Kong, however, cryptocurrencies are not legal currency, since the Hong Kong Monetary Authority (HKMA) specifies three characteristics of money. To begin with, cryptocurrencies are not frequently recognized as a form of payment. This is seen in the instance of Bitcoin, a sort of digital money whose value has fluctuated. Cryptocurrency price fluctuations have the potential to make them unusable as a means of trade. The HKMA also said that Bitcoin is a "highly inefficient mode of payment" due to a number of factors, including its lengthy validation procedure. Furthermore, as is typical with cryptocurrencies, its value has been exclusively determined by market demand and supply. This trait makes adopting cryptocurrency as a store of value or a unit of account difficult for key stakeholders. Furthermore, according to the HKMA's proposed "moneyness" addition specification, cryptocurrencies are not scalable, and hence do not fulfil the ultimate condition of forming money or legal tender.

⁸⁶ Securities and Futures Commission, "Circular to Licensed Corporations and Registered Institutions on Bitcoin Futures Contracts and Cryptocurrency-Related Investment Products" (December 2017), available at: <https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC79> (last accessed January 7, 2021).

⁸⁷ Securities and Futures Commission, "Statement on Initial Coin Offerings" (September 2017), available at: <https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-initial-coin-offerings> (last accessed January 7, 2021).

In general, this is consistent with how countries around the world have approached the legal status of cryptocurrencies; for example, the Bank of Thailand issued a notification in 2018 clarifying that cryptocurrencies are not legal tender under Thai law (the Currency Act B.E.2501 (1958)), or Bank Negara Malaysia issued a policy document declaring that cryptocurrencies are not legal tender in the country.⁸⁸

It's worth noting that the HKMA focuses on the legal tender status of cryptocurrencies like Bitcoin and ignores other crypto asset classifications. Furthermore, other forms of crypto assets, like stablecoins, may have unique characteristics that might complicate the HKMA's study of cryptocurrencies' legal tender status. However, despite the fact that a big number of individuals in Hong Kong recently employed stablecoins to relocate their personal assets outside the government's jurisdiction after the enactment of Hong Kong's national security legislation, there is currently no special legislative framework for stablecoins.⁸⁹

The SFC first released a statement on the regulatory framework for virtual assets for portfolio managers, fund distributors, and trading platform operators, with the goal of limiting possible hazards. Given that a virtual asset, under the SFC's definition ('...A virtual asset is a digital representation of value, often known as 'cryptocurrency,' 'crypto-asset,' or 'digital token...'), offers considerable risks to investors. The hazards may arise as a consequence of the features of virtual assets and the operations of important stakeholders, such as virtual asset intermediation.⁹⁰

⁸⁸ Bank Negara Malaysia, "Bank Negara Malaysia Issues Policy Document for Digital Currencies," available at: https://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4628&lang=en (last accessed November 15, 2020).

⁸⁹ Pan, "Hong Kong Citizens Turn to Stablecoins to Resist National Security Laws" (July 2020), available at: <https://www.coindesk.com/hong-kong-citizens-turn-to-stable-coins-to-resist-national-security-law> (last accessed January 7, 2021).

⁹⁰ Securities and Futures Commission, "Statement on the Regulatory Framework for Virtual Asset Portfolios Managers, Fund Distributors and Trading Platform Operators" (November 2018), 13, available at: <https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-regulatory-framework-for-virtual-asset-portfolios-managers> (last accessed January 7, 2021).

As a result, authorities have mostly concentrated on regulating and overseeing the connected activities of ICOs and crypto asset exchanges⁹¹ in terms of crypto asset regulation. In this respect, it's worth noting that the SFC's approach is likewise rather comparable to those of other countries that prioritize meaningful intermediation. When it comes to crypto asset regulation and supervision in Hong Kong, however, there are a few different ways to examine.

CONCLUSION

Bitcoin, Ether (Ethereum), and XRP (Ripple) stand out amongst the numerous crypto assets⁹² available owing to their persistently large market capitalizations when compared to other crypto assets. A crypto token's market capitalization is determined by multiplying the number of tokens in circulation by the current market price. Bitcoin, Ether, and XRP accounted for over 70% of the total market capitalization in April 2021, i.e., the entire market capitalization of all traded tokens.⁹³

The issue of whether crypto and, in particular, 44 currency tokens constitute money or even currencies in the traditional sense is at the heart of the present economic debate. Despite the fact that the economic significance and consequences of crypto assets are several times greater and extend well beyond the currency element, this issue continues to be a subject of scholarly discussion in this area.⁹⁴ This is mostly due to Bitcoin's dominant position and its related goal of creating a payment and currency system that is decentralized and free of intermediaries.⁹⁵

⁹¹ Cambridge Centre for Alternative Finance (University of Cambridge, Judge Business School), "Global Cryptoasset Regulatory Landscape Study" (April 2019), 13, available at: <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf> (last accessed January 7, 2021).

⁹² See The website CoinMarketCap lists 12,910 tokens (as of 20.10.2021) with a total market capitalization of USD 2.53 trillion.

⁹³ See CoinMarketCap.

⁹⁴ Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal," in Lee and Chuen, *Handbook of Digital Currency*, Bitcoin, Innovation, Financial Instruments, and Big Data (Academic Press, 2015), 32; Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (2018), 167 f.

⁹⁵ See "Bitcoin: A Peer-to-Peer Electronic Cash System" accessed June 30, 2021, <https://perma.cc/MU7N-AWPD>.

Assigning a specific digital/crypto asset or token to a particular category is not always a straightforward process. For instance, certain assets may be utilized in various ways depending on the context, and therefore may fall into two or more categories. Furthermore, assets may change over time in response to changing user behaviour. As a result, an asset's categorization is not fixed, but rather requires a continuous and dynamic evaluation of its characteristics, use, nature and related rights. Accordingly, this may result in asset categories overlapping.

It is necessary to discuss further on legal and regulatory perspectives on crypto assets. In particular, they will consider such issues as the "ownership" and "property" of crypto tokens, contractual ties in Initial Coin Offering (ICO) and secondary market transactions, as well as intermediaries and distance contracts. There are other issues; for instance, prospective responsibility under capital market laws, as well as other aspects of capital market tort and liability law, along with mining and mining pools need to be analysed. Additionally, as crypto token transactions are typically cross-border in nature, this results in the need to determine the place of (international) jurisdiction (through the relevant law of jurisdiction as part of International Procedural Law (IPL)). The main aim of the following chapter to catalogue the legal and regulatory framework is associated with asset tokenization. This draws relevant constraints and proposes an applicable framework, particularly for ASEAN developing economies with fewer resources. Also, various factors need to be considered, such as the socioeconomic and cultural aspects, including local social and organizational structure, local resources, and the structure of supervisory agencies, industry-standard organizations, and collaborative mechanisms.



