



Helping Governments to
Leverage Financial Innovation



Commonwealth FinTech Toolkit

Helping Governments to Leverage
Financial Innovation



Australian Government

Department of Foreign Affairs and Trade



The Commonwealth



© Commonwealth Secretariat 2020

All rights reserved. This publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or otherwise provided it is used only for educational purposes and is not for resale, and provided full acknowledgement is given to the Commonwealth Secretariat as the original publisher.

Views and opinions expressed in this publication are the responsibility of the author(s) and should in no way be attributed to the institutions to which they are affiliated or to the Commonwealth Secretariat.

This project was part-financed by the Government of Australia, Department of Foreign Affairs and Trade and Australian Aid.

Wherever possible, the Commonwealth Secretariat uses paper sourced from responsible forests or from sources that minimise a destructive impact on the environment.

Printed and published by the Commonwealth Secretariat.

Preface

The Commonwealth Secretariat has developed the Commonwealth FinTech Toolkit in response to a specific request from the Commonwealth Central Bank Governors (CCBGs). Recognising the growth and impact of technology-enabled financial services (fintech) in the Commonwealth, the Governors endorsed the development of a Commonwealth FinTech Toolkit at a meeting in October 2018.

The threefold aims of the Toolkit are to:

- provide technical guidance on fintech and fintech applications, including using fintech to achieve development outcomes;
- set out a framework for creating enabling environments for fintech, including with appropriate legislation, regulation, institutions and policies; and
- build fintech capacity among government staff.

With support from the Australian Government's Department of Foreign Affairs and Trade, the Commonwealth Secretariat commissioned an expert group from Visionary Future LLC to help with this project.

Contents

Preface	iii
Abbreviations and Acronyms	ix
Executive Summary	xiii
Introduction	1
PART 1 Tech Topics	3
1 Digital Financial Services	5
1.1 Introduction	6
1.2 Context	6
1.3 Description	7
1.4 Key Considerations for Future Development	12
Endnotes	15
2 Artificial Intelligence	19
2.1 Introduction	20
2.2 Context	20
2.3 Description	20
2.4 Key Considerations for the Future	23
Endnote	24
3. Blockchain and Financial Services	25
3.1 Introduction	26
3.2 Context	28
3.3 Description	29
3.4 Key Considerations for Future Development	32
Endnotes	33
4 Digital Identity	35
4.1 Introduction	36
4.2 Context	37
4.3 Description	39
4.4 Key Considerations for Future Development	41
Endnotes	43

5	Big Data/Big Data Analytics	45
5.1	Introduction	46
5.2	Context	46
5.3	Description	48
5.4	Key Considerations for Future Development	49
	Endnotes	50
6	Cybersecurity	53
6.1	Introduction	54
6.2	Context	54
6.3	Description	56
6.4	Key Considerations for Future Development	57
	Endnotes	57
	PART 2 Application and Action	59
7	Policy Interventions and Outcomes	61
7.1	Introduction	62
7.2	Financial Inclusion	63
7.3	Improved Cross-border Transactions and Trade	70
7.4	Improved Economic Growth	71
	Endnotes	73
8	Considerations	75
8.1	Introduction	76
8.2	Diversity among Commonwealth Nations	76
8.3	Small States: Opportunity and Challenge	77
8.4	Advanced Economies and Legacy Systems	78
8.5	Developing Economies	78
8.6	Regional Considerations	80
8.7	Conclusion	81
	Endnotes	82
9	Action Framework for Creating an Enabling Environment for Fintech	85
9.1	Introduction	86
9.2	Building an Effective Fintech Task Force	87
9.3	Creating an Enabling Environment for Fintech	89
9.4	Building on Success	99
	Endnotes	100

10 Case Studies	101
Case Study 10.1 The Journey of Emerging Technologies: Blockchain in Papua New Guinea	102
Case Study 10.2 Pioneering Mobile Money in Kenya	106
Case Study 10.3 Digital Assets Businesses in Bermuda	108
Case Study 10.4 Malta's Support for Virtual Financial Assets	111
Endnotes	114
Appendix 1 Commonwealth Government Interviews	115
Appendix 2 Methodology	117
Appendix 3 Findings	119
Contributors and Acknowledgements	121

Abbreviations and Acronyms

5AMLD	Fifth Money Laundering Directive (EU)
AAI	applied artificial intelligence
ADB	Asian Development Bank
AfDB	African Development Bank
AI	artificial intelligence
AML	anti-money-laundering
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
ASIC	Australian Securities and Investment Commission
ATM	automatic teller machine
BATs	Baidu, Ali Baba and Tencent
BIS	Bank for International Settlements
BMA	Bermuda Monetary Authority
BPNG	Bank of Papua New Guinea
BSBD	basic saving bank deposit
CARICOM	Caribbean Community
CBB	Central Bank of Bahrain
CBDC	central bank digital currency
CBK	Central Bank of Kenya
CCBGs	Commonwealth Central Bank Governors
CCP	central counterparty
CDR	consumer data right
CFT	countering the financing of terrorism
CGAP	Consultative Group to Assist the Poor
CPMI	Committee on Payments and Market Infrastructures (BIS)
CSD	central securities depository
DABA	Digital Assets Business Act 2018 (Bermuda)
DFAT	Department of Foreign Affairs (Australia)
DfID	Department for International Development (UK)
DFS	digital financial services
DIT	Department for International Trade (UK)
DLT	distributed ledger technology
ECCB	Eastern Caribbean Central Bank
ECCU	Eastern Caribbean Currency Union

X Abbreviations and Acronyms

EMI	e-money issuer
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority (UK)
FCP	financial consumer protection
FDC	Foundation for Development Cooperation
FIAU	Financial Intelligence Analysis Unit (Malta)
FMI	financial market infrastructure
forex	foreign exchange
FSB	Financial Stability Board
GAI	generalised artificial intelligence
GDP	gross domestic product
GDPR	General Data Protection Regulation (EU)
GFIN	Global Financial Innovation Network
GNP	gross national product
GPS	Global Positioning System
GPSDD	Global Partnership for Sustainable Development Data
GSMA	Global System for Mobile Communications
HFT	high-frequency trading
HKMA	Hong Kong Monetary Authority
HMRC	Her Majesty's Revenue and Customs (UK)
IADB	Inter-American Development Bank
ICO	initial coin offering
ICT	information and communications technology
ID	identity
IDB	Inter-American Development Bank
IFC	international finance corporation
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IP	Internet Protocol
ITAS	innovative technology arrangements and services
KYC	know your customer
KYCC	know your customer's customer
LEI	Legal Entity Identifier
MAS	Monetary Authority of Singapore
MDIA	Malta Digital Innovation Authority
MFSA	Malta Financial Services Authority

NBFI	non-bank financial institution
NI	National Insurance
NMSE	nano and micro sector enterprise
NPS	Net Promoter® Score
OECD	Organisation for Economic Co-operation and Development
P2P	peer-to-peer
PBD	privacy by design
PCS	payments, clearing and settlement
PESTLE	political, economic, social, technological, legal, environmental [analysis]
PIN	personal identification number
PIRI	Pacific Islands Regional Initiative
PMJDY	Pradhan Mantri Jan Dhan Yojana [National Mission for Financial Inclusion] (India)
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations 2018 (Malta)
PNG	Papua New Guinea
PPP	public-private partnership
PRC	People's Republic of China
PSD2	revised Payment Services Directive (EU)
QOS	quality of service
SCI	SEPA credit identifiers
SDGs	Sustainable Development Goals (UN)
SEPA	Single Euro Payments Area
SMEs	small and medium-sized enterprises
SSS	securities settlement system
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWOT	strengths, weaknesses, opportunities and threats
UBO	ultimate beneficial owner
UN	United Nations
USAID	US Agency for International Development
VC	virtual currency
VFA	virtual financial asset
VFA Act	Virtual Financial Assets Act 2018 (Malta)
VFA Regulations	Virtual Financial Assets Regulations 2018 (Malta)
WEF	World Economic Forum

Executive Summary

At the 2018 meeting of the Commonwealth Central Bank Governors (CCBGs), member countries recognised the growth and impact of technology-enabled financial services (fintech) on Commonwealth populations, and endorsed the development of a Commonwealth FinTech Toolkit.

The Governors noted demand for improved technical guidance regarding the implementation of fintech—an area with which many member countries are grappling. Acknowledging that some states are more advanced in this area than others, the Governors noted that it would be extremely useful for future action in this area if states were to share the lessons they had learned.

This Commonwealth FinTech Toolkit therefore includes:

- a resource bank of material that covers:
 - tech topics, such as artificial intelligence (AI), blockchain and cybersecurity; and
 - anticipated outcomes, such as greater financial inclusion;
- discussion of issues impacting on small nations and large nations;
- discussion of regional concerns (spanning Africa, the Americas, Asia Pacific and Europe);
- a framework for creating enabling environments for fintech; and
- case studies of four innovative fintech initiatives.

PART I Tech Topics

In Part I, we look at the ways in which emerging technologies are transforming financial services.

Chapter 1 Digital Financial Services

- Digital financial services (DFS) can unlock productivity and investment, reduce poverty, empower women and help governments to build stronger institutions with less corruption—all while offering a profitable, sustainable business opportunity for financial services providers.
- Digital financial services can include mobile services and other kinds of digital service.
- As well as new opportunities, DFS open up new risks and involve consumer protection issues, of which regulators need to be aware and which they must address.

Chapter 2 Artificial Intelligence

- Artificial intelligence is the technology that helps a machine to think like a person.
- Artificial intelligence is already being deployed both within banks, to interface with consumers and businesses, and within government itself.

- Machine learning—a particular type of AI—has offered new opportunities in financial services and shaped new offerings.
- Inevitably, however, with new opportunity comes new risks and regulators need to address these proactively.

Chapter 3 Blockchain and Financial Services

- Blockchain is a type of peer-to-peer (P2P) database that uses data 'blocks', all of which update one another automatically as they grow, to build an immutable (permanent) record.
- It is both more secure than other forms of database (because it is harder to insert bad data) and more user-friendly (because it makes it easier to access that data).
- As a distributed ledger technology (DLT), blockchain allows parties who do not necessarily trust each other to co-operate towards shared outcomes, which is useful in a number of financial services applications.
- Central banks have both proposed and trialled a range of blockchain experiments, ranging from land registry to introducing their own central bank digital currencies (CBDCs).¹

Chapter 4 Digital Identity

- Digital identity is a keystone issue in helping an additional 1.1 billion people—mostly in Africa and Asia—to access financial services. The World Bank has highlighted the introduction of robust, inclusive and responsible digital identification systems as a

priority action with the potential to progress many of the United Nations Sustainable Development Goals (SDGs), including aspects such as social protection, the empowerment of women and girls, financial inclusion, governance, digital development and humanitarian assistance.

- Analogue, paper-based identity systems are siloed and inflexible, exacerbating financial exclusion. Digital identity systems remedy many of these effects.
- Experiments with digital identity are being conducted across the Commonwealth, with an emphasis on federated (versus centralised) approaches.
- Public consultation prior to introducing a new identity system is key to its success. It allows users to make valuable comment on the system's design, and it builds their trust and confidence in the system, which can help to drive its adoption.

Chapter 5 Big Data/Big Data Analytics

- Big data/big data analytics is the lifeblood of AI, because it is what fuels AI algorithms.
- Big data is evaluated in terms of its volume, velocity, variety, veracity and value.
- Financial institutions use big data/big data analytics for activities ranging from marketing to credit assessment.
- Big data/big data analytics introduce new risks in financial services if not partnered with digital identity systems (see above) because their widespread

adoption could otherwise exacerbate financial exclusion.

Chapter 6 Cybersecurity

- Cybersecurity is a serious and widespread challenge for financial services, with significant impact on both consumers and businesses.
- Commonwealth member countries must invest in both technology and training.
- A disciplined cybersecurity approach will look at systems, people and processes, and the 2018 Commonwealth Cyber Declaration enshrines these key principles.²

PART II Application and Action

Having explored six of the key technologies that shape fintech, we look in Part II at how member countries can use those technologies to achieve their development goals.

Chapter 7 Policy Interventions and Outcomes

Three common policy objectives readily illustrate the relevance and applicability of fintech.

Financial inclusion is both a result of and can result in:

- stronger consumer protection;
- lowered costs of complying with anti-money-laundering (AML) and know your customer (KYC) rules;
- increased levels of financial and data literacy;
- inclusion of those with historically marginalised identities; and
- lower rates of identity theft.

Recommended actions include promoting financial education and the role of financial literacy in developing financial health among the underserved to increase pull from the demand side, and developing incentives or a facilitative regulatory environment that encourages private sector actors to invest in supplying a broader range of products.

Despite the significant social and economic imperatives for women's economic inclusion, gender issues are rarely, if ever, factored into national development strategies, including national financial inclusion strategies. In addition, then, the design and implementation of all of these strategies should be assessed through a 'gender lens'.

Likewise, **improved cross-border transactions and trade** both result from and result in:

- lowered costs of remittances;
- lowered costs of AML/KYC compliance; and
- more robust cybersecurity.

Over the longer term, a more ambitious effort towards these ends would be to create supranational government-sponsored identity registries.

Finally, **improved economic growth** will not only result from and in quicker transactions, but also facilitate the financial support of small and medium-sized enterprises (SMEs).

Indeed, the financing of SMEs remains one of the mechanisms with the most far-reaching potential to effect change at a societal level and should be a priority for all central banks.

Chapter 8 Considerations

Several demographic, economic and geographic considerations must be taken into account in applying the Commonwealth FinTech Toolkit.

Notably, the Commonwealth member countries are diverse in terms of population size.

Small nations benefit from agility in that they are able to make decisions swiftly and hence several Commonwealth countries have already embraced fintech. While smaller developing economies have historically been limited by resource constraints, a new paradigm suggests that population size may not be a constraint to digital transformation, as evidenced by the activities of The Bahamas, Barbados, Bermuda, the Eastern Caribbean Central Bank, Mauritius, Singapore and others detailed in this report. Imagination, agility and aspiration all may allow small states to leapfrog others and become leaders in a new digital economic order.

In fact, **larger and wealthier nations** in the Commonwealth may benefit from more resources and/or larger populations across which to amortise the costs of investment in new technologies, but larger nations are typically slower to make decisions and to implement solutions. Indeed, wealthier nations are more likely to have 'legacy' systems—that is, older technology that will need to be upgraded or replaced if the nation is to take advantage of fintech.

In addition, the needs of countries that neighbour one another may be shared, while they may differ from the needs of countries in other regions.

In discussing the specific issues and opportunities in each of these, we have

grouped the member countries of the Commonwealth into **four basic regions**: **Africa**, the **Americas**, **Asia Pacific** and **Europe**.

Chapter 9 Action Framework for Creating an Enabling Environment for Fintech

Through consultation with the Commonwealth Central Bank Governors (CCBGs), academics and subject-matter experts from the private sector, the Commonwealth has devised an 'action framework' outlining:

- how to build an effective national or regional fintech task force;
- the steps that governments and that task force can take to create an enabling environment for fintech and fintech applications, from first establishing context right through to public launch; and
- the ways in which governments and other stakeholders can support one another to build on success.

Chapter 10 Case Studies

The Commonwealth FinTech Toolkit closes with four case studies of fintech interventions promoting growth and development. In doing so, it aims to highlight the sensitivity with which governments should apply fintech in their own distinct contexts.

The case studies are as follows.

- Case Study 10.1 The Journey of Emerging Technologies: Blockchain in Papua New Guinea
- Case Study 10.2 Pioneering Mobile Money in Kenya
- Case Study 10.3 Digital Assets Businesses in Bermuda

- Case Study 10.4 Malta's Support for Virtual Financial Assets

Dissemination and Future Work

There is a significant opportunity to build fintech capacity among the Commonwealth central banks. Around three-quarters of those surveyed expressed interest in training on the Commonwealth FinTech Toolkit in both digital and in-person formats, noting preference for a blended learning approach.

Some organisations expressed belief that the Toolkit could be useful not only for building the capabilities of core fintech groups within the central banks

or monetary authorities, but also for educating a wider array of colleagues in multiple government departments on the issues, risks and opportunities that fintech presents.

Endnotes

- 1 For more in-depth guidance on digital currencies, see Commonwealth Working Group on Virtual Currencies (2019). *Regulatory Guidance on Virtual Currencies*. Retrieved from https://thecommonwealth.org/sites/default/files/key_reform_pdfs/D16999_GPD_Virtual_Currncs.pdf
- 2 The Commonwealth (2018). *Commonwealth Cyber Declaration*. Retrieved from <https://thecommonwealth.org/commonwealth-cyber-declaration>

Introduction

The emergence in the past two decades of technology-enabled financial services (fintech) has wrought profound changes to the production and delivery of financial services. Global investment has soared in recent years, fuelling the rise of offerings ranging from mobile financial services to blockchain infrastructure.

At their 2018 meeting, the Commonwealth Central Bank Governors (CCBGs) endorsed the development of a Commonwealth FinTech Toolkit. The Governors noted demand for improved technical guidance regarding the implementation of fintech—an area with which many member countries are grappling. Acknowledging that some states are more advanced in this area than others, the Governors noted that it would be extremely useful for future action in this area if states were to share the lessons they had learned.

This Commonwealth FinTech Toolkit is a response to that request and was developed with feedback from central banks and other relevant government officials, as well as industry experts.

The Toolkit aims to build the capabilities of senior leaders and their teams, helping them to identify which policy interventions may make sense in a given context and then to implement that decision.

In particular, the Commonwealth is seeking to build capacity and offer technical assistance to governments aiming to foster an environment enabling fintech innovation at the same time as securing consumer protection and financial stability. Numerous governments around the world are seeking to engage with the potential of fintech to offer new choices and better prices to

consumers, new capabilities that serve both consumers and businesses alike, new ecosystems that generate high-paying, high-value jobs within developing economies, and new ways of ensuring financial stability.

At the same time, the Commonwealth recognises that with this new technology come new risks and new issues of consumer protection. With a single swipe or a few keystrokes, cyber thieves can steal huge sums, while hackers can access the irrevocable identity information (such as fingerprints) of 1 billion people. Hackers can even co-ordinate cyber attacks across dozens of countries simultaneously, increasing systemic risk globally.

This Commonwealth FinTech Toolkit therefore includes:

- a resource bank of material that covers:
 - tech topics, such as artificial intelligence (AI), blockchain and cybersecurity; and
 - anticipated outcomes, such as greater financial inclusion;
- discussion of issues impacting on small nations and large nations;
- discussion of regional concerns (spanning Africa, the Americas, Asia Pacific and Europe);
- a framework for creating environments that enable the development of fintech and fintech applications; and
- case studies of four innovative fintech initiatives.



Part 1 of the Commonwealth FinTech Toolkit introduces in brief six disruptive technologies that are transforming financial services and impacting on the lives of Commonwealth citizens.

If they are to effectively design and deploy policy and other interventions that enable the development and application of fintech, government officials must understand—at a summary level—the nature of key technologies that are categorised as fintech, and they must appreciate the potential risks and opportunities that each of these technologies offers.