Fintech for Financial Inclusion

Felix Honecker and Dominic Chalmers

INTRODUCTION

A central claim of many financial technology firms is that they provide new ways in which to address ‘the unbanked’, that is, groups that are currently unable (or unwilling) to access traditional financial services. The potential of digital technologies to address financial inclusion has taken centre stage in numerous policy reports and development strategies over recent years. This chapter delves into the intricacies of the debates around fintech for financial inclusion and outlines some of the main issues affecting practitioners and policymakers today.

First, we will provide a comprehensive overview of the causes and consequences of financial exclusion. Second, we will outline the fintech opportunity by illustrating how fintech introduces a new toolkit for addressing these intractable problems and how it enables approaches that had previously not been at our disposal. Third, we summarise three success stories that illustrate how fintech for financial inclusion is making an impact in markets as diverse as Kenya, China, and Scotland. Fourth,

F. Honecker (✉) · D. Chalmers
University of Glasgow, Glasgow, UK
e-mail: felix.honecker@glasgow.ac.uk

we discuss opportunities for the public sector and elaborate how ‘fintech for social good’ does not have to be market-driven. Finally, we discuss the other side of the coin and illustrate how, despite the immense potential, we must remain sensitive to potentially negative social impacts of financial technology.

FINANCIAL INCLUSION

Today, many societies are financialised to a degree that makes social life difficult for people who struggle with (or are prevented from) accessing or using financial services. Access to finance has become a central element underpinning essential services around the globe. It facilitates day-to-day living and money management, but also enables individuals and families to plan for long-term goals or to make provisions against unexpected drops in income—for example due to crop failures or job losses. It also helps people escape from poverty and opens opportunities to invest into their health, education, or businesses. Financial inclusion, thus, is not an end, but a means to an end: it has been identified as a crucial enabler for 7 out of 17 UN Sustainable Development Goals (e.g., No Poverty, Good Health and Wellbeing, or Decent Work and Economic Growth). Policymakers and development organisations around the globe are therefore striving for higher levels of financial inclusion. But what exactly does financial inclusion mean?

According to the World Bank, being financially included means having access to and being able to use affordable financial products and services that are provided by sustainable, mainstream institutions (World Bank Group 2018). Access to four types of products has been deemed essential: transaction accounts, credit, savings, and insurance. For each of these four types, which are widely perceived as the pillars of financial inclusion and resilience, we can typically distinguish between unbanked and marginally banked (or underserved) individuals. Because of their distinct characteristics, we now elaborate on the different degrees of financial exclusion for each of the essential products.

Transaction Banking. For this product category, people with no bank account at all would be considered unbanked. People with access to a bank account without electronic payment facilities as well as individuals who have access to a transaction account but make little use or no use of it are considered ‘marginally banked’ or underbanked. Account ownership across the globe is growing quickly, but a significant number

of people remains cut off from basic financial services. Globally, about 1.7 billion people remain unbanked—meaning they have no access to an account at a mainstream financial institution at all (Demirguc-Kunt et al. 2018). A large majority of unbanked adults live in the developing world, where account ownership sits at 63% on average but varies widely across countries, even among those in close proximity. According to the Global Findex Database 2017, there is still a considerable number of countries in which less than 20% of the adult population owns a bank account (Demirguc-Kunt et al. 2018; World Bank Group 2017).

In developed societies, however, access to a bank account (and transaction banking facilities in particular) has become a universal need. In fact, account ownership is perceived as the standard, and the lack of access to or usage of such facilities is so uncommon that it carries a stigma. Consequently, 94% of adults in high-income economies have an account at a mainstream financial institution (Demirguc-Kunt et al. 2018). Most official payments are made electronically, thus an account is a *de facto* requirement for receiving regular funds such as wages, pensions, or social welfare (Kempson et al. 2007). Crucially, other aspects of social life are built on the fact that transaction accounts have become customary—it is, for example, unlikely for someone without a bank account to find quality employment or housing in a highly financialised society. Moreover, meeting basic financial obligations such as paying for utility bills becomes considerably more difficult, more time consuming, and sometimes even more expensive if it cannot be done electronically (i.e., via transaction account).

Owning and using a transaction account is often perceived as a gateway to further financial services (e.g., credit, insurance, or sophisticated savings products). Promoting and enabling account ownership has therefore become a priority for many governments, development organisations, and other NGOs.

Credit. Access to credit plays a significant role in smoothing consumption, protection against income shocks, and enabling expenditures that oversize the usual household budget. Even small credit can therefore have substantial positive effects for individuals and families, for example by facilitating social mobility or improving the quality of housing (and therefore, indirectly, health and self-esteem) (Kempson et al. 2007). For credit, too, we can identify various degrees of exclusion. This ranges from no access to credit, to having access but being inappropriately served (e.g., sub-prime or any type of money lender that charges particularly

high interest or offers unfavourable conditions). A good understanding of the structure of national credit markets is particularly relevant to identify problems of credit exclusion. The existence of interest rate ceilings, illegal lenders, credit unions, and other social or not-for-profit providers, for example, can impact the situation drastically.

Because some types of credit (such as overdraft facilities or credit cards) have very high adoption rates, particularly in developed economies, lack of access to these instruments may stigmatise and negatively affect social life. By contrast, borrowers in developing economies need to rely on informal lenders such as family and friends much more often (Emran and Farazi 2009).

Savings. Findex data suggest that people are saving money in vastly different ways. Many savers, particularly in high-income economies, save formally through depositing money into an account at a mainstream financial institution. More sophisticated options of formal savings include investment products or government securities. Common alternatives to savings are semiformal approaches (e.g., savings clubs) or entrusting money to family members and friends for safekeeping (Demirguc-Kunt et al. 2018). Informal saving methods include saving in the form of live-stock or jewellery, or simply keeping cash at home ('under the mattress'). Just like credit, savings are a good way to build up emergency funds and improve financial resilience. Moreover, savings are key to ensuring financial independence and security in retirement.