In arriving at the topics included in the Toolkit, a working group of experts drawn from the Commonwealth central banks, large global banks, start-up companies and non-profits, as well as representatives of the Commonwealth Secretariat, narrowed a list of more than 24 potential areas for discussion.

The group set aside immature technologies that have not yet attained critical mass or which are not ready to be rolled out at scale in the developing world, such as quantum computing or augmented reality. It is possible that one of these technologies will

rise to the fore in the next three, five or ten years and that its impact will be such that a future version of this Toolkit might explain its relevance and a government's likely response.

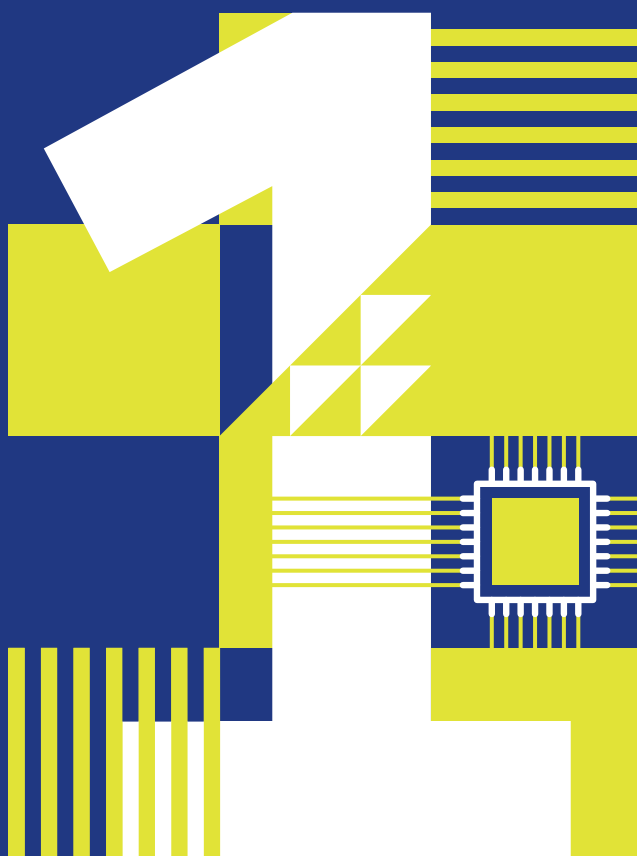
The working group also applied filters on dimensions including, but not limited to, the maturity of the technology, its relevance, its scale, and its potential impact on consumers, businesses and financial systems.

In Part 1, discussion therefore focuses on the following six key areas that the expert working group determined to be most relevant to Commonwealth member countries in the immediate term:

- digital financial services (DFS) (Chapter 1);
- artificial intelligence (AI) (Chapter 2);
- blockchain (Chapter 3);
- digital identity (Chapter 4);
- big data/big data analytics (Chapter 5); and
- cybersecurity (Chapter 6).

Chapter 1

Digital Financial Services



Digital Financial Services

Key points

- Digital financial services (DFS) can unlock productivity and investment, reduce poverty, empower women and help governments to build stronger institutions with less corruption—all while offering a profitable, sustainable business opportunity for financial services providers.
- Digital financial services can include mobile services and other kinds of digital service.
- As well as new opportunities, DFS open up new risks and involve consumer protection issues, of which regulators need to be aware and which they must address.

1.1 Introduction

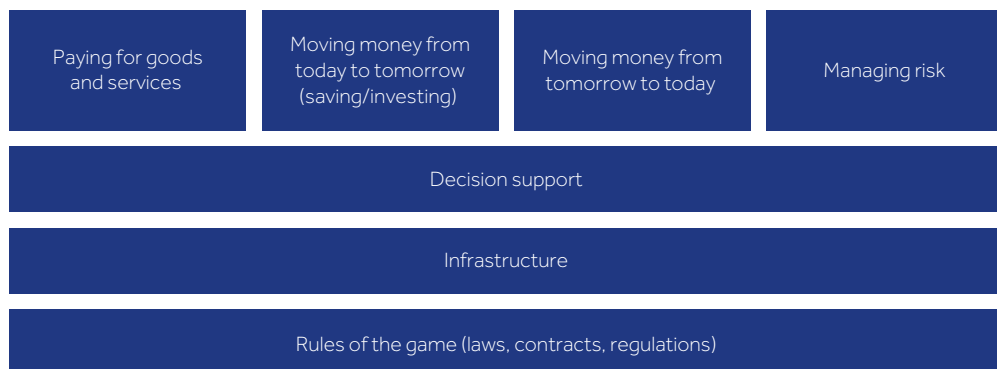
Digital financial services (DFS) are a vehicle that can help providers to overcome the barriers that leave 3.5 billion people underserved or unserved by financial services today, including by lowering the costs of compliance with international laws and regulation. While many DFS are delivered through mobile devices and hence may be referred to as 'mobile financial services', the Commonwealth prefers to use the more comprehensive 'digital financial services' to also capture

non-mobile technologies such as Paytm, which is used in India.¹

1.2 Context

Any type of financial services should be considered in the context of the financial services ecosystem. Professors Peter Tufano (Saïd Business School, University of Oxford) and Robert Merton (MIT Sloan School of Management) have developed a functional explanation of how the global financial services ecosystem works, as set out in Figure 1.1.

Figure 1.1 The global financial services ecosystem.



Source: Adapted from D B Crane *et al.* (1995). *The Global Financial System: A Functional Perspective*. Boston: Harvard Business School Press.

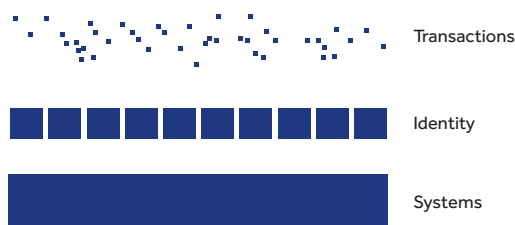
Broadening access to finance through digital means can unlock productivity and investment, reduce poverty, empower women, and help governments to build stronger institutions with less corruption—all while offering a profitable, sustainable business opportunity for financial services providers. The benefits of DFS for individuals, businesses and governments have the potential to transform the prospects of developing economies.²

Digital financial services can fill a gap left by banks that are unable or unwilling to service those at the bottom of the wealth and income scales. They are often driven by non-bank financial institutions (NBFIs) aiming to offer the financially excluded an alternative to cash as a means of payment and transfer.³

Few people and small businesses in today's developing economies fully participate in the formal financial system. They commonly transact exclusively in cash, have no safe way of saving or investing money, and cannot access credit other than through informal lenders and personal networks. Even those with bank accounts may have only limited product choice and face high fees. In more developed countries where participation is wider, the banking experience has left many feeling unhappy and many financial institutions have a customer satisfaction rating—expressed as a Net Promoter® Score (NPS)—that is negative.

Using digital channels rather than bricks-and-mortar branches dramatically reduces costs for providers and increases convenience for users, opening up access to finance for people at all income levels and even in remote rural areas. For businesses, financial services providers and governments, digital payments and DFS can erase inefficiencies and unlock significant productivity gains.

Figure 1.2 The dimensions of digital financial services.



Source: D. Shrier (2019). *Digital Financial Services*. University of Oxford, Women's World Banking and Alliance for Financial Inclusion (AFI) Leadership and Diversity Program for Regulators [Webinar].

A second simplified functional model is useful as we consider the ways in which financial services can be digitised. Figure 1.2 sets out three specific dimensions of the digital realm, disaggregating these layers from the broader context of the functional model set out in Figure 1.1.

These three foundational layers can help a central banker to understand readily where a particular DFS offering fits into the financial services 'stack'.

1.3 Description

1.3.1 The Core Elements of Digital Financial Services

We will now examine the core elements of DFS within the simplified three-layer framework.

- **Transactions** At this layer, we are looking at the movement of money from one person to another, from a person to an organisation (such as a bank, a company or a government), from an organisation to a person, or from one organisation to another.
- **Identity** An identity, in the context of DFS, is a model that uniquely represents an individual person or an organisation. Identities can comprise

government-issued documents or corporate-issued identifiers, such as Dun & Bradstreet's D-U-N-S® Number (a unique nine-digit identifier for businesses) or the Legal Entity Identifier (LEI) of legal entities participating in financial transactions, as well as biometric data, financial data and/or myriad other types of data.

- **Systems** This layer refers to the infrastructure that underpins all DFS activities and it encompasses communications networks, hardware, software and a wide range of other technologies.

At the level of **transactions**, DFS have revolutionised payments, remittances and transfers. Payment transactions are perhaps the most common financial activity of any individual and hence the entry point into financial services for millions. By lowering costs, DFS have enormous potential to broaden financial inclusion. Private companies such as M-Pesa and Bitpesa, both based in sub-Saharan Africa, are introducing lower-cost, higher-throughput transactions and reducing cross-border remittance rates from 12–15 per cent to 1 per cent or less by replacing antiquated systems that have historically demanded layers of manual labour and rent-extracting intermediaries. Bitpesa, for example, has replaced the activities of Western Union with Bitcoin technology to manage and track the movement of money from one account to another. For other market providers, mobile financial services have empowered consumers to interact with a human agent in real time—a hybrid DFS model that has helped to overcome some mistrust of digital systems by giving technology a human face. Devolving financial services even further, DFS has enabled peer-to-peer (P2P) payments systems that eliminate some of the conventional functions of the banking system and hence lower costs.

Identity is a keystone issue for financial inclusion. Some 3.5 billion people are underserved or unserved by today's financial services providers, and approximately 1 billion (largely women and children) have no legal identity at all—a barrier to access of financial services.

Identity is a keystone issue for financial inclusion. Some 3.5 billion people are underserved or unserved by today's financial services providers,⁴ and approximately 1 billion (largely women and children) have no legal identity at all⁵—a barrier to access of financial services. In addition, small and medium-sized enterprises (SMEs) may lack adequate corporate identity, and hence some 65 million formal micro businesses or SMEs are underbanked or unbanked.⁶ Access to credit for consumers and small businesses is intimately linked with identity;

a credit profile is a subset of the individual's or business's identity attributes. It is an enhanced set of data that derives from the actions of the consumer or business and it is tied to other identifiers such as an individual's National Insurance (NI) number or a company's business identifier. By feeding new forms of credit modelling driven by alternative data, digital data streams—including streams of transactions-level data—are enabling lending to a broader audience. At the same time, data portability—driven by new open banking regulations⁷—empowers consumers by giving them control over their identity-linked data (see Chapter 4 on digital identity).⁸

At a **systems** level, digital technologies are helping to modernise activities in various banking environments. New digital technologies are enabling improved security across all dimensions of infrastructure and are narrowing the gaps between nations' capabilities. In some cases, those gaps are large: some developing economies lack even basic process flow systems for loans and continue to progress loan applications in hard copy, with inevitable negative implications for cost and speed. New digital platforms support a transition that, accompanied by blockchain (see Chapter 3), is seeing the costs of interbank transfers dramatically reduced and speed increased.

Four building blocks for effective DFS regulation

Based on its work in ten countries in Africa and Asia, the Consultative Group to Assist the Poor (CGAP)—a non-profit think tank—has identified four basic building blocks for creating an enabling and safe DFS regulatory framework.

- **E-money issuance by non-banks** A basic precondition to effective DFS is the licensing of institutions other than banks as e-money issuers (EMIs).
- **Use of retail agents** Retail agents make inclusive DFS possible and are therefore a key focus of enabling regulation. Providers use agents—third parties such as shops—to provide customers with easy access to financial services close to where they live, thus expanding their reach at relatively low incremental cost.
- **Risk-based customer due diligence** Because DFS are offered within the contexts of anti-money-laundering (AML) regulations and other policy measures countering the financing of terrorism (CFT), providers must take care to implement proportionate AML/CFT frameworks. Such frameworks use a risk-based approach to protect the integrity of the system while minimising the constraints on DFS outreach.
- **Consumer protection** To drive financial inclusion, DFS providers must prove themselves reliable and cultivate trust, and this in turn depends on effective financial consumer protection (FCP).

Source: CGAP (2018). *Regulation for Inclusive Digital Finance*. Retrieved from www.cgap.org/topics/collections/regulation-inclusive-digital-finance

While most DFS at the transactions and identity layers are delivered through mobile platforms, some are not. For example, in India, the Paytm is a type of automatic teller machine (ATM) that allows a consumer who has neither a mobile phone or smartphone nor access to the internet to transfer money, make bill payments and engage in other financial services activities without visiting a bank. As such, the Paytm—a form of DFS—is a vehicle for the financial inclusion of some of the poorest individuals among Commonwealth member states.

1.3.2 The Role of Central Banks in Digital Financial Services

Government bodies in general—and central banks in particular—have a crucial role to play in the success or failure of the implementation of DFS in a country.

The local regulatory environment within which DFS are provided is said to be 'enabling' or 'non-enabling'—terms first used by the Global System for Mobile Communications (GSMA), the industry's non-profit trade association.⁹ An enabling environment is one in which non-banks can independently provide DFS without needing to partner with a licensed bank.¹⁰

In most jurisdictions, a country's central bank is its lead regulator on DFS. At a minimum, it will:

- define criteria for the licensing and authorisation of DFS providers and EMIs, as well as standards for agents;
- establish consumer protection mechanisms, including schemes safeguarding pooled funds and customer accounts;
- set out guidelines on the safety and soundness of services, and on quality

of service (QOS) and risk management; and

- develop AML and know your customer (KYC) policies for use within the financial sector.

In some cases, it may also develop and implement interoperability standards and policies, which aim to support a DFS 'ecosystem'. The central bank or regulator may build or facilitate the building of an interoperable platform at national level or otherwise take steps to integrate e-money-based financial services providers and agent networks working with e-money with more 'traditional' financial services, such as those involving ATMs and card networks.¹¹

Businesses and government leaders will need to make a concerted effort if we are to see the potential benefits of DFS realised. Three structural prerequisites will underpin any enabling environment:

- a widespread mobile and digital infrastructure;
- a dynamic business environment for financial services; and
- DFS products that meet the needs of individuals and small businesses in ways that improve on the informal financial tools they use today.

1.3.3 Examples of Digital Financial Services

Several Commonwealth nations have had significant success in deploying DFS.

The Bahamas

In May 2019, the Central Bank of The Bahamas entered into an agreement to deliver the first national digital currency by 2020. Its key collaborator was NZIA.io, alongside Singapore-based software

development firm Zynesis. Named 'Project Sand Dollar', the Bank said that it intended the initiative to be an 'integrated, affordable electronic payment system for all businesses and residents'. The Bank confirmed that the project would comply with local financial regulations and provide equal access to digital payments for the residents of the island country, reducing the costs of cash transactions and other services.¹²

India

Paytm is a digital payments platform that enables online payments, as well as cash deposits via select banks and partners, into an integrated virtual wallet. Customers can then use the Paytm wallet to pay for goods and services such as travel fares and hotel bookings, cinema visits, recharging a mobile phone and paying utility bills, as well as online shopping. The funds held in the wallet are protected under escrow—a type of account from which funds are released only once an agreement is fulfilled.¹³

Kenya

M-Pesa and similar DFS are indicative of a mobile banking revolution in Kenya: financial institutions have embraced M-Pesa as a platform on which to manage micro accounts, to build customer deposits and to broaden their customer networks. Kenya has therefore emerged as a leader in financial inclusion in sub-Saharan Africa. In 2006, just before the launch of M-Pesa, only 26.7 per cent of Kenyans had access to formal financial services (such as bank accounts and money transfers); this figure now exceeds 80 per cent (see Case Study 10.2).¹⁴

Malawi

Since launching its first mobile money pilot in 2012, Malawi has seen the number of people using DFS as of June 2018 leapfrog from 1,000 active users to 2.3 million (measured in a period of 90 days)—a figure that represents

25 per cent of the adult population. The 2017 Global Findex released by the World Bank in April 2018 highlights this remarkable achievement.

The Reserve Bank of Malawi played an important role in creating an enabling regulatory environment that fostered innovation and growth led by the private sector. The Bank permits both banks and NBFIs to offer DFS. Parliament passed critical laws in 2016, including the Payment Systems Act, E-Transactions Act and Communications Act, which have guided further development of the DFS market. In September 2017, the Bank issued a directive mandating DFS interoperability and hence Malawi has now delivered a reality for multinational organisations of which many countries can still only dream.¹⁵

Nigeria

According to the World Bank's World Development Report 2016, Nigeria's 2012 Growth Enhancement Support Scheme introduced mobile technology to transfer fertiliser subsidies directly to farmers, taking the government out of the business of procuring and distributing fertiliser. The Scheme now helps up to twice as many farmers at a sixth the cost of the government's former mechanisms. The transfer system relies on a database of more than 10.5 million farmers, who, as registered recipients of the subsidies, now have a better chance of accessing formal or regulated financial services. Based on this initial success, the system is expanding, with the help of a digital identity system and biometric signatures, to extend the reach of financial services into Nigeria's more remote rural areas.¹⁶

United Kingdom

At digital bank Monzo, chief executive officer Tom Blomfield and his team are harnessing

technology to authenticate and provide basic bank accounts for people who have been granted asylum in the UK. Blomfield has suggested that better digital identification in the UK could help to reduce the cost of providing financial services to disadvantaged groups.

At OakNorth Bank, co-founder Rishi Khosla is using machine learning to apply lending techniques formerly limited to large business to underserved SMEs. By drawing on shared public data (with permission), such as tax returns, OakNorth is helping to unlock savings for small businesses.¹⁷

Zambia

The Zambia National Commercial Bank (Zanaco) has invested in a distinctive brand for financial inclusion. In 2008, the Bank successfully launched Zambia's first mobile banking service, Xapit. Opening a Xapit account takes only minutes, and it allows consumers to access credit and other banking services over a mobile phone. Targeting Zambia's underbanked markets, Xapit now serves more than 200,000 customers and conducts more than 1 million transactions per month. Xapit users include other Zanaco customers that have easy access to the product through their savings and current accounts.¹⁸

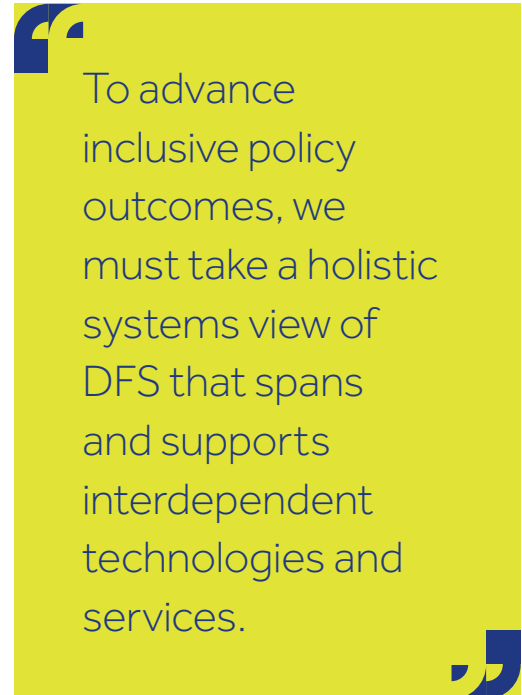
1.4 Key Considerations for Future Development

1.4.1 Critical Issues in and Obstacles to Digital Financial Services

Several critical issues have arisen in the past several years as DFS have been adopted more widely.