The problems relating to savings exclusion are of a different nature than those for transaction banking and credit. The availability of simple deposit accounts seems not to be an intricate problem globally, and while not having access to a savings account might cause various inconveniences, it does not necessarily relate to social exclusion (Kempson et al. 2007). Conversely, savings exclusion is often a consequence rather than a cause of social problems: individuals might simply not have enough money to save, might be unwilling to deal with banks due to a lack of trust (often based on past experiences with lost or devalued savings) or unable to develop a sustainable saving habit.

Insurance. Insurance can be fundamental to ensuring medium- and long-term financial security and offers protection against unexpected fluctuations in income or expenditure. In many modern societies, several insurances have become so important that they are now mandatory (e.g., traffic liability insurance, health insurance, etc.). However, there is no clear definition of which types of insurance are essential so that the lack of

a particular insurance does not necessarily indicate exclusion. The discussion on insurance is therefore somewhat different than those relating to banking, credit, and savings. For this analysis, we understand insurance inclusion as the ability to access appropriate health, disability, and home contents insurance products (e.g., affordable premiums, appropriate coverage, and suitable payment method).

Examining Financial Exclusion. To understand why many fintech innovations are touted game-changers for enhancing financial inclusion, it is necessary to first understand the intricacies of financial exclusion in detail. Most importantly, we need to comprehend who remains excluded and why.

Poorer people account for a disproportionate share of the unbanked population worldwide, with half of the unbanked adults coming from the poorest 40% of households (Demirguc-Kunt et al. 2018; World Bank Group 2017). The pattern varies strongly across economies, however. In those where the unbanked population is generally very high, unbanked people are as likely to come from poorer households as they are from wealthier ones, signalling distrust or other systemic problems with local financial markets. In countries with an unbanked population of 25% or lower, however, adults who are unbanked are much more likely to suffer from financial poverty. They are also more likely to have been deprived of educational opportunities: globally, only one third of unbanked adults have completed high school or post-secondary education.

To shed light on why so many people are excluded from financial access, World Bank researchers conducted the Global Findex survey (Demirguc-Kunt et al. 2018). The most common reason for being financially excluded was *having too little money* to use an account, a response that links to the observation of poorer households being excluded more often. Two-thirds of study respondents cited this as at least one of the reasons, with about 20% stating this was the sole reason for being unbanked. About 25% declared *cost* and *distance to providers* as reasons for exclusion, and a similar share mentioned that they do not have an account because another member of the household already had one. Other frequently mentioned reasons related to a *lack of documentation*, *distrust* in the financial system, and *religious concerns*.

Up to this point, we have depicted financial inclusion and exclusion as two states—having and not having access to bank accounts, access to appropriate credit, and so on. This description is also common

in academic research or policy analyses. More critically, such analyses typically suggest a unidirectional nature for the exclusion-inclusion continuum, implying that there is a threshold that needs to be crossed just once in order to ‘join the banked’ (e.g., by opening an account). However, there are also conceptualisations of financial exclusion as a more dynamic phenomenon. Elaine Kempson and Claire Whyley found that it is not uncommon for households to close bank accounts if their immediate circumstances change (Kempson and Whyley 1999). Similar evidence was found for other financial products such as saving accounts or home contents insurance. This indicates that people who are financially included might revert to being excluded at a later point in time.

It also indicates that sometimes, there is a choice involved in accessing and using even the four essential financial products. The use of protective services (e.g., insurance beyond the mandatory ones), for example, largely depends on an individual’s perception of risk. Some people choose to remain without insurance because they feel they will never need it or because they are generally more venturesome than others. Similarly, there is ample evidence signifying that many people are averse to borrowing and make a conscious decision not to take use credit. Financial exclusion, then, occurs for a variety of reasons ranging from companies outright refusing to accept certain households as their customers all the way to people who ‘self-exclude’ by making a conscious and unconstrained choice not to access or use financial products. Oftentimes, however, the barrier between direct and voluntary exclusion are blurred and people face systemic barriers that encourage self-exclusion. The *perceived extent* of individual choice is therefore another important element when analysing financial exclusion.

THE FINTECH OPPORTUNITY

Globally, technological innovations are transforming how people engage with money and finance. The fintech innovation movement has accelerated throughout the COVID-19 pandemic, attracting record sums in research and venture funding. A frequent prediction, endorsed by academics, businesses, and policymakers alike, is that fintech will revolutionise financial inclusion as it offers a whole new tool kit for addressing the intractable problems that are typically causing exclusion from finance. We follow the Financial Stability Board in defining fintech as ‘technology-enabled innovation in financial services that could result in new business

models, applications, processes, or products with an associated material effect on the provision of financial services’.

The application of technology in finance is not new, but the current wave of innovation proves to be a step change. New applications are mobile-first, customer-centric, and disruptive to previously unchallenged ways of the sector. These innovations are built on a financial technology stack that is still evolving at a rapid pace. Artificial intelligence and machine learning, cloud computing, open application programming interfaces, and blockchain are among the technologies expected to have the greatest impact. But how exactly can fintech help to address the intricate problems that we have highlighted in previous sections of this chapter? To answer this question, we connect fintech technologies and business models to the most common reasons for financial exclusion as identified by the 2017 Findex survey and exemplify their potentially game-changing effects.

Spatial Barriers. The concept of financial exclusion was first used to describe geographical barriers to financial access, such as the distance to (or complete lack of) bank branches or other essential infrastructure within reach of a community. While the term’s meaning has evolved significantly over the years, the problem from which it initially emanated often remains—about a quarter of unbanked adults mentioned distance to providers as a reason for being excluded (Demirguc-Kunt et al. 2018).

The increasing adoption of mobile and smartphones paired with fintech innovations, however, open unprecedented opportunities to address this issue. A simple mobile phone can potentially open access to a mobile money account and eliminate the need to travel long distances to a financial institution (if this was even possible). Popular mobile phone-based services allow users to deposit money into an account stored on their phones, transfer money via text message (e.g., to pay for goods or send money to friends), and access credit. Having access to a smartphone and the internet expands the range of possibilities even further. This is significant given that about two-thirds of the unbanked population globally have access to a mobile phone—and adoption of devices continues to soar across the globe.

Cost. Historically, financial services firms have relied on a network of brick-and-mortar branches that was expensive to operate. Recent fintech innovations and the growing adoption of digital banking services, however, are making more and more branches (and the costs associated with them) obsolete. Through fintech, similar inefficiencies can be

addressed along the finance value chain, for example where disconnected, rigid technology systems are replaced by more agile cloud-based solutions, or when previously time-intensive, manual tasks that are typical for finance businesses (e.g., searching, matching, comparing, filling forms, reviewing, and other rules-based back-office activities) are automated through artificial intelligence, machine learning, and robotic process automation. These cost reductions potentially make financial products and services more affordable to low-income consumers.