Digital Inclusion

Digital inclusion drives financial inclusion, but digital exclusion remains so significant a problem globally that one of the United Nations Sustainable Development Goals (SDG 9)



includes access to information and communications technology (ICT) among its targets.¹⁹ Even though every 10 per cent increase in internet penetration sees gross domestic product (GDP) increase by 1.35 per cent,²⁰ the world seems stuck at around 54.8 per cent connectivity, with a slowing growth rate (2.9 per cent in 2019²¹) inhibiting the potential for financial inclusion. Some 3.8 billion people still lack access to fast and/or reliable internet, making it difficult to deliver financial services digitally.²² And the issue is gendered, with the GSMA finding that 313 million fewer women than men are using mobile internet in low- and middle-income countries.²³

To advance inclusive policy outcomes, we must take a holistic systems view of DFS that spans and supports interdependent technologies and services. For example, Africa should be home to more than 700 million smartphones by 2025—up from 302 million in 2018²⁴—but if access to power and access to bandwidth remain limiting factors, DFS efforts will fail.

Rising Usury

Despite these lofty goals, DFS platforms have come under criticism as imposing a 'poor tax' in the form of the high interest rates charged to people with low incomes in comparison with those granted to the wealthy and financially secure. In an era of historically low (in some cases, negative) interest rates in developed nations, why is it that developing economies and underbanked/unbanked populations remain able to access only high-cost loans? Yet, in some countries, policy initiatives aiming to cap interest rates have had unintended consequences, limiting the capacity of companies to compete and leading several players to abandon those markets as unsustainable economically.

Economists argue over solutions. A 2018 study of developing nations found that, of the 69 studied, 51 had imposed interest rate caps.²⁵ The rationale offered is typically to protect consumers from usury, to improve access to credit and to reduce costs to consumers. Leora Klapper of the World Bank points out the unintended adverse consequences of interest rate caps and instead advocates for policy tools such as fostering competition, reducing the cost of funds to lenders and so on, echoing sentiments dating back to Milton Friedman.²⁶

Know Your Customer (KYC)

One challenge that links with identity relates to KYC regulations. The rules currently require that a customer be tied to a physical address—but even those who have no fixed address may need to access financial services.

In a positive step towards financial inclusion, new technologies delivered by mobile phone can partner Global Positioning System (GPS) co-ordinates with device-acquired biometrics to provide high-resolution means

of identifying an individual that actively improve on current methods and which are more secure. Governments are exploring these and alternative methods of identifying individuals digitally.

Privacy

Importantly, the ability to access alternative data opens up new issues of digital privacy, with personal data stripping citizens of anonymity. Telecommunications and bank datasets may even be misused, breaching personal privacy or targeting groups negatively on the basis of protected characteristics, such as race, gender or religion. In recent years, we have heard much about the part that analysis of this type of data has played in manipulating voters during elections, and while supranational data protection legislation such as the European Union's General Data Protection Regulation (GDPR) aims to secure personal data and model best practices for its use, domestic regulators may struggle to apply it.²⁷

Cybersecurity

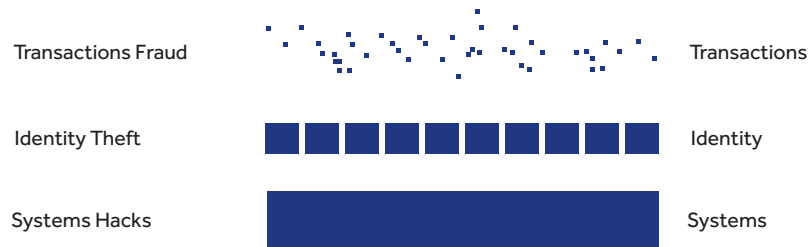
In Figure 1.3, we look at the simplified three-layer model of the DFS realm that we set out in Figure 1.2 through a cybersecurity lens.

At each layer of the DFS stack, new vulnerabilities arise.

- At the level of transactions, we see the risk of **transaction fraud**.
- The identity layer is exposed to the risk of **identity theft**.
- Interoperable and easily accessed digital systems can be subjected to **systems hacks**.

The downstream impacts should cybersecurity risks manifest can be serious.

Figure 1.3 The cybersecurity risks of digital financial services.



Source: D Shrier (2019). *Digital Financial Services*. University of Oxford, Women's World Banking and Alliance for Financial Inclusion (AFI) Leadership and Diversity Program for Regulators [Webinar].

At a personal level, rising fraud and identity theft rates can reverse rising financial inclusion. For example, false decline rates are highest in emerging markets such as Bangladesh, sub-Saharan Africa, Colombia and Mexico: 50 per cent or more of transactions are declined simply because fraud systems are unable to determine whether the transaction originates with a legitimate customer or a hacker. At a systemic level, hackers undermine confidence in the banking system. (See Chapter 6 on cybersecurity for more detail.)

Financial Literacy

Limited levels of financial literacy may limit the adoption of DFS. In interviews, central banks revealed that consumers in their countries commonly questioned new offerings. Some of those currently underserved or unserved simply do not understand the benefit of a savings account or a credit facility—and the necessary remedy is investment in financial literacy.

1.4.2 Future Opportunities for Digital Financial Services

Digital financial services have the potential to be a powerful tool for inclusion and improved economic velocity. A systems view of DFS should include efforts to:

- improve financial literacy;

- invest in modern technology infrastructure;
- shape policy interventions that engage and empower the private sector; and
- protect consumers in light of the sophisticated effects of different DFS offerings.

The rise of non-traditional providers of services such as money transfers, savings and lending is a characteristic of DFS that gives rise to some concerns.²⁸

One concern is that traditional financial regulation does not always cover these companies or holds them to a different (reduced) standard, even though they can scale up quickly. To some extent, these problems mimic the 'shadow banking problem' that preceded the global financial crisis and hence regulators are exploring a shift from regulating entities to regulating activities.

Another concern is that digital finance is drawing large numbers of people into the financial system for the first time. This has consequences should they not be financially literate, and hence DFS efforts must be partnered by consumer education

and consumer protection, including the promotion of fraud prevention, dispute resolution mechanisms and data privacy.

A third concern is that financial innovation could pose a systemic risk to a country's banking sector, involving any and all of credit, liquidity, operational and consumer risk. Prudential regulation of DFS reduces these risks, but it may involve high compliance costs that are barriers to entry and thus to competition. For example, concerns were raised about the risks that Bitcoin posed to the banking system, but the Bank of England's analysis suggested that most digital currencies play too small a role (at present) to threaten financial stability.²⁹ A greater concern may be that financial innovations create distortions in financial markets that could have larger implications. For example, if automation and 'big data' approaches were to make it easier to issue consumer credit but not commercial credit, then financial institutions might over-allocate to the former, potentially creating a credit bubble and reducing the credit available to investments that increase productivity.

Moreover, while the Bank of England may have dismissed the systemic risks posed by Bitcoin, it was more concerned by the advent of multinational digital currency Libra, proposed by a private consortium of companies led by Facebook, and by the digital yuan, or e-RMB, issued by the People's Bank of China. In August 2019, outgoing Bank of England Governor Mark Carney called for a digital currency backed by several countries that would address rising concerns around these two digital currencies and the hegemony of the US dollar.³⁰

Finally, the spread of DFS gives rise to concerns about increased fraud in the financial system. As financial institutions have digitised, they and other sectors

processing electronic financial transactions have been exposed to cyber attacks.

The theft of credit card information from retailers at scale has highlighted the stakes and banks have been at the forefront of efforts to develop secure transaction processes. Larger financial institutions have the resources and knowhow to upgrade online and mobile security continuously, with tools such as encryption or strong authentication, but smaller banks and NBFIs may be more at risk.

Perhaps the most significant concern to be overcome is that systemic risk—the risk of a loss of trust in digital financial systems—may hinder further innovation in the sector.

Endnotes

- 1 Sharma R (2016). 'What Is Paytm, and How to Use Paytm Wallet?' *Gadgets360*, 13 December [online]. Retrieved from: <https://gadgets.ndtv.com/apps/features/what-is-paytm-and-how-to-use-paytm-wallet-1625271>
- 2 McKinsey & Co. (2016). *Digital Finance for All: Powering Inclusive Growth in Emerging Economies* [online]. Retrieved from: www.mckinsey.com/-/media/McKinsey/Featured%20Insights/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx
- 3 Perlman L, Wechsler M (2019). 'Mobile Coverage and Its Impact on Digital Financial Services'. *SSRN Electronic Journal* [online]. Retrieved from: <https://dfsobservatory.com/sites/default/files/Mobile%20Coverage%20and%20its%20Impact%20on%20Digital%20Financial%20Services%20-%20PUBLIC.pdf>
- 4 Aggarwal R et al. (2017). *Blockchain and Financial Inclusion: The Role Blockchain Technology Can Play in Accelerating Financial Inclusion* [online]. Retrieved from: <https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf>

- 5 World Bank (2018). *Global ID4D Dataset* [online]. Retrieved from: <https://id4d.worldbank.org/global-dataset>
- 6 International Finance Corporation (2017). *MSME Finance Gap: Assessment of the Shortfalls and Opportunities in Financing Micro, Small and Medium Enterprises in Emerging Markets* [online]. Retrieved from: www.ifc.org/wps/wcm/connect/03522e90-a13d-4a02-87cd-9ee9a297b311/121264-WP-PUBLIC-MSMEReportFINAL.pdf?MOD=AJPERES&CVID=m5SwAQA
- 7 Zachariadis M, Ozcan P (2017). 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking'. SWIFT Institute Working Paper No. 2016-001 [online]. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199
- 8 Chakravorti B (2020). 'Why It's So Hard for Users to Control Their Data'. *Harvard Business Review*, 30 January [online]. Retrieved from: <https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data>. See also Hardjono T, Shrier D L, Pentland A (2019). *Trusted Data: A New Framework for Identity and Data Sharing*. MIT Press.
- 9 For the GSMA view, see di Castri, S (2013). *Mobile Money: Enabling Regulatory Solutions* [online]. Retrieved from: www.gsma.com/publicpolicy/wp-content/uploads/2013/02/GSMA2013_Report_Mobile-Money-EnablingRegulatorySolutions.pdf
- 10 Perlman, L (2015). *An Introduction to Digital Financial Services* [online]. Retrieved from: www.academia.edu/39099268/An_Introduction_To_Digital_Financial_Services
- 11 *Ibid.*
- 12 Partz, H (2019). 'Bahamas Central Bank Enters Agreement to Deliver First National Digital Currency by 2020'. *Cointelegraph*, 29 May [online]. Retrieved from: <https://cointelegraph.com/news/bahamas-central-bank-enters-agreement-to-deliver-first-national-digital-currency-by-2020>
- 13 Sharma R (2016). 'What Is Paytm, and How to Use Paytm Wallet?' *Gadgets360*, 13 December [online]. Retrieved from: <https://gadgets.ndtv.com/apps/features/what-is-paytm-and-how-to-use-paytm-wallet-1625271>
- 14 Ndung'u N (2017). 'M-Pesa: A Success Story of Digital Financial Inclusion' [online]. Retrieved from: www.geg.ox.ac.uk/sites/geg.bsg.ox.ac.uk/files/M-Pesa%20-%20a%20success%20story%20of%20digital%20financial%20inclusion%20-%20Njuguna%20Ndung%E2%80%99u.pdf
- 15 United Nations (2018). 'Exciting Changes in Malawi DFS Market'. *UNCDF Blog*, 28 December [online]. Retrieved from: www.uncdf.org/article/4270/exciting-changes-in-malawi-dfs-market
- 16 World Bank (2016) *World Development Report 2016: Digital Dividends* [online]. Retrieved from: www.worldbank.org/en/publication/wdr2016
- 17 Van Steenis H (2019). *Future of Finance: Review on the Outlook for the UK Financial System—What It Means for the Bank of England* [online]. Retrieved from: www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report
- 18 Accenture, CARE International (2015). *Within Reach: How Banks in Emerging Economies Can Grow Profitably by Being More Inclusive* [online]. Retrieved from: www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_23/accenture-banking-withinreach.pdf#zoom=50
- 19 United Nations (2015). *Sustainable Development Goal 9* [online]. Retrieved from: <https://sustainabledevelopment.un.org/sdg9>
- 20 Minges M (2016). 'Exploring the Relationship between Broadband and Economic Growth'. *World Development Report 2016 Digital Dividends Background Paper* [online]. Retrieved from: <http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf>
- 21 ITU (2019). 'Global Internet Growth Stalls and Focus Shifts to "Meaningful Universal Connectivity" to Drive Global Development'. Press release, 22 September [online]. Retrieved from: www.itu.int/en/mediacentre/Pages/2019-PR16.aspx

- 22 United Nations (2017). *The State of Broadband: Broadband Catalyzing Sustainable Development* [online]. Retrieved from: www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf
- 23 GSMA Connected Women (2019). *The Mobile Gender Gap Report 2019* [online]. Retrieved from: www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/GSMA-The-Mobile-Gender-Gap-Report-2019.pdf
- 24 GSMA Intelligence (2019). *The Mobile Economy: Sub-Saharan Africa 2019* [online]. Retrieved from: www.gsmainelligence.com/research/?file=36b5ca079193fa82332d09063d3595b5&download
- 25 Ferrari A, Oliver M, Ren J (2018). *Interest Rate Caps: The Theory and the Practice*. World Bank Policy Research Working Paper 8398 [online]. Retrieved from: <http://documents.worldbank.org/curated/en/244551522770775674/pdf/WPS8398.pdf>
- 26 See, e.g., Friedman M (1980). *Free to Choose: A Personal Statement*. New York: Harcourt.
- 27 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, 4 May 2016, OJ L 119/1.
- 28 World Bank (2016). 'Enabling Digital Development: Digital Finance'. In *World Development Report 2016* [online]. Retrieved from: http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263021313/additional/102725-PUB-Replacement-PUBLIC.pdf
- 29 Canadian Press (2018). 'Bank of England's Mark Carney Says Cryptocurrencies Aren't Financial State Risk, But Likely to Be Regulated'. *The Star*, 12 April [online]. Retrieved from: www.thestar.com/business/2018/04/12/bank-of-englands-mark-carney-says-cryptocurrencies-arent-financial-state-risk-but-likely-to-be-regulated.html
- 30 Inman P (2019). 'Mark Carney: Dollar Is Too Dominant and Could Be Replaced by Digital Currency'. *The Guardian*, 23 August [online]. Retrieved from: www.theguardian.com/business/2019/aug/23/mark-carney-dollar-dominant-replaced-digital-currency

Chapter 2

Artificial Intelligence



Artificial Intelligence

Key points

- Artificial intelligence (AI) is the technology that helps a machine to think like a person.
- Artificial intelligence is already being deployed within banks, to interface with consumers and businesses, and within government itself.
- Machine learning—a particular type of AI—has offered new opportunities in financial services and shaped new offerings.
- Inevitably, however, with new opportunity comes new risks, and regulators need to address these proactively.

2.1 Introduction

Commercially scalable artificial intelligence (AI) has become widespread over the past decade. The financial services sector adopted it quickly, and it has since created both opportunities and risks that central banks need to consider. There are several implications for the use of AI within a central bank and for the adoption of AI by financial services institutions and in other industries.

2.2 Context

Artificial intelligence is a term we use to describe machines that can think in highly sophisticated ways—ways that aim to imitate (or surpass) human cognition. Some notable examples of AI are Google's DeepMind, IBM's Watson, Amazon's Echo and Apple's Siri.

While AI is the superset, subsets of AI that we might hear discussed in relation to financial services include applied AI (AAI), generalised AI (GAI), deep learning and machine learning. We will look closely at the last of these in the next section.

From a regulatory standpoint, it is helpful to think of major deployments of AI within:

- a supervised bank or non-bank financial institution (NBFI);
- the market (whether consumer- or business-facing); and
- government, including the central bank.

We will look at these in brief, before considering the future of AI in digital financial services (DFS).

2.3 Description

2.3.1 Artificial Intelligence, Machine Learning and Deep Learning

Machine learning is a subset of AI that involves supplying machines with enough data that they can learn what it means or learn to interpret it. This contrasts with traditional computer programming, which involves giving a computer a discrete set of instructions that it simply follows (a 'rules-based system'). The terms 'AI' and 'machine learning' can be confusing because they are

often (incorrectly) used interchangeably. When banks or entrepreneurs, for example, talk about AI, they are usually talking about machine learning.

One example of machine learning is the natural language processing that powers applications such as Apple's Siri, Amazon's Echo, Google Home or Tesla's Autopilot. By integrating vast quantities of data about what people say and how they say it, the devices are able to interpret meaning and, for example, order a pizza when we say the words 'Order me a pizza'.

By contrast, an example of a rules-based system is the system underpinning self-driving vehicles.

Machine learning is something that we already encounter in a number of applications today. Generalised AI, meanwhile, is still several years away, although great strides have been made. DeepMind, for example, grew out of a research effort at University College London's Computational Neuroscience Unit. The Unit's goal was to 'solve intelligence' and the

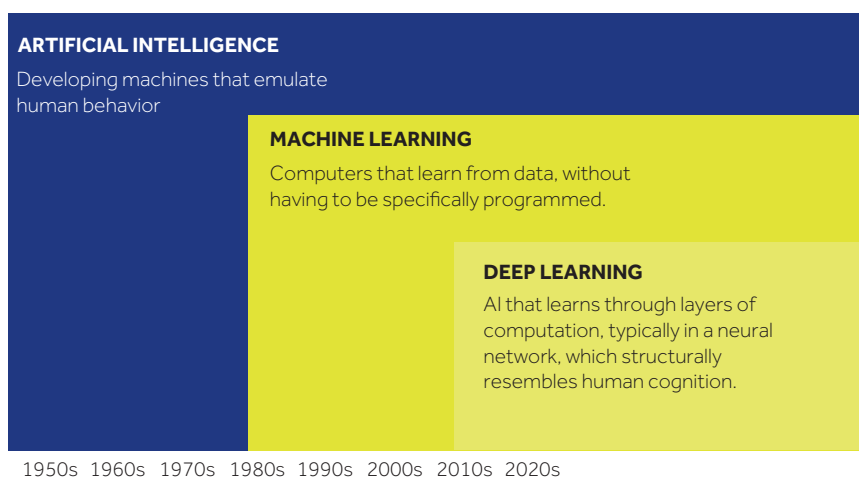
team approached its research by combining machine learning with systems neuroscience (a discipline that involves understanding how neurons form networks). Unlike many other 'guided' AI systems, DeepMind is said to learn only from experience and not to follow predefined paths, relying instead on general-purpose learning algorithms. DeepMind and other efforts such as Watson are starting to find their way towards broader applications.

Figure 2.1 explains the relationships and differences between deep learning, machine learning and AI, and the evolution over time of these different systems.