Other innovations, including many blockchain-based services, try to disintermediate various aspects of financial services and promise further cost reductions across payments, capital markets, trade services, and wealth management. There is also the notion of using artificial intelligence paired with complementary technologies (e.g., sensors or tracking apps) to make predictions more accurate and further individualise pricing. For many insurances, for example, businesses are trying to enable customers to directly influence the price of their policies (e.g., by driving more carefully people could lower their traffic liability premiums, by eating healthier or doing more sports they could lower their health insurance premiums and so on).

Lack of Trust. While the exact figure varies widely across regions, an average of about 16% of financially excluded adults cite a lack of trust in financial providers as a reason for being unbanked (Demirguc-Kunt et al. 2018). And the mistrust towards banks and other providers has only been growing—fuelled by oblique fees, questionable behaviour, and full-blown scandals. In the aftermath of the 2008 financial crisis, for example, distrust in financial institutions spread rapidly around the globe (Sapienza and Zingales 2012).

Fintech innovators used this trust crisis to their advantage and quickly legitimised new technologies, products, and business models. Many tech-driven companies are aiming to increase transparency and encourage competition by building digital marketplaces that allow for easier comparisons between providers. Others introduce solutions that make banks (and therefore trust in them) redundant altogether, for example through peer-to-peer lending platforms or blockchain-based digital wallets. Hence, fintech offers a range of alternatives to individuals who have preciously renounced financial access due to a lack of trust in traditional providers.

Lack of Documentation. Documentation requirements continue to be a major barrier to account ownership in many economies. Several fintech companies are working on digital identification services which can

provide a critical enabler for alleviating this issue. Such services allow users to digitally store a recognised form of identification on their phone. This digital ID can be authenticated unambiguously through digital channels (e.g., a central database that is accessible to select institutions). It can be used to unlock access to finance, but also government services, education, and other critical services (White et al. 2019). Other innovations, such as cryptocurrencies, remove the need for documentation altogether and allow everyone with access to the internet to participate in peer-to-peer transactions without central institutions acting as intermediaries.

Financial Literacy and Capability. Knowledge and understanding of financial products as well as financial skills and the confidence to apply them are crucial elements of financial inclusion. They directly relate to the perceived extent of choice that we discussed earlier in this chapter: without appropriate levels of financial literacy and capability, individuals are discouraged from accessing (potentially more appropriate) financial services and oftentimes revert to self-exclusion.

Fintech offers new opportunities to make financial education more engaging and effective. The sector has developed successful solutions for digitally improving financial literacy through features such as video lessons, flashcards, quizzes, simulations, and games. Many of these tools are tailored towards children and young adults, trying to build capability and good habits from a young age. Well-designed applications educate their users about finance and help them make the right decision for themselves.

Poverty. Financial poverty remains the most common and intractable cause for financial exclusion. Almost two-thirds of World Bank survey respondents stated having too little money as a reason for being excluded, with 20% citing it as the sole reason for not accessing any form of financial services. Financial exclusion itself, however, is often a contributor to poverty since exclusion often severely limits economic and educational opportunities.

Poverty is an extremely complex, multifaceted concept, and discussing its intricacies is beyond the scope of this chapter. And fintech will certainly not eradicate poverty (particularly extreme poverty), but it shows the potential to alleviate the issue for a significant share of unbanked or underbanked individuals. Innovators have flooded the market with tools that help with personal financial management and budgeting. Applications help consumers identify opportunities to reduce expenditure and maximise their income, for example by identifying benefits eligibility or

by providing automated money guidance. Moreover, fintech can play an important role in poverty prevention. By combining financial and non-financial data, for example, machine learning algorithms can potentially uncover early warning signs of financial vulnerability that humans might not be able to identify.

SUCCESS STORIES: HOW FINANCIAL INCLUSION CAN BE PROFITABLE AND SOCIALLY PRODUCTIVE

As illustrated, fintech creates a range of opportunities to drive social change and increase financial inclusion. Crucially, it allows businesses to address these societal problems in ways that go beyond philanthropy or corporate social responsibility. Rather, their motivation is increasingly business-driven as new technologies allow them to tap into these unserved and underserved markets in economically viable ways. There are plenty of success stories outlining how fintech firms successfully created both economic and social value. In this section, we summarise some of them to illustrate how financial inclusion can be a profitable business opportunity.

Kenya. M-PESA in Kenya provides a prime example of how mobile technology can successfully deliver financial services to the unbanked. As recently as 2006, more than 80% of the Kenyan population was working with cash only and as few as 10% had bank accounts. A major reason for this was that two-thirds of the population lived in rural areas, but an overwhelming majority of bank branches and cash machines were in urban centres. If city workers wanted to send money to their families living in villages, they had to seal their wages in an envelope and send cash by post. Mobile phone adoption, however, was very high, and telecommunications providers had established a vast network of agents including retail outlets and airtime resellers. The availability of this infrastructure had led Kenyans to treat airtime as a substitute currency: minutes were easy to purchase, store, transfer, and sell.

In 2007, as part of a financial deepening initiative, telecom operators Safaricom and Vodafone launched their money transfer service M-PESA (Ndung'u 2018). Initially, the idea was to make it easier for microfinance borrowers to receive and repay loans while simultaneously allowing lenders to offer more competitive rates. During the piloting phase, however, Safaricom and Vodafone noticed the use of airtime as a medium of exchange. Additionally, they realised that customers were frequently repurposing the product to send remittances to friends and

families. They changed M-PESA's value proposition and turned it into a huge success. M-PESA now allows its users to deposit and withdraw money at local telecom retailers, transfer money to other users, pay bills, purchase minutes, and deposit money into a virtual savings account. By 2016, about 96% of households in Kenya were using M-PESA, and the service had lifted 194,000 households out of poverty (Suri and Jack 2016).

China. China has become one of the world's premier financial technology markets, leading the race in product innovation, market size, and consumer adoption (Patwardhan 2018). While the Chinese fintech sector began with thousands of companies introducing innovative products to the market, it has recently consolidated around China's internet giants. Alibaba, Tencent, and JD have leveraged their nationwide e-commerce infrastructure to provide a variety of financial services to their vast customer bases. Interestingly, these firms have focused on extending financial access (and access to credit in particular) to the historically excluded countryside, where the adoption of smartphones and internet access have recently skyrocketed. The tech-companies created financial products that seamlessly integrated with their existing solutions, a move that boosted adoption. Moreover, they can draw on the massive amounts of data collected through their existing online businesses to assess credit risk. This is a step change for rural areas, where traditional institutions often struggled to assess risk and provide loans due to a dearth of financial information (Kong and Loubere 2021).