As Figure 2.1 explains:

- AI is the broadest possible category, encompassing all efforts to make a machine imitate human thinking;
- machine learning is a subset, focused on computers that can learn to imitate human thinking without being programmed specifically to do so

Figure 2.1 The relationship between AI, machine learning and deep learning.



Source: D Shrier (2021). 'The Convergence Revolution'. In D Shrier and A Pentland (eds). *Global Fintech*. Cambridge, MA, and London: MIT Press. Reproduced with permission of the author.

(rather like how a human child learns language); and

- deep learning is a special kind of machine learning that can address more sophisticated types of problem and its work is much more accurate if it has access to sufficiently large quantities of data.¹

2.3.2 How is AI (Primarily Machine Learning) Being Applied in Financial Services?

We can examine the main applications of AI in financial services and how those applications relate to the concerns of regulators by considering them in relation to the areas in which they are deployed.

Within a Supervised Bank or NBFIs

Artificial intelligence—particularly machine learning—is streamlining financial services infrastructures. Banks and NBFIs can use it to assess risk, to monitor transaction flow, to implement cybersecurity and even to make critical decisions rapidly. Inevitably, however, each of these new applications involves potential new risks. Since, historically, many AI systems have operated as ‘black boxes’ within which where and how they make decisions is obscure to the average human being, it can be difficult to audit those decisions and attest to their compliance.

Some financial institutions have begun to use algorithmic models to make core lending decisions such as credit underwriting. If applied with care, this type of model creates an opportunity for the 3.5 billion people who are underbanked or unbanked because machine learning can help to break the ‘credit trap’—that is, the fact that an individual or business has to demonstrate a credit history to get credit in the first place. New models based on human behaviour and alternative datasets are now making it possible for a bank to

extend credit responsibly to first-time borrowers.

If not properly trained or supervised, however, machine learning systems can end up configured such that they further exclude already-marginalised groups on the basis of characteristics such as race or low incomes, so deepening the divide that they have the potential to bridge. To militate against this risk, regulators may require banks to submit to an annual algorithm audit, certified by a third-party firm, which should examine particular areas of compliance and risk.

Within the Market (Consumer- or Business-facing)

Artificial intelligence systems offer numerous opportunities for inclusive consumer and business financial services. For example, in Bangladesh, an effort is under way to implement voice-enabled technologies, opening up access to financial services to that portion of the population whose literacy is poor. Teaching the machine learning system to recognise numerous local dialects and accents therefore means training it in a local context. A speech recognition engine trained only in received British English pronunciation, for example, would fail to meet local needs.

Large tech companies may lay digital identification and biometrics over AI pattern recognition systems, and this can create issues in implementation. For example, Google initially trained its facial recognition algorithms—an expression of machine learning—largely on pictures of people of European descent. When confronted with a photo of a person of colour, the systems produced errors that did reputational damage to the company—and unfortunately the steps it took to remedy the issue were likewise controversial.

When deciding on policy that will guide AI applications in DFS, it is therefore essential that regulators understand both the principles and the implementation of such systems.

Within Government, Including the Central Bank

The technology that financial services regulators use to manage processes such as monitoring compliance is known as regtech. Regtech has been lagging behind the fintech industry in several ways, but efforts are now being made to address this. Artificial intelligence systems could help government regulators and policy-makers to collect revenue, to monitor the financial system, to highlight or predict risk events, and in other ways to more readily accomplish their mission.

One area in which governments have been successful is in using large-scale datasets (including financial data) to develop and implement government policy through efforts such as Data for Development and, more recently, the Global Partnership for Sustainable Development Data (GPSDD). These initiatives saw government ministries assemble and sandbox large-scale datasets. They then invited hundreds of academic research groups from around the world to develop insights into issues ranging from inclusion to public health based on these datasets.

2.4 Key Considerations for the Future

It is increasingly important to align the use of AI with the values and cultural norms of any given country. Certain intrinsic bias is built into any such systems, so it is important to understand what this bias is and how it intersects with legislative and regulatory priorities. For example, all credit underwriting contains known bias that the regulator has deemed acceptable.



Artificial intelligence systems could help government regulators and policy-makers to collect revenue, to monitor the financial system, to highlight or predict risk events, and ... to more readily accomplish their mission.

Similarly, newer AI systems (whether for credit or for other applications) will require a regulator to understand how the algorithm arrives at its decisions if that regulator is to ensure that the application complies with relevant law and regulation. In fact, this form of 'explainable AI' is a growing subset of the broader AI commercial world.

Central banks and regulators will want to increase the sophistication with which they approach AI. They should appoint working groups to ensure that they stay up to date with developments in the field, and they should ideally train and employ in-house experts who know how to evaluate

and monitor AI systems. There are also opportunities for governments to support economic development and to stimulate or focus industry activity in particular areas to encourage private industry to apply AI towards desired policy outcomes.

Endnote

1 Mahapatra S (2018). 'Why Deep Learning over Traditional Machine Learning?'. *Towards Data Science*, 21 March [online]. Retrieved from: <https://towardsdatascience.com/why-deep-learning-is-needed-over-traditional-machine-learning-1b6a99177063>

Chapter 3

Blockchain and Financial Services



Blockchain and Financial Services

Key points

- Blockchain is a type of peer-to-peer (P2P) database that uses data 'blocks', all of which update one another automatically as they grow, to build an immutable (permanent) record.
- It is both more secure than other forms of database (because it is harder to insert bad data) and more user-friendly (because it makes it easier to access that data).
- As a distributed ledger technology (DLT), blockchain allows parties who do not necessarily trust each other to co-operate towards shared outcomes, which is useful in a number of financial services applications.
- Central banks have both proposed and trialled a range of blockchain experiments, ranging from land registry to introducing their own central bank digital currencies (CBDCs).¹

3.1 Introduction

Disruption is rife in the financial services sector. Nimble market entrants and rapidly penetrating technologies are challenging consumer expectations of financial services delivery. As they gradually adopt blockchain technology, large financial institutions will experience dramatic efficiency gains—and equally dramatic cost reductions and reduced risk.

Banks and central banks are the dominant players in exploring the potential of blockchain to drive major institutional change in the financial services sector. Blockchain can eliminate redundant systems, automate processes, introduce new modes of contracting and open business models, drive radical institutional cost reductions and capital market restructuring, reduce risk, and ensure stable economic performance and compliance with international regulation. Recognising the value of these opportunities in relation to digital currencies, the Commonwealth Secretariat published its *Regulatory Guidance*

on *Virtual Currencies* in 2019, paying specific attention to issues of enforcement relating to criminal activity, taxation, financial products, consumer protection and financial inclusion.²

In this chapter, we will use real-world examples to describe how the core features of blockchain technology—such as security, transparency, auditability and immutability on a peer-to-peer (P2P) network—are driving its adoption in the financial services sector and are likely to change the ways in which we manage the recording, storage and transfer of digital assets.

We will look at how blockchain technology is maturing alongside complementary technologies, such as artificial intelligence (AI) (see Chapter 2), the Internet of Things³ and big data/big data analytics (see Chapter 5), to reach beyond financial processes alone.

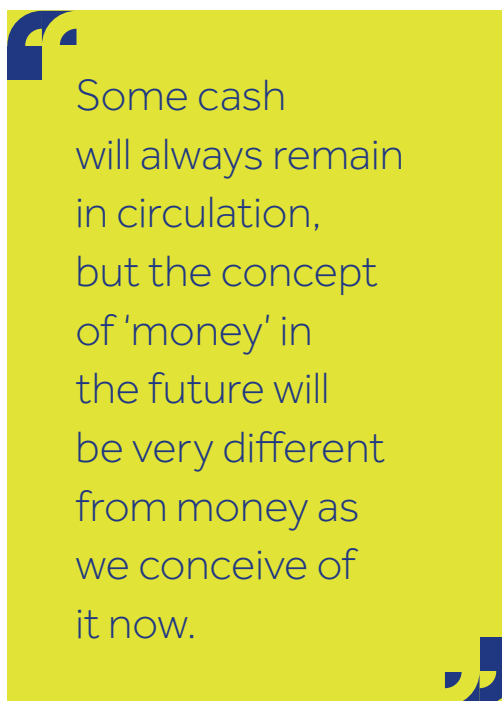
In the short-to-medium term, we can expect to see blockchain applied to influence domestic and international monetary policy and to introduce new payment channels,

shifting financial services away from the dominant central bank model and helping to restructure debt burdens. With blockchain technologies providing secure data transfer and surveillance, the integration of complementary technology will provide new modes of identification, data structures and management protocols, boosting investor and market confidence and reducing risk. Data that are more reliable will lead to more sustainable lending decisions and—with enforcement automated—improved debt recovery, reducing debt-related costs and burdens.

In the medium-to-long term, we can expect blockchain to facilitate a hyper-personalised digital payments ecosystem, comprising programmable money—a vast suite of digital currencies—underpinned by central bank digital currencies (CBDCs). While we might anticipate that some cash will always remain in circulation, the concept of 'money' in the future will be very different from money as we conceive of it now.

Since 2016, more than 200 banks and 40 central banks worldwide have experimented with blockchain. Also known as distributed ledger technology (DLT), cases in point include applications targeting:

- financial inclusion;
- payments efficiency;
- payment system operations;
- cyber resilience;
- trade finance;
- the provision of Single Euro Payments Area (SEPA) credit identifiers (SCIs);
- bond issue and management;
- interbank securities settlement;



Some cash
will always remain
in circulation,
but the concept
of 'money' in
the future will
be very different
from money as
we conceive of
it now.

- know your customer (KYC) and anti-money-laundering (AML) processes;
- wholesale and retail CBDCs; and
- improved data management and information sharing.

The primary motivation behind efforts to develop and deploy DLT is its potential to reduce or even eliminate the operational and financial inefficiencies—or to smooth the other frictions—that result from current methods of storing, recording and transferring digital assets throughout financial markets.

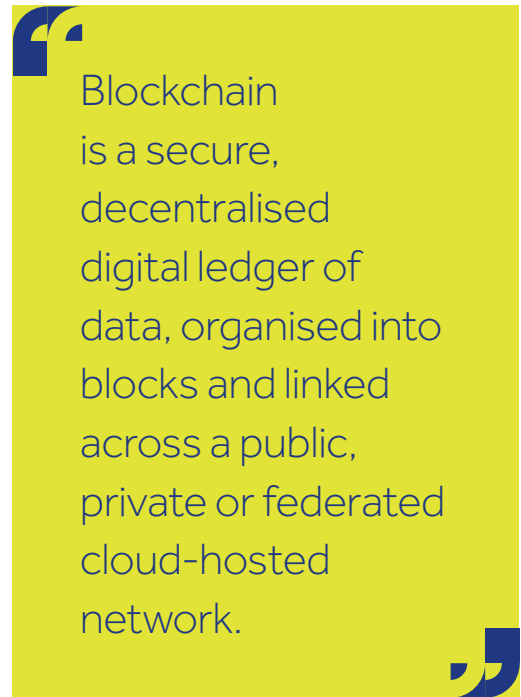
Banks with experience of blockchain cite benefits such as:

- wide-ranging oversight of trade transactions, from trade to settlement;
- reduced risks of discrepancy and delayed settlement;

- real-time access to a shared ledger among multiple stakeholders;
- automation of traditionally manual processes;
- reduced reliance on external settlement networks;
- efficiency gains in capital velocity; and
- reduced counterparty, market and credit risks.

Blockchain is a secure, decentralised digital ledger of data, organised into blocks and linked across a public, private or federated cloud-hosted network. A public blockchain (such as Bitcoin or Ethereum) may have millions of nodes authorising transactions on the network; a private or federated network may have as few as three nodes on the network. The number of nodes on the network affects the transaction speed. Public blockchains may consequently be criticised for slow throughput, because potentially millions of computers on the network must be co-ordinated. Instances of institutional application therefore increasingly centre on private and federated networks. Popular blockchains in the financial services sector include Hyperledger, AWS, IBM, Multichain, R3's Corda, the Linux Foundation's Hyperledger Fabric, J P Morgan's Quorum or private configurations of the Ethereum blockchain.

Blockchain's proponents posit that DLT could help to foster a more efficient and safer payments system, affect the way in which payment, clearing and settlement (PCS) activities are conducted, and change the roles that financial institutions and infrastructures play in the financial services market—or even fundamentally change that market's structure. While



Blockchain
is a secure,
decentralised
digital ledger of
data, organised into
blocks and linked
across a public,
private or federated
cloud-hosted
network.

others believe that effective real-world applications of blockchain technologies are still years away, the financial services sector has already witnessed several significant early-stage developments. Indeed, while traditionally cautious, banking institutions have been early adopters of blockchain technologies, incentivised by potential operational cost savings, competitive market positioning (particularly among emergent and disruptive fintech start-ups), and the potential for efficiency gains in capital markets.

3.2 Context

The transfer, trade and settlement of payments, securities, commodities or derivatives involves time-consuming steps that are facilitated and overseen by financial intermediaries—also known as financial market infrastructures (FMIs)—such as payment systems, securities settlement systems (SSSs),

central securities depositories (CSDs) and central counterparties (CCPs). These intermediaries provide services, manage financial, operational and legal risks, and are responsible for good governance structures for themselves, their customers and the markets they serve. End users, such as households and businesses, typically trust intermediaries such as banks and broker-dealers to store and maintain records of the users' assets and then to transfer those assets on the users' behalf. When a user initiates a transaction, their bank or broker-dealer will interact with one of these FMIs.

As transaction volumes have risen and market participants have become more complex, frictions have emerged and increased both the costs and the risks of transacting in financial markets. Such frictions, including operational and financial inefficiencies, have prompted market participants to seek solutions in areas such as payments, the transfer of money, cross-border trade and the trading of securities. Thus far, these solutions have comprised either developing technology or changing market structures, or a combination of both. The availability and maturity of technology are key factors in determining which of the two will best address a particular friction or inefficiency.

To date, blockchain—a nascent technology—has been piloted in cross-border transactions. Research by the World Economic Forum also indicates proof of concept for forthcoming deployments in financial services contexts, including:

- establishing syndicated loan joint ventures to reduce transaction times;
- providing utility settlement coins to make clearing and settlement efficient;

- settling high-value securities transactions in minutes by reducing paper-based processes;
- reducing bond issuance and settlement from days to minutes;
- mutualising KYC servicing to reduce compliance costs;
- efficiency gains in cross-border transactions and verification;
- simplifying and improving foreign-exchange balance-sheet reconciliation;
- creating back-office business management efficiencies by using smart contracts (i.e., self-executing computer programs with defined business logics) to automate processes; and
- providing secure interbank letters of credit efficiently using smart contracts, addressing issues of data forgery.⁴

In any case, introducing new technology in financial services often requires the restructuring of markets (consider, for example, the radical difference the internet has made to previously paper-based processes such as stock issue). The functionality of blockchain is therefore likely to reshape the architecture of financial markets by facilitating disintermediation and eliminating redundant processes.

3.3 Description

We can organise the applications of blockchain into three broad categories:

- the storage of digital records (identities, assets or voting rights);
- the exchange of digital assets (via direct P2P transactions that eliminate intermediaries); and

- the recording and execution of smart contracts.

The structure and functionality of the blockchain network offers multiple opportunities for cost savings in the financial services sector. The P2P network disintermediates numerous parties responsible for processing and approving the registration and transfer of assets, and the use of smart contracts automates these processes.

Smart contracts are lines of code that execute automatically when certain conditions are met, which can eliminate time-consuming and costly manual processes, for example, by paying on a derivative when a financial instrument meets a certain benchmark or resetting the interest rate on a debt when it reaches a certain balance. Smart contracts are already digital, yet Oracle's external data warehouses could automate them further, even more transparently, for example, by automatically calculating an interest rate reset on a floating-rate mortgage. Accordingly, blockchain would reduce the associated costs of human resources and third-party professional support. It would reduce the need for financial analysts and lawyers, because blockchain-enabled smart contracts can assess delinquency rates, compile monthly repayment reports and trigger enforcement action where required automatically. Indeed, in a 2017 report, Accenture found that repointed operational, risk and finance systems represent long-term return on investment in blockchain: investment banks report up to 70 per cent savings on central finance reporting and 50 per cent in business operations such as trade support, middle office, clearance, settlement and investigations.⁵

In addition to these radical cost reductions for financial services firms, blockchain

promotes reduced counterparty and market risk, and it supports efficient capital markets. If a shared, transparent ledger is populated automatically with real-time financial data, investors can be assured of a prospect's creditworthiness and overall organisational financial performance, enabling a swift response to collateral performance and economic stability. Smart contracts and permissioned ledgers can thus provide investors and creditors with unprecedented confidence in data reporting and accuracy by enabling more accurate forecasting, improved risk management and sustainable financing, the impact of which contributes to efficient securitisations and ratings.

Automated collection and reconciliation of information, the reduced potential for human error and secure network integrity can all increase stakeholder faith in blockchain technology. In financial services, we see this trust emerging as the technology matures from nothing more than a way of managing financial processes to become a way of resolving economic policy concerns. In May 2019, the Monetary Authority of Singapore—Singapore's central bank—and the Bank of Canada piloted a currency swap: the first successful trial between two central banks. This activity repositioned DLT as not only a reliable method of facilitating a near-instantaneous currency swap, but also a tool with which to ensure that central banks inside and outside of the G20 can trust one another.

Blockchain also builds stakeholder trust in collection and recovery. The immutability of the data allows loan pools to be audited and independently verified, using the digital signature of the source provider as proof of authenticity and confirming compliance with underwriting guidelines. In the event that a delinquency trigger is tripped, custody of a loan

on blockchain facilitates outreach to borrowers in default and ensures that subsequent special servicing complies with servicing guidelines. Furthermore, blockchain simplifies the enforcement of investors' rights and protects asset values by immutably recording on chain the beneficial owners of assets in every transaction—including ownership transfers—and hence building a comprehensive and secure ownership registry that ensures deals can be credit-positive.

Existing market participants, including large financial institutions, are using blockchain to achieve these effects and to leverage competitive advantage.

- **Provenance.io** is the first blockchain to support the successful origination, financing and servicing of loan assets on chain, permitting evaluation of real-time financial performance.
- The **National Bank of Cambodia** will use blockchain technology in its national payments system in a full-scale deployment across 12 banks by the end of 2020.
- **Globacap** offers investment in tokenised assets. The token's smart contract automatically fulfils all legal and administrative requirements for the registration and transfer of assets.
- The **Commonwealth Bank of Australia**, in partnership with the World Bank, created Project BOND-1 in 2018—the world's first bond to be created, allocated, transferred and managed through its life cycle using blockchain technology.
- In France, **Project MADRE** has replaced the centralised process for the provisioning and sharing of SCIs

with smart contracts using a private Ethereum implementation.

- The **People's Bank of China** announced the launch of a yuan-denominated blockchain-based CBDC in 2019, shortly after Facebook launched Libra.

Banking institutions are adopting blockchain not only to drive interbank efficiency, but also to raise levels of financial inclusion. The National Bank of Cambodia, for example, has implemented blockchain to provide access to retail banking for Cambodia's underbanked, supporting interoperable retail payments between citizens and businesses. By encouraging citizens to adopt bank accounts, the government is supporting individual savings, promoting financial stability and supporting economic growth.