The results of China's digital finance revolution are astonishing. In 2016, the total value of mobile payments exceeded \$790 billion—11 times more than that of the United States (Woetzel et al. 2017). Crucially, the number of non-bank digital payments in rural China grew by a staggering 93% from 2017 to 2018, indicating rapid adoption and use of fintech tools among previously excluded consumers.

Scotland. Issues of financial exclusion and vulnerability are of course not limited to developing economies. In the United Kingdom, for example, there are still approximately 1.2 million individuals without access to the most basic financial services. Additionally, over 11 million adults from a wide range of demographics (e.g., young people, over 80-year olds, people with disabilities, people with mental health issues, people of faith, and migrants and refugees) are underserved. A large share of excluded and underserved individuals are people on low income.

The Scottish fintech firm InBest.ai has recognised that many people could be better off but miss out on some or all the benefits they are eligible for. Their research found that this problem existed for as many as 8 million households across the United Kingdom, with about £16 billion in benefits being overlooked. The reasons for not taking up benefits were diverse: almost half of InBest's customers had simply assumed they weren't entitled, another 39% were unaware of their benefits, and about a fifth struggled with the complexity of the application process. The firm developed a benefits calculation platform that would help vulnerable consumers to understand, apply for, and monitor their benefits. The platform is integrated into the workflows of partner companies (e.g., financial institutions, debt advice providers, etc.) with services customers were already using. This contributed to a seamless customer journey and data sharing with other stakeholders in the support ecosystem.

The company found that 70% of its customers could claim an additional £500 per month. For 5% of their customers, they identified a staggering £1,500 of unclaimed monthly benefits. InBest quickly became a success and a valuable tool to the Scottish support network. By helping financially vulnerable households to maximise their income, InBest increases their financial resilience, avoids over-indebtedness, and potentially prevents financial poverty.

PUBLIC SECTOR-LED APPROACHES TO FINTECH FOR FINANCIAL INCLUSION

In the previous section, we have described how fintech businesses can address societal problems through a commercial logic. Such approaches are usually positioned under the umbrella of social innovation, a concept that appears in various academic disciplines, including sociology (Zapf 1991), creativity (Mumford 2002), entrepreneurship (Swedberg 2009; Ziegler 2010), and welfare economics (Jenson 2015). While conceptualisations within and across these fields vary, they generally share the idea that social innovation includes a form of reconfiguration that causes a macro-level social change. Crucially, it is not considered the prerogative or privilege of businesses but can also be introduced by NGOs or governments.

Many administrations are increasingly embedding fintech in government services, for example to distribute subsidies, unemployment benefits, or welfare payments. Most governments are also experimenting

with standalone public sector financial technologies. Some of the most promising government-driven fintech innovations are central bank digital currencies (CBDCs). CBDCs are an exclusively digital form of central bank issued money made accessible to the broad public (Bindseil 2020). While there are several technological approaches to CBDCs, the most prominent one was inspired by Bitcoin and similar blockchain-based cryptocurrencies. However, CBDCs would differ from those ‘private’ digital currencies in that they would operate on a distributed but centrally controlled database (managed and maintained by the respective central bank or government) rather than on a decentralised system.

The advantages expected from CBDCs range from improved technological efficiency (Bindseil 2020) through easier tax collection processes and all the way to having new channels for monetary policy (Heller 2017). CBDCs could also enable governments to make huge strides towards financial inclusion. Governments could, for example, offer safe money accounts at the central bank for free (or at very low cost) to every citizen or legal resident. This could constitute a strong instrument for financial inclusion, connecting all legal residents to a secure, digital payments system without facing many of the traditional exclusionary issues. Unsurprisingly, about 80% of all central banks are currently exploring central bank digital currencies, with some of them having progressed into pilot phases (Galbraith and Shen 2022).

FINTECH FOR FINANCIAL INCLUSION—A DOUBLE-EDGED SWORD?

So far, we have illustrated that fintech innovations have led to significant progress around financial inclusion and that there is much more to be excited about. However, the potentialities we have outlined in this chapter only show one side of the fintech coin and are accompanied by a range of socio-political risks that require thorough consideration going forward. We are worried that current narratives of ‘fintech for social good’ legitimise a form of techno-solutionism, that is, the flawed idea that any social problem, no matter how complex, has a technological fix (Morozov 2013). Financial technology should not be framed as a panacea to the intractable, multifaceted issues that excluded individuals often face. We suggest analysing the downsides of fintech from three angles: first, we employ a sociocultural lens and contend that the increasing digitisation of essential services creates a significant risk of exacerbating existing and

creating new forms of financial and social exclusion. Second, we shed light on the power structures that are embedded in and further enabled by the technologies underlying many fintech innovations. Finally, we question the motivations and ideologies behind some of the initiatives that drive fintech adoption among previously unserved consumers.

Sociocultural Factors and Contradictory Effects. In a previous section, we have matched fintech potentialities to common causes of financial exclusion (spatial barriers, cost, lack of trust, lack of documentation, financial literacy and capability, and poverty). There are, however, potentially adverse effects involved in applying fintech to these problems as well. The increasing digitisation of financial services, for example, can help to overcome existing spatial barriers, but also create new ones. Digital finance has led to the closure of a significant number of bank branches, potentially excluding technology-averse individuals. The withdrawal of mainstream financial institutions is most pronounced in rural (and often deprived) areas, where underappreciated hurdles relating to broadband availability, network signals, and data poverty¹ amplify its exclusionary effects. At worst, this aggravates existing inequalities, expands the digital divide, and further isolates vulnerable groups.

Earlier we have pointed towards the opportunity of fintech to improve financial literacy and capability through methods like gamification. This potential should not obscure the fact that most fintech applications themselves require high levels of financial and digital capability, thereby reinforcing exclusion. In some of our own research, we found vulnerable consumers often feel excluded from existing fintech services as they struggle to make sense of new product and service offerings. Further, attempts to ‘educate’ marginalised consumers are often patronising and the complexity of technological jargon in combination with overused buzzwords act disengaging.

The new, data-hungry applications might also create new drivers of financial exclusion. If algorithms make credit or insurance decisions, for example, then accessing these products requires an extensive data history. People who suffer from data poverty or deliberately avoid leaving a data trail, then, might be disadvantaged and denied access to these essential services. Individuals might have no choice but to establish a data history

¹ Data poverty occurs where disadvantaged groups cannot afford to purchase enough data to access online services.