Moreover, this rare instance of a national rollout of blockchain technology demonstrates the ability of technology to leapfrog traditional wholesale interbank processes, providing a highly efficient PCS process that other, similar countries in the Association of Southeast Asian Nations (ASEAN) could easily replicate. The Bank of Thailand has launched its Scripless Bond project: in a successful trial using HyperLedger Fabric, Thailand reduced to just 2 days a bond registration and issuance that has traditionally taken 15 days.⁶

The Government of the People's Republic of China (PRC), meanwhile, caused both interest and alarm in governmental, public and private sector circles when it announced its digital yuan. To some extent, it was a response to launch of the Facebook-backed Libra project a few months previously⁷ and, with one of the world's largest economies now supporting a CBDC, we can expect other governments to accelerate their own efforts in the near future.

3.4 Key Considerations for Future Development

With consumers becoming more digitally aware and questions being asked about the future of cash, new market entrants are challenging traditional expectations of bank-based service delivery. So-called programmable money may diversify the range of currencies and shift the focus away from stalwarts such as the US, Canadian or Australian dollar; CBDCs may become familiar as part of the financial services ecosystem.

Central bank digital currencies offer benefits such as a resilient payment system and the potential to improve AML/KYC functionalities while reducing illicit activities. There are, however, equally significant risks to CBDCs, including financial exclusion should populations not bridge the digital divide, financial instability as a consequence of bank disintermediation and new risks that may yet be unknown. There has consequently been a lot of research into CBDCs and most early-stage pilots have focused on their domestic use.

Some of the central banks currently considering digital currencies include:

- the **Bank of Thailand**, whose Project Inthanon is exploring how a CBDC can make interbank payments and liquidity management more efficient;
- the **Eastern Caribbean Central Bank**, which is exploring DLT in the context of economic growth, payments system resilience and financial inclusion; and
- **Sveriges Riksbank** (Sweden's central bank), which is investigating a blockchain-based digital krona as an alternative to cash as the use of cash in Sweden declines.

Because pilots often occur in countries whose domestic interbank payment systems are already efficient, however, early conclusions are that there is no significant value in centring a CBDC on this goal alone—as the Bank of Canada's Project Jasper, the South African Reserve Bank's Project Khokha, and the European Central Bank and Bank of Japan's joint Project Stella all demonstrate. In a 2017 report, for example, Danmarks Nationalbank (Denmark's central bank) explicitly noted its uncertainty that a CBDC would be of any benefit to Denmark's existing payment solutions.⁸ Where domestic interbank payment systems are *not* yet highly efficient, however, such as in some developing economies, a CBDC has positive potential.

More broadly, some experts believe that we may see forms of CBDC facilitate alternative or bilateral international payments systems that operate outside the current dominant models. A blockchain-based state currency could supersede the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system, diversifying and moving international payment processes and monetary systems away from the US dollar.



Banking institutions are adopting blockchain not only to drive interbank efficiency, but also to raise levels of financial inclusion.

In this way, a CBDC might offer states and financial actors more autonomy over international payments. For example, in February 2018, Venezuela allegedly issued its petromoneda (or petro) digital currency on NEM's blockchain platform in a bid to attract government financing during rapidly deteriorating domestic economic conditions and a plummeting bolivar, while China's digital yuan, today focused on M0 money supply, could readily be expanded. Given China's global importance as an economic superpower, the digital yuan could be a ready vehicle to facilitate trade.

Blockchain technology is therefore an ecosystem enabler—but it is not a panacea: as it is implemented more widely, complementary technologies will mature, and blockchain will come to be only one element in blended technology.

Endnotes

- 1 For more in-depth guidance on digital currencies, see Commonwealth Working Group on Virtual Currencies (2019). *Regulatory Guidance on Virtual Currencies* [online]. Retrieved from https://thecommonwealth.org/sites/default/files/key_reform_pdfs/D16999_GPD_Virtual_Currnecs.pdf; Boar C, Holden H, Wadsworth A (2020). 'Impending Arrival: A Sequel to the Survey on Central Bank Digital Currency'. Bank for International Settlements (BIS) Papers No. 107 [online]. Retrieved from www.bis.org/publ/bppdf/bispap107.pdf; Ye C, Desouza K (2019). 'The Current Landscape of Central Bank Digital Currencies'. *Brookings*, 13 December [online]. Retrieved from: www.brookings.edu/blog/techtank/2019/12/13/the-current-landscape-of-central-bank-digital-currencies/
- 2 Commonwealth Secretariat (2019). *Regulatory Guidance on Virtual Currencies* [online]. Retrieved from: https://thecommonwealth.org/sites/default/files/key_reform_pdfs/D16999_GPD_Virtual_Currnecs.pdf
- 3 By the 'Internet of Things', we mean the informal network of connected electronic devices that helps to provide us with ubiquitous data about the world around us.
- 4 World Economic Forum (2019). *Central Banks and Distributed Ledger Technology: How Are Central Banks Exploring Blockchain Today?* [online]. Retrieved from: www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf
- 5 Accenture (2017). *Banking on Blockchain: A Value Analysis for Investment Banks* [online]. Retrieved from: www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf
- 6 Bank of Thailand (2018). *Project DLT Scripless Bond: Investing in Thailand's Future—Transforming the Securities Markets Infrastructure with Blockchain* [online]. Retrieved from: www.bot.or.th/English/DebtSecurities/Documents/DLT%20Scripless%20Bond.pdf
- 7 Baker P (2019). 'Unlike Libra, Digital Yuan Will Not Need Currency Reserves to Support Value: PBOC Official'. *Coindesk*, 23 December [online]. Retrieved from: www.coindesk.com/unlike-libra-digital-yuan-will-not-need-currency-reserves-to-support-value-pboc-official
- 8 Danmark's Nationalbank (2017). 'Central Bank Digital Currency in Denmark'. *Analysis*, 15 December [online]. Retrieved from: www.nationalbanken.dk/en/publications/Documents/2017/12/Analysis%20-%20Central%20bank%20digital%20currency%20in%20Denmark.pdf

Chapter 4

Digital Identity



Digital Identity

Key points

- Digital identity is a keystone issue in helping an additional 1.1 billion people—mostly in Africa and Asia—to access financial services.
- Analogue, paper-based identity systems are siloed and inflexible, exacerbating financial exclusion. Digital identity systems remedy many of these effects.
- Experiments with digital identity are being conducted across the Commonwealth, with an emphasis on federated (versus centralised) approaches.
- Public consultation prior to introducing a new identity system is key to its success. This allows users to make valuable comment on the system's design, and it builds their trust and confidence in the system, which can help to drive its adoption.

4.1 Introduction

The World Bank estimates that there are more than 1.1 billion people globally who are unable to prove their identity with official documentation. As a result, they lack access to financial services, health care, education and social services. Most of these people are in Africa and Asia.¹ Global consulting firm McKinsey & Co. estimates that another 1 billion people have formal identity documentation (often referred to simply as ID) but cannot use it on digital channels, locking them out of the digital economy, while 45 per cent of women over the age of 15 in low-income countries lack ID compared to 30 per cent of men.²

The World Bank has highlighted the introduction of robust, inclusive and responsible digital identity systems as a priority action with the potential to progress many of the United Nations Sustainable Development Goals (SDGs), including aspects such as social protection, the empowerment of women and girls, financial inclusion, governance, health care, digital development and humanitarian assistance.³

Digital identity systems have the potential to allow more people to access basic services, including financial services, fuelling economic growth and reducing human rights abuses.

Global challenges such as the refugee crisis in Latin America, Europe and other regions, as well as the 3.5 billion people who are underbanked or unbanked because financial services institutions cannot verify their identity or assess their credit profile (an attribute of their identity), highlight the need for a viable identity solution.⁴

These challenges inevitably result in the exploitation of those without legal ID and the economic exclusion of those without legal ID. Moreover, the value that people add to an economy is lost when they have no ID or have ID but cannot use it on digital channels, giving the government no way of tracking their contributions.

Digital identity systems have the potential to address these wide-reaching implications, allowing more people to access basic services, including financial services, fuelling economic growth and reducing human rights abuses. McKinsey & Co. estimates that digital or electronic ID has the potential to add economic value of at least 3 per cent and potentially as much as 13 per cent of gross domestic product (GDP) by 2030.⁵

4.2 Context

In its simplest form, ID is supporting evidence that an individual is who they say they are. It has been suggested that the very first government-issued form of ID were the letters with which ancient Persian king Artaxerxes guaranteed prophet Nehemiah safe passage to Jerusalem in 450 BCE. Later, in 1414, King Henry V granted 'safe conduct' documents in what is believed to be the first form of 'passport'.⁶

As the passport has developed, it has continued—even in its most advanced form—to centre on evidencing identity in face-to-face transactions. Moreover, it is common knowledge that a passport and

other similar forms of ID can be, at the very least, inaccurate; at worst, it might be forged. There are also limitations to any form of ID that relies on an address as evidence of identity—especially in many developing economies and rural areas, where people with the same or similar names may live at the same address.

In the modern electronic era, it is becoming increasingly difficult to prove that we are who we say we are, even if we have ID. While some simple transactions do not require the parties to verify each other's identities, if a person is to participate in modern society—and especially if they are to access financial services—they need a verifiable form of identity.

4.2.1 The Basic Functions of an Identity System

The implications of today's legacy ID systems are wide-ranging, with differing impacts on those who have no ID and those who have ID that they cannot use digitally.

As Figure 4.1 outlines, an ID is one component of a system that:

- identifies an individual;
- authenticates that identity; and
- grants (or withholds) access depending on whether that individual is authorised or eligible to participate in the activity they are requesting.⁷

4.2.2 The Flaws in Legacy Identity Systems

It is evident that current identity systems are broadly inefficient and often ineffective. The design of legacy systems is:

- document-based, making them cumbersome, as well as prone to human error and exploitation;

Figure 4.1 The basic roles of an ID system.

Who are you?	Are you who you claim to be?	Are you authorised or eligible?
1	2	3
Identification	Authentication	Authorisation
Establishing a person's identity by gathering and checking relevant identity information	Checking that a person is who they claim to be based on evidence of one or more personal details	Checking specific attributes to confirm whether or not a person is authorised or eligible to participate

Source: Adapted from World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>

- siloed, storing identity information discretely; and
 - inflexible, with current forms of identity codified in documents that cannot easily be adapted to meet modern transaction requirements.⁸

Any new identity system, digital or otherwise, should address these shortfalls and their implications.

More specifically, inefficient and ineffective legacy systems leave behind those who **have no formal ID**, with profound impacts, including:

 - the economic exclusion of individuals and (sometimes large) groups of people;
 - the exclusion of individuals and groups of people from basic services such as health care and social services;
 - the exclusion of refugees who often cannot relocate without formal ID;
 - constraints on economic development when financial services and other
- businesses cannot deliver to individuals and populations;
 - compromised national safety and security when nation-states are unable to identity and manage the people crossing their borders; and
 - issues of regulatory compliance for financial services and other businesses that are required to adhere to anti-money-laundering (AML) or know your customer (KYC) rules.

Even those who **have an ID but cannot use it digitally** experience some of these impacts, including:

 - exclusion from digital services when those services fail to recognise formal ID;
 - exclusion from financial services where their ID does not meet AML/KYC requirements, which also strips the economy of the value that individual would otherwise add; and
 - the costs of compromised or forged ID, which represent both personal

and financial risks for individuals and can render a cost to financial services institutions and public services should, for example, false ID be used to claim social services benefits.

4.3 Description

4.3.1 What is Identity in the Modern Era?

We can conceive of identity as a series of attributes—physical, legal, electronic and behavioural—that combine to form a unique picture of an individual.

- **Physical attributes** are the features that identify an individual uniquely and are harder to forge or manipulate than others. They include a person's DNA, as well as *physical biometrics* such as fingerprints and facial features. Recent technological advances based on facial recognition and scanning fingerprints have, however, proved to be easily hacked.
- **Legal attributes** are those associated with the 'traditional' forms of ID that are widely used globally, such as a driver's licence or passport. Increasingly, these forms of ID are now supplanted or augmented by physical biometrics (see *above*).
- **Electronic attributes** are those that relate to the increasing amount of time individuals are spending online and on their mobile or smartphones. They include details such as a person's email address, social media accounts, online actions and Internet Protocol (IP) address. Increasingly, advertisers and other parties are using individuals' IP addresses to track and trace their online actions, which data the advertisers then commercialise.
- Using **behavioural attributes** as a form of identification is a recent technology

and it has been shown to be a unique, reliable means of identifying an individual. This type of data includes details such as locations visited and spending patterns, and using this data as part of identity is part of a growing field known as *behavioural biometrics*.⁹

It is now widely accepted that legal attributes and traditional forms of ID are flawed and are open to abuse. While each of the above attributes can be used individually to identify a person, they are more powerful and reliable when used in combination—and advances in technology have allowed actors to explore their potential in relation to a new form of *digital identity*.

4.3.2 Digital Identity

A digital identity can be defined as a set of digital records that verify that an individual is who they say they are and allow them to engage in transactions in the modern—digital—world.¹⁰ McKinsey & Co. benchmarks a 'good' digital identity as being:

- verifiable to a high degree of assurance;
- unique; and
- established with an individual's consent.

Digital identity systems have been trialled and implemented in, for example, India, Estonia, the Nordic regions, Singapore and Canada. India created the Aadhaar project in 2009, which now covers an estimated 89 per cent of its population, while the others have also all deployed formats of an electronic identity—or e-ID—system (see *later in this chapter*).

4.3.3 Digital Identity Technologies

The proliferation of mobile phone technology is one of the most significant

contributory factors in the development of digital identity. Among the data that our mobile phones gather is **biometric identity** data. Biometric identity systems use facial recognition, fingerprints, heartbeats, speech patterns, walking patterns and hand movements to build a picture of an individual's unique biometric attributes with which they can be identified.¹¹

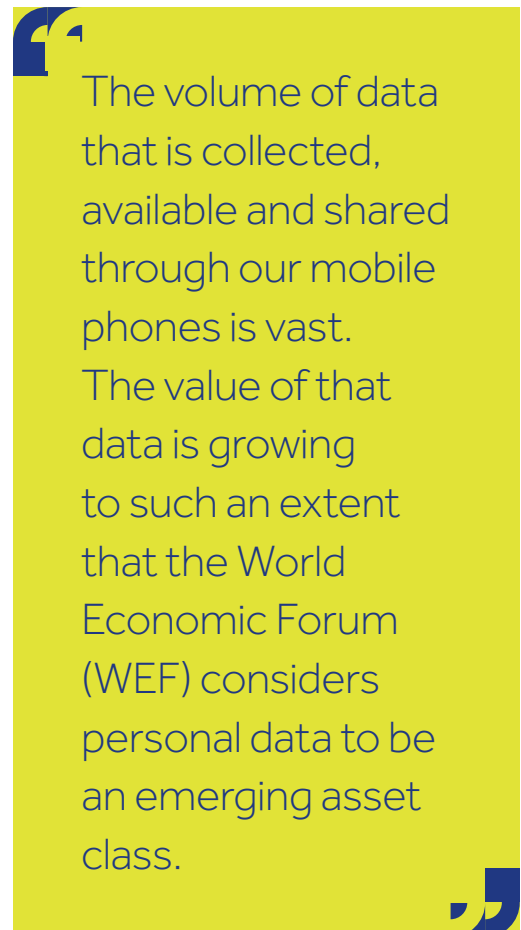
The volume of data that is collected, available and shared through our mobile phones is vast, and the value of that data is growing—to such an extent that the World Economic Forum (WEF) considers personal data to be an emerging asset class.¹² While traditional identity attributes are commonly gathered in large databases that are vulnerable to hackers, as this sensitive personal data accumulates and new models aim to monetise identity data for the benefit, rather than the detriment, of individuals, new technologies are solving new problems. **Encryption** secures that identity data, for example, and **tokenisation** organises the attributes so that they can be managed and monetised more readily.¹³

We encrypt (encode) data by inputting it—together with another parameter (or 'key')—into an encryption algorithm (or 'cipher'). There are two basic methods of encryption for securing data transmission:

- *symmetric encryption*, whereby a single key—a shared secret—is used to both encrypt (encode) and decrypt (decode) information; and
- *asymmetric encryption* (also known as public key encryption), whereby a pair of related keys are used—one to encrypt the data and the other to decrypt it.¹⁴

In that context and in light of data protection principles, **self-sovereign ID** is a model that

centres the user in the administration of their identity. Historically, an oligopolistic, corporate entity might have expected to hold a user's personal data in a central database or data repository; now, a decentralised identity system will give the user absolute control over their own identity data and the benefits to the consumer are numerous. Not only is an individual granted more insight into who is using or reviewing their personal information, but also they can exercise control over the financial or health data that allows them to access better financial or health-care services, and they can even take advantage of the 'right to be forgotten' enshrined in the General Data Protection Regulation (GDPR) in the European Union (EU).¹⁵



The volume of data that is collected, available and shared through our mobile phones is vast. The value of that data is growing to such an extent that the World Economic Forum (WEF) considers personal data to be an emerging asset class.

4.3.4 Introducing Digital Identity Systems

While it is clear that digital identity has the potential to remedy gaps in current legacy systems, digital identity systems are not without their risks. Such risks can include, among others:

- stakeholders rejecting the technology because they do not trust it and they have been consulted only inadequately on its introduction;
- the technology being ineffective because of inadequate planning;
- insufficient technical support or public education to drive widespread adoption and facilitate efficient use;
- unsustainable operations because of inefficient systems design and/or high costs; and
- policy changes at a governmental level.

To mitigate these risks, large-scale digital identity projects may take one of three main approaches to governance.

- **Centralised approach** Identity is handled by a single (usually public) entity. This approach allows for streamlined decision-making and implementation, as well as high data aggregation capability, but positioning the system with only one entity has implications for risk, liability and cost. Examples of this type of approach are the digital ID programmes launched by India and Estonia.
- **Federated approach** In this model, a few entities establish a formal digital identity network. This approach spreads the cost and mitigates the potential for abuse, but it does introduce the need for co-ordinated decision-making, which

adds complexity. Examples of this approach include SecureKey Concierge in Canada and NemID in Denmark (both led by financial institutions), gov.uk's Verify (launched by the public sector), and Sweden's BankID (a public-private partnership, or PPP).

- **Decentralised approach** This type of entity would be part of an open—potentially blockchain (see Chapter 3)—network with no institutional owners. The benefits of this approach include centring the user's control over the data and a minimised risk of abuse or manipulation by a central managing authority. However, such models remain in the early stages and have not yet been tested at scale, while there are security challenges inherent to such a system. Examples include TUPAS in Finland (a private sector solution) and Solid, launched by Tim Berners-Lee in 2018.¹⁶

With each of these approaches, the more centralised the approach, the more cost-effective and easy it is to implement, but the higher the degree of trust that the data-holding party must command.¹⁷

4.4 Key Considerations for Future Development

In looking to the future of digital identity and digital identity policy, some of the issues include stakeholder consultation and regulation.

4.4.1 Stakeholder Consultation

Governments must take the needs of all stakeholders into account when developing a digital identity policy. Public consultation at the very outset of the project will be key to building trust and buy-in, which user input on the system's design can help to drive its adoption and improve the overall success of the project.

Among the parties with which government must consult are citizens, private sector stakeholders, civil society representatives and stakeholders within government itself.

4.4.2 Regulation

Given that a range of different attributes constitutes digital identity, when developing a digital identity policy it is also imperative to consider how that personal information is managed and how much control the user is given of that information. The GDPR is the high-water mark of data protection and privacy regulation, and policies covering data protection and privacy should be measured against it.¹⁸

A useful tool in policy-making around digital identity is privacy by design (PBD), which sets out seven foundational principles for user privacy.¹⁹ Any public or private actor making policy or building digital identity systems should:

1. be proactive not reactive;
2. lead with privacy;
3. embed privacy;
4. retain full functionality;
5. ensure end-to-end security;
6. maintain visibility and transparency; and
7. respect user privacy.

In relation to the fifth principle, cybersecurity (see Chapter 6) is a key factor in developing a digital identity policy and system, and should underpin any new (and indeed legacy) security and legal frameworks.²⁰ Encryption is a critical aspect of cybersecurity in any system containing sensitive information.²¹ We should assume that any system storing personal information will be subject to cyber attack and encrypt that data accordingly.

More broadly, legislation and regulation—the legal framework at both national and supranational levels—is likely to prescribe behaviours relating to digital identity that will include, for example, rules of issuance and AML/KYC requirements in financial services. Remaining up to date with these and ensuring that any digital identity policies and systems are compliant will be crucial to their success.²²

In the regulatory context and others, when it comes to designing any digital identity policy and system, interoperability—that is, how digital identity and aspects of digital identity will be generated, managed and combined—is important. One example of an effort to increase interoperability is the EU's eIDAS Regulation, which ensures that people and businesses can use their e-IDs to access public services across borders.²³

4.4.3 The Guiding Principles for Robust Digital Identity Policies and Systems

The WEF outlines the following guiding principles to inform decision-making when developing robust and value-adding systems and, in this case, policies.

- **Social good** The system should be available to all users and designed to deliver maximum benefit to the widest possible range of stakeholders. It should be non-discriminatory and inclusive.
- **Privacy-enhancing** User information must be exposed to and shared with only the *right* entities under the *right* circumstances.
- **User-centric** Users must have control over their own information and be able to determine who holds and accesses it.

- **Viable and sustainable** The system must be economically sustainable and resilient to shifting political priorities.
- **Open and flexible** The system must be built on open and flexible standards to allow scaling and development, and those standards and guidelines must be transparent to stakeholders.²⁴

In all of this, one thing is very clear: capturing the potential value of digital identity will demand careful system design and deliberate government policies if we are to mitigate the risks.²⁵

Endnotes

- 1 World Bank (2017). '1.1 Billion "Invisible" People without ID Are Priority for New High Level Advisory Council on Identification for Development'. Press release, 12 October [online]. Retrieved from: www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development
- 2 McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx
- 3 World Bank (2017). '1.1 Billion "Invisible" People without ID Are Priority for New High Level Advisory Council on Identification for Development'. Press release, 12 October [online]. Retrieved from: www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development
- 4 Chamber of Digital Commerce (2017). *Blockchain and Financial Inclusion* [online]. Retrieved from: <https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf>
- 5 White O et al. (2019). 'Digital Identification: A Key to Inclusive Growth'. *McKinsey.com*, 1 April [online]. Retrieved from: www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-identification-a-key-to-inclusive-growth
- 6 Benedictus L (2006). 'A Brief History of the Passport'. *The Guardian*, 17 November [online]. Retrieved from: www.theguardian.com/travel/2006/nov/17/travelnews
- 7 World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>
- 8 World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
- 9 Schukai R, Chadwick S, Baker T (2017). 'Who Are You? Defining Digital Identity and Authentication Technologies'. *Thomson Reuters*, 28 June [online]. Retrieved from: <https://blogs.thomsonreuters.com/answerson/digital-identity-authentication-technologies/>
- 10 World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
- 11 Glaser A (2016). 'Biometrics Are Coming, Along With Serious Security Concerns'. *Wired.com*, 9 March [online]. Retrieved from: www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/
- 12 World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class* [online]. Retrieved from: www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
- 13 World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>
- 14 *Ibid.*
- 15 Allen C (2016). 'The Path to Self-sovereign Identity'. *Coindesk*, 27 April [online]. Retrieved from: www.coindesk.com/path-self-sovereign-identity; 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, 4 May 2016, OJ L 119/1.
- 16 McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx
- 17 *Ibid.*
- 18 European Commission (2020). 'Complete Guide to GDPR Compliance' [online]. Retrieved from: <https://gdpr.eu/>
- 19 Deloitte, Ryerson University (2016). *Privacy by Design: Setting a New Standard for Privacy Certification* [online]. Retrieved from: www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF; Cavoukian A (2011). 'Privacy by Design: The 7 Foundational Principles'. *Internet Architecture Board*, March [online]. Retrieved from: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
- 20 GSMA (2016). 'Digital Identity: Regulatory Trends and the Role of Mobile'. 3 November [online]. Retrieved from: www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-regulatory-trends-and-the-role-of-mobile/
- 21 World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>
- 22 GSMA (2016). *Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile: Considerations for Emerging Markets* [online]. Retrieved from: www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf
- 23 Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, 9 September 2015, OJ L 235/1.
- 24 World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
- 25 McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx

Chapter 5

Big Data/Big Data Analytics



Big Data/Big Data Analytics

Key points

- Big data/big data analytics is the lifeblood of AI, because it is what fuels AI algorithms.
- Big data is evaluated in terms of its volume, velocity, variety, veracity and value.
- Financial institutions use big data/big data analytics for activities ranging from marketing to credit assessment.
- Big data/big data analytics introduce new risks in financial services if not partnered with digital identification systems, because their widespread adoption could otherwise exacerbate financial exclusion.

5.1 Introduction

In all walks of life, individuals, organisations and governments rely on data to help them to make good decisions.¹ In the last 30 years, vast amounts of data have come to be collected on every possible aspect of modern life and these large datasets are now known as 'big data'—a phrase that many people began to use a decade or two ago without fully understanding what it meant.

While the amount of data collected and stored has increased exponentially, development of the skills and technology that allow us to analyse and use this data has gathered momentum more recently. Big data is the lifeblood of artificial intelligence (AI), for example. Without large datasets, AI models and algorithms cannot be refined and function effectively or accurately.

With detailed data that touches on almost every aspect of our lives never more readily available, we must be cautious of its potential to fuel both positive and negative outcomes. Solid governance of the collection and use of that data is critical if we

are to ensure it is used only for positive ends, to enhance decision-making and to protect individuals' rights.

5.2 Context

The history of data analytics goes back to 18,000BCE, with evidence that Palaeolithic peoples marked notches into sticks or bones to keep track of and compare trading activity and supplies. In 1663, John Graunt conducted what is believed to be the first statistical analyses in trying to develop an early warning system for the bubonic plague.²

In 1928, the method for storing information magnetically on tape was invented, which led later, in 1965, to the first large data centres. These were limited, however, by the fact that data was at that time recorded and stored in physical form. In 1996, shortly after the birth of the internet, electronic storage became more cost-effective than paper storage, and in the early 2000s—as the capacity to store data skyrocketed and the need to adapt analysis to suit its volume and scope become obvious—the term 'big data' was coined.³

In 2010, chair of Google Eric Schmidt told a conference that as much data was now created every two days as had been created between the beginning of human civilisation and 2010.⁴

In 2014, consultancy IDC projected that, globally, there would be more than 44 zettabytes of data generated by 2020

compared with 4.4 zettabytes in 2013.⁵ A zettabyte is a difficult measure to visualise: it is 2^{70} bytes—or as much data as can be stored on 250 billion DVDs. A gigabyte—1 million bytes—is a common unit in measuring computing memory: it has been said that if each gigabyte in a single zettabyte were a brick, those bricks would be enough to build 258 Great Walls of China.⁶

As our ability to generate, collect and store information has grown, so has the potential for us to generate richer insights from this data. It has been clear that holding large and rich datasets alone are not an end in itself; the key to the value of data lies in its analysis.

There are three key terms that we can define here.

meaningful insights and inform good business decisions.⁹

- **Big data** is used in many different ways—to refer to large datasets, and to refer to the exponential increase of data and availability of data in the world today.⁷ Big data is said to display the following '5Vs'.

- **Volume** Big data—the size of the dataset—has to be large. There is no set agreement on how large 'large' is; it is relative and it is ever increasing.
- **Velocity** This refers to the speed at which data is collected and analysed.
- **Variety** With increasing volume and velocity comes increased variety. A dataset with wider variety can lead to richer insights.
- **Veracity** This refers to the quality of the data: is it 'clean' and accurate?⁸
- **Value** By this, we mean whether the data and its analysis lead to

- **Data science** is the field of studying data. The goal of data science is to improve decision-making through the analysis of data.¹⁰
- **Data analytics** is the multidimensional field that uses mathematics, statistical modelling and machine learning to find meaningful patterns in data.¹¹

As technology evolves, so does our ability to collect, store and analyse data—but all of these processes are dependent on advances in hardware and software development, which act as the key enablers in a big data ecosystem.

While the positive implications of big data are vast, including enhanced decision-making, predictive technology and increased profitability, the potential for abuse is equally apparent. One instance emerged when political consulting firm Cambridge Analytica was found to have misused individual data, mined from Facebook, during the 2016 US presidential elections.¹² It is therefore essential that any big data ecosystem also include measures to prevent such abuse.

5.3 Description

The application of big data across financial services touches many aspects of our lives, ranging from payments, through lending and investment decisions, to impact more broadly on how financial services markets function. This section will present an overview of some of the relevant technologies and applications that support the use of big data in these contexts.

5.3.1 Customer Segmentation and Personalised Marketing

Big data offers financial and other services providers the ability to refine their customer segmentation at a more granular detail than was previously possible. This allows them to understand in detail what different customer segments need and it allows financial services organisations, such as credit card companies, to offer personalised marketing and tailored discounts to their users.¹³

5.3.2 Credit Assessment

Big data has given rise to alternative credit models aiming to address the role of existing credit models in financial exclusion.¹⁴ Credit assessment procedures have long relied on regression analysis, which assumes that one behaviour predicts another, such as that companies and individuals who do not pay their loans on time will continue not to pay their loans on time. Alternative credit assessment models are now emerging that are based on an individual's education level or the reputation of their school as an indicator of whether or not they will default on a loan, while others use social media analysis.

These new models are not, however, without their challenges. Not all data is reliable for credit scoring, for example, and there are currently gaps in the law governing these new models to ensure that they are, and are used in ways that are, accurate, fair and transparent.¹⁵

The rise of behavioural analytics and social physics has fuelled a more robust approach to alternative modelling based on big data indicators to assess the likelihood of someone defaulting or repaying a loan.

- **Behavioural analytics** is the study of human behavioural data to identify meaningful patterns and draw inferences or make predictions based on those patterns.¹⁶
- **Social physics** applies the principles of physical sciences to study of how groups of people make decisions by analysing how information and ideas flow from person to person.¹⁷

Both of these can be applied to improve not only credit scoring, but also fraud detection, identity verification, regulatory compliance and enforcement, predictions of consumer behaviour, and stock trading and investing decisions.

5.3.3 Stock and Commodity Trading

Big data and machine learning have significantly influenced stock and commodity trading. Not only does big data improve the likely outcomes of financial services for individuals, but also the application of AI technology to capital markets reduces the barriers to entry for many individuals and widens participation in the market.¹⁸ These types of new trading technology have fuelled adoption of electronic trading platforms and virtualised trading environments¹⁹—although this is not without risk. For example, algorithmic and high-frequency trading (HFT) have been known to cause flash crashes in the market, such as the 2010 US flash crash.

In foreign exchange (forex) brokerage, assessing risk is essential to successful operations. The broker must be able to see

data in real time and be alerted to specific preferences, market statuses, profit and loss, exposure and market volatility. The unified data that we can now gather from a wide spectrum of resources (Web, mobile, social, customer relationship management, affiliates, etc.) is the key to a holistic overview of platform performance on which managers can base their decisions.²⁰

5.3.4 Regulatory Compliance and Fraud Detection

For financial services organisations, regulatory compliance is a key priority that typically involves significant amounts of paperwork, resulting in millions of user records. Machine learning and other AI technologies analyse this big data to detect compliance irregularities and even fraud more accurately and efficiently than ever before. In some cases, it can detect instances that would be beyond human capacity. For example, in 2017 Credit Suisse reported a 45-fold increase in productive alerts resulting from its predictive monitoring of transactions compared to the year before, and it measured resolution of the alerts as 60 per cent faster at a fraction of the historical cost.²¹

Some large financial services providers, such as JP Morgan Chase, use big data/big data analytics to detect fraud by analysing the activities of their own staff, including not only internet search histories, but also personal data including emails and call history. JP Morgan also applied big data in an optimised real-estate price-determination model for use when selling property the bank acquired as collateral on loans that are now in default (see below).²²

5.3.5 Other Contexts

Other contexts in which big data can be valuable include real-estate markets. With big data/big data analytics, lenders can

minimise social loss by analysing a local property market to determine the most marketable price at which a property will sell quickly, allowing a debtor to avoid insolvency.²³

Big data also has the potential to underpin productivity and release consumer surplus. For example, McKinsey & Co. estimates that a retailer using big data can increase its operating margin by more than 60 per cent, while services enabled by personal-location data can allow consumers to capture US\$600 billion in economic surplus.²⁴

5.4 Key Considerations for Future Development

It is important to view big data not in isolation but as an ecosystem that includes the various sources from which data is gathered, the spaces in which this data is traded, the analysis of that data and the decisions that the analytics inform.

Among the key considerations in these regards is **data protection**. While effective AI systems of this type are dependent on personal data, users' rights must remain at the forefront of any policy governing big data. The leading example of regulation in this context is the General Data Protection Regulation (GDPR) of the European Union (EU): a benchmark against which policies covering data protection and privacy should be measured.²⁵ Its basic principles include user control of their own personal data, the requirement that users explicitly consent to others using their data and a right to be 'forgotten' (i.e., to request deletion of data).²⁶

Policy considerations should also reinforce corporate responsibility for data governance. Businesses that are collecting data of any sort, but personal data in particular, are responsible—and should be held accountable—for the security and

Big data has the potential to underpin productivity and release consumer surplus. It is estimated that a retailer using big data can increase its operating margin by more than 60 per cent.

legitimate use of this data. Any organisation gathering, storing and/or managing data must therefore put sound data governance structures in place.²⁷

Open data can therefore be contrasted with personal data. Open data is (a) publicly available and (b) licensed for reuse, and it is ideally relatively easy to (re)use.²⁸ Open data is available to researchers and other organisations who will analyse it to extract the most value. Clearly, therefore, this type of data does not include personal data and data scientists must take care when selecting their sources.

In fact, in 2019 it was estimated that while the number of trained **data scientists** was increasing, demand for these skills was growing even more rapidly.²⁹ From a policy perspective, the recruitment and development of skilled data science

professionals is consequently a fundamental component of the big data ecosystem and an effective digital economy.

Finally, while availability and types of data vary from country to country and personal data varies according to demographics including age groups, income brackets, gender and geographic locations, any policies focused on big data in financial services or elsewhere must take care to bridge the **digital divide**. We must take care to ensure that big data applications and solutions do not exclude any one or more groups, nor should we assume that our findings are universally applicable unless proved to be so.³⁰

Endnotes

- 1 United Nations (2020). 'Big Data for Sustainable Development' [online]. Retrieved from: www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html
- 2 World Economic Forum (2015). 'A Brief History of Big Data Everyone Should Read'. 25 February [online]. Retrieved from: www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/
- 3 *Ibid.*
- 4 *Ibid.*
- 5 Adshead A (2014). 'Data Set to Grow 10-fold by 2020 as Internet of Things Takes off'. *ComputerWeekly.com*, 9 April [online]. Retrieved from: www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off
- 6 Barnett T Jr (2016). 'The Zettabyte Era Officially Begins (How Much Is That?)'. *Cisco Blogs*, 9 September [online]. Retrieved from: <https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that>
- 7 University of Wisconsin Data Science (2020). 'What Is Big Data?' [online]. Retrieved from: <https://datasciencedegree.wisconsin.edu/data-science/what-is-big-data/>
- 8 BBVA (2017). 'The Five V's of Big Data'. 8 May [online]. Retrieved from: www.bbva.com/en/five-vs-big-data/

- 9 Jain A (2016). 'The 5 V's of Big Data'. *Watson Health Perspectives*, 17 September [online]. Retrieved from: www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/
- 10 Kelleher J D, Tierney B (2018). *Data Science*. Cambridge, MA: MIT Press.
- 11 SAS (2020). 'Analytics: What It Is and Why It Matters' [online]. Retrieved from: www.sas.com/en_us/insights/analytics/what-is-analytics.html
- 12 Malan D (2018). 'The Law Can't Keep up with New Tech: Here's How to Close the Gap'. *World Economic Forum*, 21 June [online]. Retrieved from: www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/
- 13 Kim S (2016). 'Big Data Use Cases in Finance'. *Samsung.com*, 6 September [online]. Retrieved from: www.samsungsds.com/global/en/support/insights/090617_Eng_BigData1.htm
- 14 Pan W, Aharony N, Pentland A (2011). 'Composite Social Network for Predicting Mobile Apps Installation'. *arXiv.org*, 2 June [online]. Retrieved from: <https://arxiv.org/abs/1106.0359>
- 15 Hurley M, Adebayo J (2017). 'Credit Scoring in the Era of Big Data'. *Yale Journal of Law and Technology*, 18(1) [online]. Retrieved from: <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt>
- 16 Biddle S (2019). 'Thanks to Facebook, Your Cellphone Company Is Watching You More Closely than Ever'. *The Intercept*, 20 May [online]. Retrieved from: <https://theintercept.com/2019/05/20/facebook-data-phone-carriers-ads-credit-score/>
- 17 Wladawsky-Berger I (2018). 'Social Physics: Reinventing Analytics to Better Predict Human Behaviors'. *Wall Street Journal*, 14 September [online]. Retrieved from: <https://blogs.wsj.com/cio/2018/09/14/social-physics-reinventing-analytics-to-better-predict-human-behaviors/>
- 18 Cuen L (2017). 'Fintech is Rebuilding Capital Markets, from AI to Crowdfunding Startups'. *International Business Times*, 20 October [online]. Retrieved from: www.ibtimes.com/fintech-rebuilding-capital-markets-ai-crowdfunding-startups-2559398
- 19 Deutsche Börse AG, Celent (2016). *Future of Fintech in Capital Markets* [online]. Retrieved from: www.deutsche-boerse.com/resource/blob/37024/ed055219caeb553f43950609d29e1bb3/data/future-of-fintech-in-capital-markets_en.pdf
- 20 Levy T L (2017). 'How Trading Companies are Leveraging Behavioral Analytics to Win Conversions and Retention'. *Datafloq*, 20 July [online]. Retrieved from: <https://datafloq.com/read/trading-companies-leveraging-behavioral-analytics/3442>
- 21 Credit Suisse (2017). 'How Big Data Analytics Is Transforming Regulatory Compliance'. 30 November [online]. Retrieved from: www.credit-suisse.com/about-us-news/en/articles/news-and-expertise/how-big-data-analytics-is-transforming-regulatory-compliance-201711.html
- 22 Kim S (2016). 'Big Data Use Cases in Finance'. *Samsung.com*, 6 September [online]. Retrieved from: www.samsungsds.com/global/en/support/insights/090617_Eng_BigData1.htm
- 23 *Ibid.*
- 24 Manyika J *et al.* (2011). 'Big Data: The Next Frontier for Innovation, Competition, and Productivity'. *McKinsey.com*, 1 May [online]. Retrieved from: www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation
- 25 Allen C (2016). 'The Path to Self-sovereign Identity'. *CoinDesk*, 27 April [online]. Retrieved from: www.coindesk.com/path-self-sovereign-identity; 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, 4 May 2016, OJ L 119/1.
- 26 European Commission (2020). 'Complete Guide to GDPR Compliance' [online]. Retrieved from: <https://gdpr.eu/>; Violino B (2019). 'Get Ready for More Data Privacy Regulations'. *ZDNet*, 12 March [online]. Retrieved from: www.zdnet.com/article/get-ready-for-more-data-privacy-regulations/