(at the expense privacy) if they want to evade unfair price discrimination or exclusion.

Technological Politics. A holistic understanding of fintech risks requires a closer look at the technologies that are at the core of the global fintech movement, and the politics they potentially enable. Central bank digital currencies, for example, might enable governments to equip their citizens with cheap access to transaction accounts but also represent a potentially troubling encroachment on consumer privacy. Such government-issued accounts would provide new tools for surveillance and new means to assert control. Imagine, for example, that the fine for a parking violation would be taken out of your account automatically. What would stop governments from weaponising this power by freezing accounts or blocking lawful transactions of government critics or other people who have fallen into disfavour? If implemented without well-designed privacy protection mechanisms, CBDCs might lead to (self-) censorship and regressive social developments.

Other concerns can be found in the field of artificial intelligence. AI has been subject to increased criticism highlighting the issue of biased algorithmic decision-making and how it might lead to unjust or prejudicial treatment of marginalised groups based on race, gender, disability, religion, income, or other characteristics historically associated with discrimination (Buolamwini and Gebru 2018; Tsamados et al. 2021; Zou and Schiebinger 2018). By delegating decisions about who receives credit, who is eligible for benefits, or who pays what for insurance to an algorithm, we are running the risk of automating inequality and restricting peoples' access to public resources rather than providing greater support (Crawford 2021). The citizens of Michigan experienced this problem at first hand when former Republican governor Rick Snyder introduced algorithmically driven austerity programmes. Between 2012 and 2015, one of the programmes misidentified nineteen thousand citizens as 'fugitive felons' and automatically disqualified them from food assistance. The other one inaccurately identified forty thousand Michigan residents as defrauding the state's unemployment insurance system, many of whom had to declare bankruptcy due to hefty civil penalties, the seizure of tax refunds, and the confiscation of wages (Richardson et al. 2019). Crawford (2021) details how AI-systems are designed to serve and reinforce existing systems of power, and how they fuel a shift to undemocratic governance whose potential implications we must consider when evaluating fintech for financial inclusion.

Ideological Factors and Finance-led Capitalism. There is increasing suspicion towards both the intentions and methods of organisations that are addressing social ills through business logics. This suspicion is certainly justified. The recent history of international development initiatives is littered with hyped-up innovations that were touted game-changers in the fight against poverty (e.g., microcredit). Many of these innovations, unfortunately, were shown to be ‘quite ineffective and only really promoted for ideological, political, or narrow profiteering reasons’ (Bateman et al. 2019, p. 482).

A closer look at the success story of M-PESA, for example, reveals a near-monopolistic provider who is sometimes condemned for imposing high prices on its financially vulnerable users (Bill and Melinda Gates Foundation 2013). Critics go as far as to accuse M-PESA of employing extractive practices that generate large profits through taxing payments that would have been free if cash was used (Bateman et al. 2019). There is an argument to be made that, much more than its marginalised user base, it was Safaricom that has benefitted from M-PESA. (Wyche et al. 2016).

Understanding poverty as a new frontier for profit-making and accumulation carries the risk of equating financial inclusion and financialisation (Bayliss et al. 2017), and the growing push for applying information technologies to problems of exclusion potentially confines policy-making to an increasingly powerful digital elite that experiences little contestation from global development players. The digitalised approach to financial inclusion encourages practices that delineate marginalised and excluded individuals into categories of ‘borrowers’ and sometimes gives the impression that incorporating these consumers into global strategies of capital accumulation, not lifting them from poverty, is the overarching goal of these initiatives (Gabor and Brooks 2017).

CONCLUSION

This chapter provides a comprehensive overview of the opportunities that financial technology introduces to the global financial inclusion agenda. We have illustrated that recent fintech innovations have the potential to be a step change as they offer new tools to directly tackle common causes of financial exclusion, including spatial barriers, high costs, a lack of trust in traditional financial providers, a lack of documentation, financial

literacy and capability, and poverty. Nevertheless, we need to acknowledge that fintech also poses risks to financial and social exclusion of which we need to remain cognisant. Only then can we ensure fintech is socially productive and alleviates these intractable issues rather than exacerbating them.

REFERENCES

- Bateman, M., Duvendack, M., & Loubere, N. (2019). Is fin-tech the new panacea for poverty alleviation and local development? Contesting Suri and Jack's M-Pesa findings published in Science. *Review of African Political Economy*, 46(161), 480–495. doi:<https://doi.org/10.1080/03056244.2019.1614552>
- Bayliss, K., Fine, B., & Robertson, M. (2017). Introduction to special issue on the material cultures of financialisation. *New Political Economy*, 22(4), 355–370.
- Bill and Melinda Gates Foundation. (2013). *Fighting poverty, profitably: Transforming the economics of payments to build sustainable, inclusive financial systems*. Bill and Melinda Gates Foundation. Retrieved from: <https://docs.gatesfoundation.org/Documents/Fighting%20Poverty%20Profitably%20Full%20Report.pdf>
- Bindseil, U. (2020). Tiered CBDC and the financial system. Available at SSRN 3513422.
- Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Paper presented at the Conference on fairness, accountability and transparency.
- Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. New Haven: Yale University Press.
- Demirguc-Kunt, A., Klapper, L., Singer, D., & Ansar, S. (2018). *The global finance database 2017: Measuring financial inclusion and the fintech revolution*: World Bank Publications.
- Emran, M. S., & Farazi, S. (2009). Lazy banks? Government borrowing and private credit in developing countries. *Government borrowing and private credit in developing countries (June 11, 2009)*.
- Gabor, D., & Brooks, S. (2017). The digital revolution in financial inclusion: international development in the fintech era. *New Political Economy*, 22(4), 423–436. doi:<https://doi.org/10.1080/13563467.2017.1259298>
- Galbraith, A., & Shen, S. (2022). China central bank launches digital yuan wallet apps for Android, iOS. *Reuters*. Retrieved from: <https://www.reuters.com/markets/currencies/china-cbank-launches-digital-yuan-wallet-apps-and-roid-ios-2022-01-04/>