- 27 Sohail O, Sharma P, Ciric B (2018). '4 Pillars to Guide Data Governance for New Platforms'. *Wall Street Journal*, 10 October [online]. Retrieved from: <https://deloitte.wsj.com/cio/2018/10/10/4-data-governance-pillars-for-modern-data-platforms/>
- 28 Maarooof A (2015). *Big Data and the 2030 Agenda for Sustainable Development* [online]. Retrieved from: www.unescap.org/sites/default/files/Final%20Draft_%20stock-taking%20report_For%20Comment_301115.pdf
- 29 LinkedIn (2018). *LinkedIn Workforce Report: United States—August 2018* [online]. Retrieved from: <https://economicgraph.linkedin.com/resources/linkedin-workforce-report-august-2018>
- 30 Maarooof A (2015). *Big Data and the 2030 Agenda for Sustainable Development* [online]. Retrieved from: www.unescap.org/sites/default/files/Final%20Draft_%20stock-taking%20report_For%20Comment_301115.pdf

Chapter 6

Cybersecurity



Cybersecurity

Key points

- Cybersecurity is a serious and widespread challenge for financial services, with significant impact on both consumers and businesses.
- Commonwealth member countries must invest in both technology and training.
- A disciplined cybersecurity approach will look at systems, people and processes, and the 2018 Commonwealth Cyber Declaration enshrines these key principles.¹

6.1 Introduction

Cybersecurity remains one of the major challenges for financial institutions around the world. A lack of digital literacy and underinvestment in technology systems has resulted in a weak cyber infrastructure that has seen not only hundreds of millions of pounds stolen, but also billions of people's personal information (including irreplaceable biometric data files).

The Commonwealth Secretariat issued a Cyber Declaration at its Heads of Government meeting in April 2018, committing to a series of principles and actions around cybersecurity. The major thematic components of the Declaration were developing '[a] cyberspace that supports economic and social development and rights online ... [b]uild[ing] the foundations of an effective national cybersecurity response ... [and p]romot[ing] stability in cyberspace through international co-operation'.²

To address issues of cybersecurity, governments must:

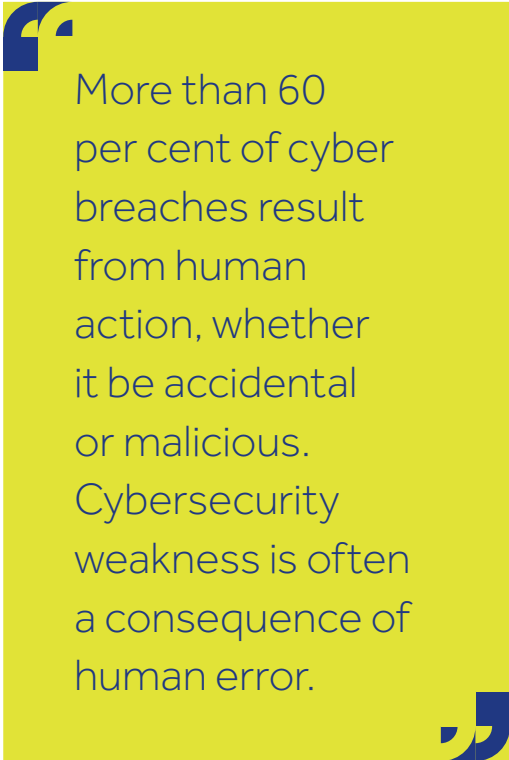
- improve the digital capacities of all government executives and professionals;

- invest in better cyber solutions;
- regulate to protect consumer and business data and assets, without unduly restricting access;
- adopt harmonised, interoperable, global standards; and
- extend the rights of citizens offline into their online experiences.

6.2 Context

More than 60 per cent of cyber breaches result from human action, whether it be accidental or malicious. Cybersecurity weakness is often a consequence of human error.

Numerous Commonwealth countries have experienced large-scale and significant cyber incidents in recent years, and the trend will accelerate as independent (criminal) cyber thieves and state-sponsored cyberterrorism and espionage become more sophisticated. Cyber attackers are taking advantage of advances in artificial intelligence (AI) and big data/big data analytics that rapidly outstrip the capabilities of national systems. Highly sophisticated personality profiling and even 'humint'



More than 60 per cent of cyber breaches result from human action, whether it be accidental or malicious. Cybersecurity weakness is often a consequence of human error.

(i.e., human intelligence) on key targets have increased the level of risk.

Efforts to mitigate cyber risk have at times done more harm than good. For example, fingerprint and facial recognition are biometric forms of data that are often perceived to be 'stronger' than others—and yet they introduce new risks. If someone steals our password, we can change that password; if someone steals our fingerprint file, we can do nothing to change our fingertips—and a hacker can use a 3D printer to recreate that print in minutes.

6.2.1 Device- and System-level Security

Some hackers take advantage of poor discipline in relation to updating operating systems or implementing firewalls. As low-cost internet devices proliferate, often with minimal or no cybersecurity, new vulnerabilities are entering the system.

(According to cyber expert Howard Shrobe of MIT, many devices still use old, unpatched versions of Linux software—meaning that hackers can exploit a series of well-known issues.) At the national level, some countries have failed to invest in upgrading computer systems within the financial services sector itself, which exposes core banking functions to serious risk and has resulted in attacks in which tens of millions of pounds are stolen in a matter of minutes.

6.2.2 Access Control

When we speak of 'access control', we are talking about controlling access by using aspects of identity. The three components of access control are validation, verification and authentication.

- **Validation** means making sure that the identity data given is real data, for example, that the National Insurance (NI) number given for an individual is not that of someone who is dead, or that an account number refers to a live account and not a closed account.
- **Verification** involves making sure that the information given is genuinely associated with a specific person, for example, that the date of birth and home address given actually belong to that person, or that the account they are trying to access is an account in that name or to which that person has legal access.
- **Authentication** is the process whereby we determine that a particular individual is who they claim to be.

All three of these components are required for a secure identity scheme. Traditional access control—the type of security we commonly use to access our accounts or computer systems—uses

elements such as a user name, a password and/or a personal identification number (PIN) code. In the modern world, if people were to use a different password for every account or system that they needed to access, they would typically need to remember 140–160 distinct passwords—and so the likelihood is that most individuals will reuse passwords, set weak passwords or in other ways compromise their online security.

6.3 Description

We can think through the elements of effective cybersecurity in terms of three key factors: systems, people and processes.

6.3.1 Systems

On a systems level, cybersecurity architects will examine the various components of a computer system and determine how each can be 'hardened' against breach or misuse. For example, some breaches have seen large companies such as Facebook storing passwords in plain text form. Encryption, which uses maths to make plain text or data unreadable, is one part of a robust cybersecurity scheme and central banks can, for example, require that the commercial, retail and institutional banks under their oversight follow industry best practices. This will include encrypting data at rest and data in flight, including passwords and PIN codes, and annual certification by third-party firms, such as EY (formerly Ernst & Young), Deloitte, Accenture, IBM, TCS or other consultancies.

Good cybersecurity hygiene will also include the following elements.

- **Vulnerability assessment** An inventory of the core financial system should be conducted on at least an

annual basis, to identify vulnerabilities and recommend remedies.

- **Monitoring and intrusion detection** Systems focused on both technology and processes must be put in place to trigger early alert of any cyber incident and swift response. For example, AI systems should be the first line of defence and they should begin to manage risk as soon as an incident is detected. This might involve throttling or controlling the pace of transactions, or requiring additional approvals before significant transactions or transaction patterns can be processed. At all times, day and night, a responsible individual must be on hand to make decisions during a cyber incident. More sophisticated systems can alert a bank employee if they are looking at types of data, or at patterns of data, that could be worthy of investigation.
- **Penetration testing** 'White hat' hackers should be engaged, ideally monthly, to test government and private sector systems. They should use both electronic tools and software, as well as 'social engineering', to identify weaknesses and suggest remedies.

6.3.2 People

Increased cybersecurity at a systems level must be partnered with efforts to raise levels of digital literacy among central bank officials, as well as banking professionals in the private sector. Cyber risk can be mitigated if professionals are more aware, better disciplined and change their behaviours when it comes to handling data. Given that human error is often at the root of breaches of cybersecurity, ongoing training is essential to instil good cyber hygiene across all institutions.

6.3.3 Processes

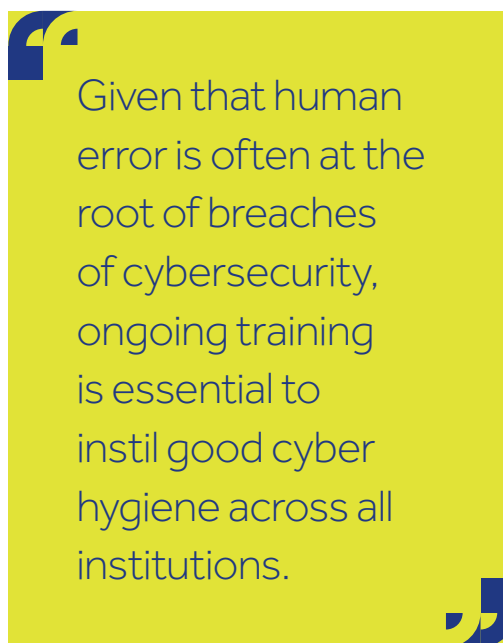
Tied to the culture shift needed among people is the design and implementation of better cyber processes that align behaviours with outcomes. This includes:

- identifying and eliminating redundant processes;
- regularly repeating activities to identify and remedy vulnerabilities;
- steps to identify and manage areas vulnerable to human error; and
- establishing formal mechanisms to identify new cyber threats and new cybersecurity technologies, and to rapidly respond to each.

6.4 Key Considerations for Future Development

Commonwealth countries need to invest significantly more in cybersecurity, given how vulnerable to attack the financial services sector is, not only within the Commonwealth but also globally. Cybersecurity is an area of technology in which we commonly underinvest, paying attention to it only after the fact of an incident. With financial services systems so highly interconnected, the risk that a breach in a country outside the Commonwealth would nonetheless impact on member countries is high.

We need approaches that are more sophisticated. Strong cybersecurity can unlock meaningful opportunities for countries, including financial inclusion and economic development, and it is inextricably linked with, for example, issues of digital identity. For example, verification and authentication are critical to both securing



systems and facilitating financial inclusion via identity inclusion.

One barrier to the broader implementation of improved cybersecurity is the absence of standards in a number of mission-critical areas. A consultative, multistakeholder process will help us to shape, implement and uphold such standards.

Likewise, given that more than 60 per cent of cybersecurity breaches result from human error or action, investing in digital literacy will help consumers and institutions, both private and public, to mitigate the risks.

Endnotes

- 1 The Commonwealth (2018). *Commonwealth Cyber Declaration*. Retrieved from <https://thecommonwealth.org/commonwealth-cyber-declaration>
- 2 *Ibid.*



PART 2

Application and Action

People do not invest in technologies; they invest in solutions to their problems. Understanding the technologies is an important first step, but understanding how we can use those technologies to support development is how we complete the journey.

Having explored six of the key technologies that shape fintech in Part I, this Toolkit looks in Part 2 at how countries can use those technologies to achieve development goals.

- Chapter 7 explores how disruptive technologies such as artificial intelligence (AI) and/or digital financial

services can help to promote development outcomes.

- Chapter 8 highlights the nuanced considerations to which countries must pay attention depending on their size and/or region.
- Chapter 9 outlines an action framework for governments seeking to create an enabling environment for fintech and fintech applications.
- Chapter 10 highlights case studies from four countries of fintech initiatives successfully applied to tackle development challenges.

Chapter 7

Policy Interventions and Outcomes



Policy Interventions and Outcomes

Key points

- **Financial inclusion** is a result of and also can result in:
 - stronger consumer protection;
 - lowered costs of complying with anti-money-laundering (AML) and know your customer (KYC) rules;
 - increased levels of financial and data literacy;
 - inclusion of those with historically marginalised identities; and
 - lower rates of identity theft.
- **Improved cross-border transactions and trade** both result from and result in:
 - lowered costs of remittances;
 - lowered costs of AML/KYC compliance; and
 - more robust cybersecurity.
- **Improved economic growth** will not only result from and in quicker transactions, but also facilitate the financial support of small and medium-sized enterprises (SMEs).

7.1 Introduction

In taking steps to create an enabling environment for fintech, governments can take strides towards commonly key policy interventions and outcomes.

This chapter will look at how disruptive technologies such as artificial intelligence (AI) and/or digital financial services (DFS) can help to promote three specific policy areas as examples. In this way, this Toolkit aims to equip countries with the principles that will allow them to use fintech to tackle a broader range of development goals.

In this chapter, we therefore look at **financial inclusion** and its capacity to result in:

- stronger consumer protection;
- lowered costs of complying with anti-money-laundering (AML) and know your customer (KYC) rules;
- increased levels of financial and data literacy;
- inclusion of those with historically marginalised identities; and
- lower rates of identity theft.

We look at improvements that can be delivered in **cross-border transactions and trade**, resulting in:

- lowered costs of remittances;
- lowered costs of AML/KYC compliance; and
- more robust cybersecurity.

Finally, we consider the **economic growth** that can result from and in quicker transactions, while also facilitating the financial support of small and medium-sized enterprises (SMEs).

7.2 Financial Inclusion

Financial inclusion¹ is one of the key tools with which governments can reduce poverty and bolster prosperity.² Despite this fact, approximately 1.7 billion adults globally remain unbanked—that is, without access to an account at any financial institution or to mobile banking services. In developing economies, in particular, few people and small businesses fully participate in the formal financial system. Instead, they transact exclusively in cash, have no safe way of saving or investing money, and cannot access credit other than through informal lenders and personal networks. Even those with financial accounts may have only limited product choice and face high fees. As a result, a significant amount of wealth is stored outside the financial system, and credit is scarce and expensive. This prevents individuals from engaging in economic activities that could transform their lives, which impacts negatively on economic growth.³

The rapid digitalisation of services, along with the rapid spread of digital technologies, offers institutions the opportunity to provide financial services at much lower cost, which has the potential to result in financial inclusion and large productivity gains across the economy. In 2016, consulting firm McKinsey & Co. positioned fintech as one of the key tools with which we can drive local economic

development and reduce poverty⁴—one of the United Nations Sustainable Development Goals (SDGs).⁵ Among other global voices, the World Bank, the G20, the US Agency for International Development (USAID), the Bill & Melinda Gates Foundation, Citibank and MasterCard have all equally advocated for the potential of fintech to facilitate financial inclusion.⁶

7.2.1 Key Policy Interventions

Research findings confirm that growing access to financial instruments has a positive impact on self-employment, business activities and household consumption, among other things.⁷

There are several successful examples of government-level policies and programmes established to increase financial inclusion. In 2007, the M-Pesa programme—a phone-based money transfer programme—launched in Kenya (see Case Study 10.2). In 2006, Kenyan stakeholders had launched FinAccess: a national household survey programme dedicated to improving financial access in the country, which has been updated several times since then. The initiatives have contributed to a significant rise from 26.3 per cent to 83 per cent in formal financial inclusion,⁸ and by 2019, 24.5 million Kenyans were using M-Pesa.⁹

Another example is found in India, where the Government of India and the Reserve Bank of India have positioned the National Mission for Financial Inclusion (Pradhan Mantri Jan Dhan Yojana, or PMJDY) as one of their most important objectives. Measures have included:

- all banks opening basic saving bank deposit (BSBD) accounts with minimum common facilities, such as no minimum balance, the ability to deposit and withdraw cash at bank branches and

by card through an automatic teller machine (ATM), and the ability to receive or send money through electronic payment channels;

- relaxed and simplified know your customer (KYC) rules to make opening bank accounts easier for individuals whom traditional identity requirements might otherwise exclude (see Chapter 4 on digital identity); and
- a simplified branch authorisation policy, to address the uneven spread of bank branches across the country, and a compulsory requirement to open branches in unbanked villages.