- Heller, D. (2017). *The implications of digital currencies for monetary policy*. European Parliament. Retrieved from: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_IDA\(2017\)602048](https://www.europarl.europa.eu/thinktank/en/document/IPOL_IDA(2017)602048)
- Jenson, J. (2015). Social innovation: redesigning the welfare diamond. In *New frontiers in social innovation research* (pp. 89–106): Palgrave Macmillan, London.
- Kempson, E., Crame, M., & Finney, A. (2007). Financial services provision and prevention of financial exclusion. *Eurobarometer Report, University of Bristol*, 447–465.
- Kempson, E., & Whyley, C. (1999). *Kept out or opted out? Understanding and combating financial exclusion*.
- Kong, S. T., & Loubere, N. (2021). Digitally down to the countryside: Fintech and rural development in China. *The Journal of Development Studies*, 57(10), 1739–1754. doi:<https://doi.org/10.1080/00220388.2021.1919631>
- Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. Public Affairs.
- Mumford, M. D. (2002). Social innovation: Ten cases from Benjamin Franklin. *Creativity Research Journal*, 14(2), 253–266.
- Ndung'u, N. (2018). Chapter 3—The M-pesa technological revolution for financial services in Kenya: A platform for financial inclusion. In D. Lee Kuo Chuen & R. Deng (Eds.), *Handbook of blockchain, digital finance, and inclusion, Volume 1* (pp. 37–56). Academic Press.
- Patwardhan, A. (2018). Chapter 4—Financial inclusion in the digital age. In D. Lee Kuo Chuen & R. Deng (Eds.), *Handbook of blockchain, digital finance, and inclusion, Volume 1* (pp. 57–89): Academic Press.
- Richardson, R., Schultz, J. M., & Southerland, V. M. (2019). Litigating algorithms 2019 US report. *AI Now Institute*. Retrieved from <https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf>
- Sapienza, P., & Zingales, L. (2012). A trust crisis. *International Review of Finance*, 12(2), 123–131.
- Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science*, 354(6317), 1288–1292.
- Swedberg, R. (2009). Schumpeter's full model of entrepreneurship: Economic, non-economic and social entrepreneurship. *An introduction to social entrepreneurship*, 77–106.
- Tsamados, A., Aggarwal, N., Cows, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2021). The ethics of algorithms: Key problems and solutions. *AI & SOCIETY*. doi:<https://doi.org/10.1007/s00146-021-01154-8>
- White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., & Sperling, O. (2019). *Digital identification: A key to inclusive growth*. McKinsey Global Institute. Retrieved from: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>

- Woetzel, J., Seong, J., Wang, K. W., Manyika, J., Chui, M., & Wong, W. (2017). Digital China: Powering the economy to global competitiveness. *McKinsey Global Institute*, 17.
- World Bank Group. (2017). *Global financial inclusion and consumer protection survey, 2017 report*. <https://openknowledge.worldbank.org/handle/10986/28998>
- World Bank Group. (2018). *Financial inclusion: Financial inclusion is a key enabler to reducing poverty and boosting prosperity*. Retrieved from: <https://www.worldbank.org/en/topic/financialinclusion/overview#1>
- Wyche, S., Simiyu, N., & Othieno, M. E. (2016). Mobile phones as amplifiers of social inequality among Rural Kenyan women. *ACM Transactions on Computer-Human Interaction*, 23(3), Article 14. <https://doi.org/10.1145/2911982>
- Zapf, W. (1991). The role of innovations in modernization theory. *International Review of Sociology*, 2(3), 83–94.
- Ziegler, R. (2010). Innovations in doing and being: Capability innovations at the intersection of Schumpeterian political economy and human development. *Journal of Social Entrepreneurship*, 1(2), 255–272.
- Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist—It’s time to make it fair. *Nature*, 559, 324–326.

INDEX

A

Agency resource constraints, 89
Algorithms, 27, 30, 31, 38, 39, 164, 168, 169
An Investment contract, 126
Anonymization, 40
Anti-Money Laundering (AML), 12, 18–22, 41, 45, 58, 59, 63, 65, 67, 107
Artificial intelligence (AI), 10, 12, 13, 26, 34, 40, 44, 81, 161, 162, 169
ASEAN, 4, 97–100, 102, 113, 114, 146–148, 154

B

Big Data, 12, 26, 31, 114, 153
Big technology (BigTech), 9, 14, 15, 17, 23
Bitcoin, 26, 40, 41, 65, 102–104, 106, 107, 111, 132, 133, 136–142, 144, 150–153, 167
Blockchain, 7, 10, 26, 40, 41, 45, 90, 98, 108, 117, 119, 123, 126,

129–132, 134, 138, 143, 146, 161, 162, 167
Blockchain technology, 4, 40, 90, 105, 108, 110, 139
Bribery, 5, 52, 55, 56, 58, 76

C

Central Bank Digital Currency (CBDC), 6, 7, 18, 97, 102, 115, 119, 134–136, 167, 169
Characteristics, 3, 28, 36, 44, 57, 72, 81, 91, 118, 119, 122, 123, 125, 127–129, 131, 133, 134, 136, 140, 144, 145, 147, 149–152, 154, 156, 169
Classifications, 108, 120–122, 150, 152
Collaboration-oriented approach, 82, 85, 91, 92
Consent, 31, 32, 34, 37, 38, 44, 63
Consumers, 2, 3, 5, 7, 9, 11–14, 17, 23, 25–27, 38, 39, 43, 70, 71, 79, 80, 85, 86, 101, 107, 108,

117, 121, 137, 138, 148, 149,
162, 163, 165, 166, 168–170

Corruption, 5, 52, 55–57, 76

Credit, 4, 6, 12, 14–16, 53, 82, 89,
90, 94, 98, 139, 156–161, 165,
168, 169

Cross-border data flows, 42

Crypto assets, 7, 103, 104, 108,
117–128, 133, 135–137, 139,
141, 143, 146–148, 150,
152–154

Cryptocurrency, 6, 8, 18, 26, 40, 41,
45, 80, 89, 97, 103–106,
111–114, 131, 132, 136, 140,
141, 143–145, 151, 152

Cybercrime, 5, 52–54, 76

Cybersecurity, 13, 39, 45

D

Data localization, 36, 44

Data privacy, 5, 11, 17, 26, 27, 33,
39, 40, 42–46

Data processing, 26, 29, 31–36, 39,
42–44, 46

Data protection, 5, 12, 18, 28, 31,
32, 39, 42, 43, 115

Data storage, 32, 131

Detection, 5, 26, 41, 52, 60, 61, 65,
68, 71–73, 75, 76

Developing countries, 2, 4, 99, 101

Digital assets, 5, 7, 55, 97–99,
101–103, 105, 106, 108–111,
113, 115, 117–119, 126–128,
133, 146–150

Digital banking, 18–22, 161

Digital economy, 5, 51, 55, 68, 70,
71, 77, 88, 114

Digital money, 102, 140, 141, 151

Digital tokens, 98, 102, 104, 106,
107, 110, 112, 113, 117, 121,
145–147, 150–152

E

Economic growth, 99, 101, 156

Electronic money, 18–22, 118, 135

Equity Crowdfunding, 18–22

F

Financial, 1–5, 7–14, 16–18, 23,
25–27, 31, 37, 39, 41, 43–46,
52–55, 57–61, 64, 67, 68,
79–85, 87–93, 98–101, 103,
105, 106, 114, 120, 121, 126,
128, 135–137, 140, 146, 147,
150, 151, 155–168, 170, 171

Financial Conduct Authority (FCA),
85–87, 92, 119

Financial crime, 5, 51, 52, 55–57, 68,
76, 77

Financial fraud, 5, 51–53, 76

Financial inclusion, 2, 4, 7, 13, 97,
99–101, 146, 155, 156, 159,
160, 163, 164, 167, 169, 170

Financial institutions (FIs), 4, 10–14,
16, 17, 60, 66, 90, 106, 135,
136, 157, 158, 161, 162, 166,
168

Financialisation, 170

Financial literacy and capability, 163,
168, 171

Financial stability, 2, 5, 9–11, 13, 14,
17, 41, 97, 101, 107, 109

Financial technology (FinTech), 1–14,
17–19, 23, 51, 66, 79–88,
90–94, 98, 103, 105, 114, 115,
150, 155, 156, 161, 165, 167,
170

Fintech platforms, 13, 26, 27, 43

Fundraising, 83, 84, 93, 97–99, 105,
109, 142, 146

G

General Data Protection Regulation (GDPR), 28, 30–33, 35–37, 42, 44

H

The Howey test, 126, 127, 142

I

Illicit financial flow, 55, 57, 58, 66, 76
 Initial coin offering (ICO), 98, 104, 106, 109, 112–114, 147, 148, 150, 151, 154
 Innovation office, 2, 3, 6, 82, 85, 87, 88, 92, 94
 Insider trading, 52, 56–58

J

JOBS Act, 83, 84, 88, 92

L

Legal tender, 103, 110, 112, 114, 128, 137, 140, 148, 151, 152
 Legislative dysfunctionality, 89
 Lending, 12, 14, 18, 25, 80, 83, 84, 89, 93, 101, 132, 162

M

Machine learning, 10, 13, 40, 72–74, 81, 161, 162, 164
 Monetary functions, 123–125, 145
 Money laundering, 5, 7, 41, 51, 52, 58–61, 63–65, 67, 68, 71, 76, 104, 108, 117

O

Open banking, 14, 16, 18–22, 37

P

Peer to peer (P2P), 18, 40, 93
 Personal data, 5, 11, 26–38, 40–44
 Platforms, 3, 5, 11–13, 17, 26, 39, 45, 52, 71–74, 79, 83–85, 89–91, 101, 106, 112–114, 131, 141, 150, 152, 162, 166
 Poverty, 156, 159, 163–166, 168, 170, 171
 Principles-based regulatory regimes, 81
 Products, 4, 9, 11, 12, 25, 38, 53, 55, 67, 71, 81, 87, 89, 93, 101, 103, 104, 108, 113, 123, 124, 126, 127, 130, 139, 151, 156–165, 168
 Project Inthanon, 110
 Project Ubin, 108
 Public security, 43

R

Regulation, 2–8, 12, 14, 17–19, 23, 27, 29, 31–33, 35, 36, 42–44, 46, 59, 72, 81–85, 88–94, 98, 101, 102, 104, 105, 107, 109, 111–115, 118, 125, 127, 146–150, 153
 Regulators, 2–7, 9, 10, 14, 17, 18, 23, 30, 41, 43, 45, 60, 76, 80–94, 97–100, 102, 108, 109, 113–115, 117, 145–148, 150
 Regulatory implications, 145
 Regulatory innovation, 2, 6, 92
 Regulatory pendulum, 81
 Regulatory sandbox, 2, 3, 6, 80, 82, 85–88, 92, 94
 Regulatory Technology (RegTech), 3, 5, 6, 73, 75, 76
 Res incorporales, 128
 Restricted experimentation, 80
 Rights in rem, 127

Risk, 2, 3, 5, 7, 9–14, 17, 18, 23, 26, 39, 41, 45, 53, 66–68, 80, 81, 83–86, 89, 92–94, 98, 99, 101–106, 108, 109, 112, 114, 115, 117, 133, 146, 150, 152, 160, 165, 167, 169–171
 Robo advisory, 10
 Rules-based regulatory regimes, 81

S

Savings, 156–160, 165
 Securities, 7, 11, 13, 17, 18, 25, 26, 31, 32, 39–42, 45, 52, 56, 90, 94, 107–109, 112, 113, 115, 117, 121, 123, 125–130, 139, 142, 143, 145, 147, 148, 150–152, 158
 Self-regulation, 41, 45, 82, 89, 90, 92
 Small and medium-sized enterprises (SMEs), 4, 79, 98, 101
 Social exclusion, 158, 168, 171
 Social impact, 156
 Stablecoins, 7, 122, 132–134, 145, 148, 149, 152
 Standardization, 30, 44–46
 Supervision-oriented approach, 82–85, 88, 92
 Supervisory implications, 108, 122
 Sustainable Development Goals, 156

T

Taiwan FinTechSpace, 91
 Tax evasion, 5, 51, 52, 57, 58, 67–76
 Taxonomies, 118, 121, 135, 137
 TechFin, 81, 82
 Technology, 2, 10–14, 17, 25, 40, 46, 53, 65, 67, 70, 76, 81, 83, 84, 88, 90, 97–99, 101, 103, 105, 108, 114, 115, 118, 119, 133, 134, 160–162, 164, 168
 Terrorist financing, 5, 52, 54, 55, 57, 59, 65, 67, 76, 107
 Tokens, 7, 39, 98, 99, 104, 108, 112, 115, 117, 120–123, 127–134, 136, 139, 140, 142–144, 146–148, 151, 153, 154
 Too Big to Fail, 14, 86
 Too Large to Ignore, 14, 86
 Too Small to Care, 86

U

Unbanked, 79, 155–157, 159, 161–164
 Underbanked, 79, 156, 163

V

Virtual currency, 102, 107, 110, 111, 113, 140