When the programme launched in India, financial inclusion was at 53 per cent, but this figure has since soared to 80 per cent.¹⁰

Ironically, those developing economies in which large population segments are unserved or underserved by traditional financial services represent opportunity for fintech such as blockchain. Shallow banking infrastructure in developing economies lessens the 'technology debt' involved when legacy infrastructure has to be replaced, and it can mean that there is less social and institutional resistance to the new technology. In addition, while blockchain may be a disruptive technology in established markets, regulators and providers in emerging financial services markets are less likely to resist blockchain-based new entrants, who will not significantly disrupt existing market conditions.¹¹

In 2015, Accenture said that, with a scalable proof of concept for a viable mobile banking business model, blockchain could advance financial inclusion by serving previously unprofitable customers and SMEs to generate US\$380 billion in additional revenues.¹² Digital

finance has the potential to reach more than 1.6 billion new retail customers in developing economies and to increase the volume of loans extended to individuals and businesses by US\$2.1 trillion.¹³

Because digital payments allow people to transact in small amounts, known as micropayments, they create new opportunities based on pay-per-service, or pay-as-you-go, models. Businesses such as low-cost private school Bridge International Academies in Kenya, Uganda, Nigeria and India rely on technology enabling them to receive school fees and pay teacher salaries digitally as part of their cost-efficient business models.¹⁴ Digital payments also facilitate new business models such as e-commerce and the gig economy, with new ride-sharing and employment-matching service providers among them.¹⁵

Atlas is a start-up with teams in Ghana and Senegal that provides a mobile peer-to-peer (P2P) application, Access Network, aiming to give to communities in the developing world access to savings and credit through a decentralised solution that lets the unbanked 'bank with each other'.¹⁶ The app creates a network of people from local communities, which cultivates trust while building financial inclusion. In addition, the Atlas platform offers access to capital through savings accounts and loans. The blockchain underpinning the platform evidences proof of origin for the money and all transactions, ensuring that users know exactly where their money is and can see the latest transactions on their accounts.¹⁷

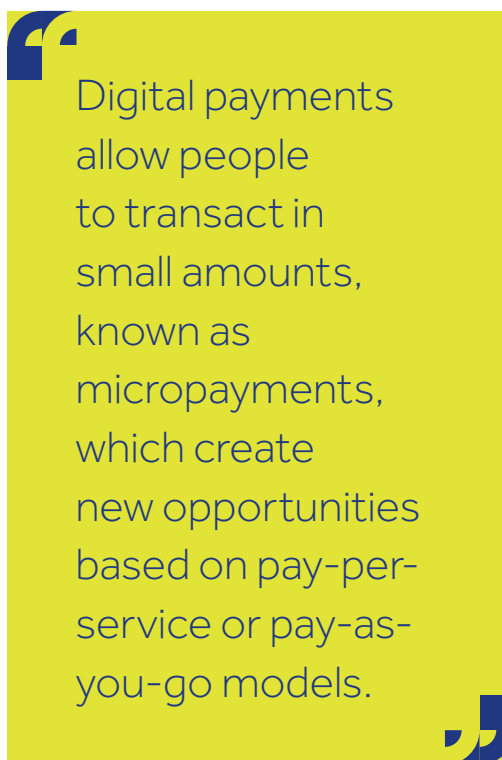
Indeed, lending more broadly is an area in which blockchain applications can open up opportunity by allowing lenders to verify a person's financial or personal history digitally and to assess whether they are looking to

finance a viable business or other prospect, eliminating much of the traditional process of securing credit.¹⁸

The merits and the scale of the opportunity that mobile finance represents are clear. Research by McKinsey & Co. indicates that the success of mobile money providers in emerging markets is predicated on preparation for the long term, adopting new methods of collaborative working—including with regulators—and investing to support scale until the benefits of network effects begin to show.¹⁹ Kenya's Capital Markets Authority has also proposed that it joins with the Central Bank of Kenya (CBK) to create a special unit that will monitor and facilitate a path for the adoption of digital currencies.²⁰

In 2018, the Asia-Pacific Economic Cooperation (APEC) recommended a series of policy initiatives, aiming to promote financial inclusion. Its first recommendation was that central banks should prioritise structural and regulatory reforms towards:

- Aiding the poor to accumulate productive assets and build greater long-term wealth and financial security.
- Enabling the poor to participate in the formal economy as represented by employment, wage growth, health insurance and pension schemes.
- Promoting investment in the NMSE [nano and micro sector enterprise] sector and providing pathways for informal enterprises to become formalised.
- Increasing the ability of women and other vulnerable populations to participate in economic activity in safe and effective ways.²¹



Digital payments allow people to transact in small amounts, known as micropayments, which create new opportunities based on pay-per-service or pay-as-you-go models.

The second recommendation was that reforms should include developing and supplying a broader range of products and services, towards:

- Promoting financial education, and its role in developing financial health, among the underserved to increase pull from the demand side and creating incentives, or a more enabling regulatory environment, to encourage greater private sector investment into the supply of a broader range of products.
- Targeting the ability for financial institutions to develop and test innovative solutions involving new technology, which could assist them to diversify their product offerings.
- Regulators need to consider methods and policies, which can be introduced to help encourage the creation and use

of savings products that allow people to build assets and resilience. The lack of disposable incomes makes it difficult for the poor to absorb shocks, which often makes them more reliant on credit and susceptible to over indebtedness. Products which mix long-term saving with the ability to access in the event of emergencies can be particularly effective in helping the poor develop assets.

- Remittances (both domestic and international) have the potential to be a major driver of inclusive growth. By combining remittance services with other complementary services such as savings, insurance or payments, migrants and their families can increase their opportunities to accumulate assets and build wealth. Governments need to understand this potential and ensure that regulatory frameworks are conducive towards enabling the underserved to access a broader range of products and services through remittance channels.²²

Setting out these recommendations in 2019, the Foundation for Development Cooperation (FDC) goes on to note that gender issues are not often considered in national financial inclusion strategies. It recommends as a third point that a 'gender lens' should be applied across all components of financial inclusion strategies. This might involve:

- Including plans to collect and analyse sex-disaggregated data to inform and improve development policies.
- Ensuring that development strategies are truly inclusive of women by engaging with them as part of the design stage and continually

throughout implementation—it is important that this engagement is not added on later during implementation (i.e. as an afterthought) but is treated as a core component of the overall strategy from the design phase.

- Identifying and prioritising reforms, which reduce inequalities and support the ability of women to actively and meaningfully engage in economic activity. This should include considerations for technology and infrastructure, which has the potential to enhance women's access to essential services such as financial services, health care or education.²³

Governments can promote the rights and entitlements of women in this context by:

- Reviewing legal frameworks, infrastructure and economic structures to identify factors which may be creating inequalities and limiting women's access to economic opportunity. ...
- Identifying cultural elements which deepen inequalities and work[ing] with the private and civil society sectors to promote attitude changes through media campaigns and community-based interventions. Working with the private sector to leverage the influence of businesses on consumers is particularly important.
- Promoting financial literacy and education to increase levels of financial health among women and enhance their economic empowerment.²⁴

The FDC introduces into discussion the idea of the regulatory sandbox: a

regulator-controlled environment in which fintech and other innovative start-ups can test their ideas under market conditions. Regulatory sandboxes are an effective way in which governments can keep pace with innovation and ensure that their regulatory frameworks are effective, while limiting their risk exposure.

By applying the concept to cross-border issues such as trade or remittances, multi-economy regulatory sandboxes can be an effective way in which governments can co-operate on technology solutions. One government can also potentially leverage another's infrastructure to help to focus development of its own.

In its seventh recommendation, the FDC sets out some examples of areas in which governments could focus efforts to realise the benefits of technology for inclusive development, including:

- Developing and testing digital finance, or Fintech, solutions which enable the underserved to access to a broader range of digitally enabled products/ services (i.e. insurance, pensions, savings, remittances, payments, etc). The creation of regulatory sandboxes is an important method of testing and developing such innovations with the involvement of a broad range of stakeholders.
- Social transfers represent one of the most important opportunities for digital financial services, including payments and ID systems, to directly impact the lives of the poor. In many cases, social transfers are the only way to reach the poorest of the poor (lower 30%) and provide them with access to formal financial systems. By digitising social transfer accounts governments can

create an effective entry point for the poorest to gain access to other beneficial digital financial services.

- Regulation which allows for the creation of digital identification systems that are secure and reliable can have a significant impact on the lives of the underserved. ...²⁵

Focusing next on the informal economy, the FDC notes that governments often respond to the issue as being about social welfare rather than economic opportunity. Yet significantly, more people are employed within the informal economy than the formal economy; by officially recognising it—with initiatives that address the needs of stakeholders such as NMSEs—governments can realise those opportunities.

This will involve formulating policy frameworks that address the critical challenges facing such stakeholders, including:

- Lack of credit history or formal identification, which limits access to formal financial services—A potential solution may include the use of unstructured data to make credit decisions.
- Lack of customised financial products and services which meet the unique needs of the informal sector—Attempts to serve the NMSE markets often incorrectly assume that products and services designed for formal enterprises will also address the needs of informal enterprises. Products and services designed for the informal economy also need to have a particular focus on women who make up the majority of nano and micro entrepreneurs.

- The need for access to non-financial services such as micro-medical insurance, school fee savings products, financial literacy or vocational training—Access to finance should be complimented [sic] with access to appropriate non-financial services to help translate financial inclusion into economic opportunity.
- The need for more diverse financing resources for smallholders—Examples may include specialised community-owned finance companies or co-operatives which can provide financing services to those unable to access credit from commercial banks.²⁶

Finally, we look here at the ninth recommendation, which advocates for policies that facilitate cross-border trade. For example, NMSEs might be allowed to settle cross-border payments in local currency, as is the case in Thailand, thereby dismantling a major barrier for many NMSEs across the region. By relaxing regulations, governments can increase the opportunities for these enterprises.²⁷

7.2.2 Key Policy Outcomes

Key policy outcomes for Commonwealth governments include:

- stronger consumer protection;
- lowered costs of complying with AML/KYC rules;
- increased levels of financial and data literacy;
- inclusion of those with historically marginalised identities; and
- lower rates of identity theft.

Stronger Consumer Protection

Consumer protection remains front and centre when looking at fintech. On the one hand, AI audit tools can help a regulator to determine that a particular institution's lending practices are legally compliant; on the other hand, loan decision engines driven by machine learning might begin to exclude in practice the very disadvantaged individuals whom government is seeking to include in theory.

Regulatory perimeter is another issue that arises in relation to fintech and consumer protection. Some digital financial services are delivered by providers or channels that may fall beyond the reach of the conventional regulator, for example, a mobile communications company or an app on a smartphone. It is consequently essential, as new technologies and other innovations emerge to engage new customers, that governments regularly evaluate the scope and focus of their regulatory agencies.

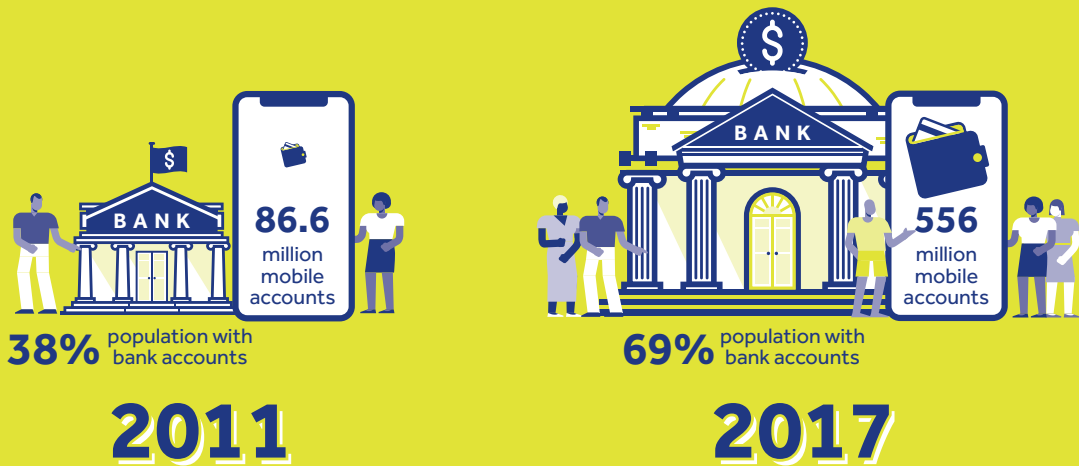
Lowered Costs of Complying with AML/KYC Rules

Current AML systems tend to have an error rate of 85–95 per cent false positives (meaning that they incorrectly flag activity as suspicious), demanding manual reconciliation efforts on a massive scale. One 'top ten' global bank has dedicated more than 4,000 highly paid professionals to cleaning up false positives.²⁸

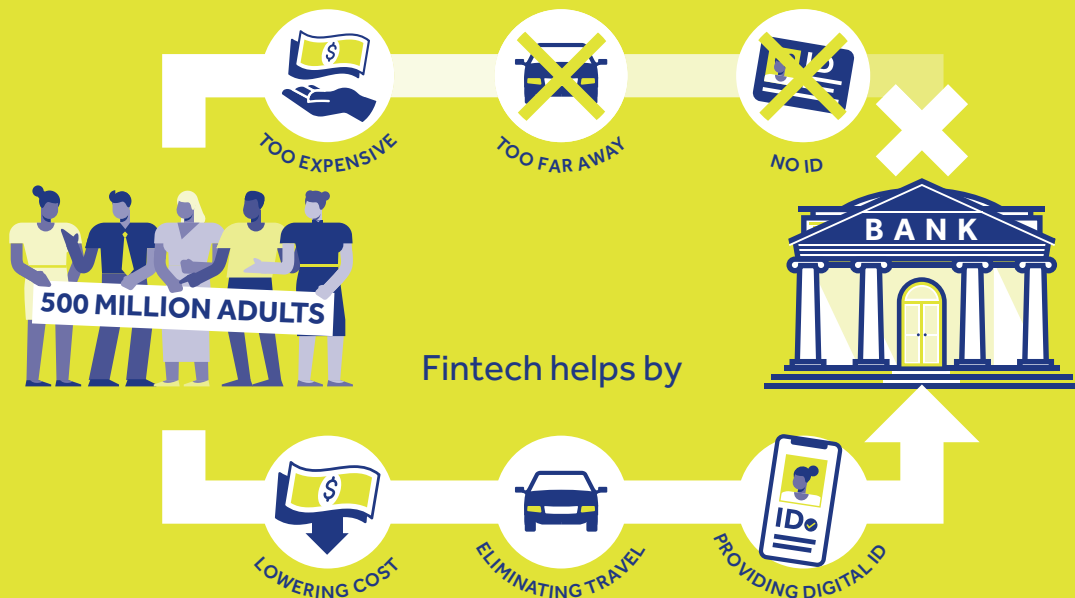
Complying with KYC rules can be equally labour-intensive. Policy-makers in regions in which the unbanked dominate should adopt strategies such as correspondent banking, savings groups, mobile branches and extending the reach of bank branches to the doorstep of the ordinary citizen. Another tool with which governments might ease the burden is a nationwide digital identity system such as Aadhaar in India (see Chapter 4).

FINTECH AND FINANCIAL INCLUSION

The number of people with bank accounts across the Commonwealth has increased.



However, 500 million Commonwealth adults still do not have bank accounts



Increased Levels of Financial and Data Literacy

As potential consumers begin to access new products and services, their financial literacy will begin to improve, and policy initiatives aiming to accelerate that improvement will see take-up escalate. Likewise, efforts to develop consumers' data literacy can help them to recognise their rights and appreciate the benefits of government interventions such as data privacy regulations or open banking legislation.

Inclusion of Those with Historically Marginalised Identities/Lower Rates of Identity Theft

Among those rights is the right to a legal identity—a prerequisite to financial inclusion. Yet many millions of people worldwide—most commonly women and children—remain unable to document their identities and hence may be denied access to government services, financial services and health care.

Coupling blockchain with biometrics offers us an alternative. The independent computers that run on a blockchain's decentralised network can update and maintain an ever-growing public ledger of transactions. They repeatedly reach a consensus on changes and thus are constantly vouching for the ledger's integrity. Information on new transactions is built on top of all preceding records in a precise, time-stamped, interlinked manner, which means that anyone who tampers with past data will distort all later records and so expose their fraud. It is this permanence and incorruptibility, combined with the fact that it is completely open and uncontrolled, that makes blockchain so valuable to governments and so attractive to citizens, offering opportunity to transform identity digitally and to lower rates of identity theft.

By establishing a secure, reliable national identity system of unique identifiers and

empowering citizens to control their own records, governments can establish the foundations for many areas of digital innovation and fast-track financial inclusion goals. The underserved can set up bank accounts, start businesses and move money. Banks and microfinance providers can lend with more confidence and, in time, they may come to provide more sophisticated financial products such as insurance and investment services. The correlation of digital identity with digital tax systems will increase government revenue, while governments will be able to distribute aid and services more efficiently and more fairly.

7.3 Improved Cross-border Transactions and Trade

Disruptive technologies hold significant promise for improving cross-border transactions and trade, by reducing friction and unlocking trapped capital, resulting in:

- lowered costs of remittances;
- lowered costs of AML/KYC compliance; and
- more robust cybersecurity.

7.3.1 Lowered Costs of Remittances

Cross-border transactions and trade have been reliant on antiquated systems and interfaces. From both costs and cybersecurity standpoints, this has generated a number of risks and issues. Fintechs have aggressively pursued the remittance market, going after fees that, in developing economies, can reach 15 per cent, and exponential reductions in cost and improvements to speed and service. Digital financial services was instrumental in the first wave of such companies, while blockchain resulted in a second wave of remittance innovators.

Trade finance also enjoys significant time and cost advantages when better data systems and blockchain are implemented. Many of the world's trade corridors rely on manual, paper-based processes, from the transfer of ship manifests and bills of lading from ship captain to port office, to the management of letters of credit for goods in transit on a container ship. This is doubly true of commodities: more than 60 per cent of the costs of commodities result from middle- and back-office functions (primarily paperwork); commodities giant Louis Dreyfus was able to use blockchain to decrease transaction time by 80 per cent.²⁹ Such systems can put more money into the hands of suppliers such as farmers faster, and AI-enabled analytics of demand forecasting and weather forecasting can better manage volatility and risk.

In these contexts, the regulator's challenge is in ensuring equitable access to data and analytics, such that smaller or newer entrants to a market are not disadvantaged, and embedding compliance into new systems, such that the risk of fraud and abuse is mitigated.

7.3.2 Lowered Costs of AML/KYC Compliance

In the realm of cross-border trade and transactions, AML/KYC is a significant pain point. If central banks can eliminate duplication of effort by encouraging federated identity registries within their jurisdictions, they may see a resulting reduction in cost. Longer-term and more ambitious efforts would see the creation of supranational government-sponsored identity registries to help to lower AML compliance costs. Multinational bodies such as the African Union and Organisation for Economic Co-operation and Development (OECD) have already undertaken exploratory work in this area;

the Commonwealth itself would be a logical sponsor of such efforts.

7.3.3 More Robust Cybersecurity

Cybersecurity issues commonly arise in domain spaces within the financial ecosystem. Attacks on government systems have resulted in the theft of tens of millions of dollars, which have been rapidly transferred and hidden throughout the global financial services infrastructure.³⁰ Other issues connected with regulating for cybersecurity mean that it can be difficult to navigate correspondent banking or to penetrate cross-border remittances markets.

Among the tools that can help to reduce friction and costs are policy interventions aiming to:

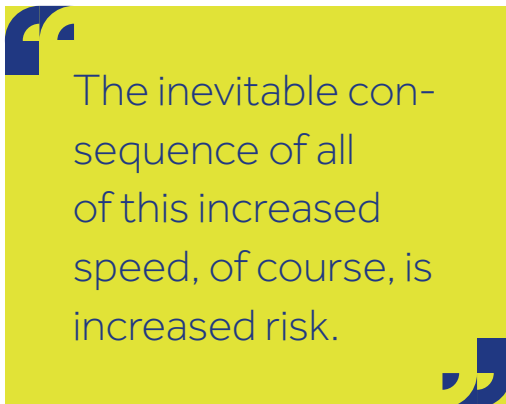
- raise digital literacy and awareness of cyber crime among regulators and policy-makers;
- harmonise and elevate cybersecurity requirements across financial services and systems providers and central banks; and
- digitally identify known 'bad actors' and share that information across borders.

7.4 Improved Economic Growth

A proactive regulatory stance can facilitate economic growth within a given country or region. Growth fuelled by fintech can result from and in quicker transactions, while also facilitating the financial support of SMEs.

7.4.1 Transaction Speed and Cost

Transaction speed and cost are rate-limiting factors of economic development. High-speed transactions reduce financing costs and improve the turnover of money through an



economic system, accelerating working capital cycles and offering opportunities for greater economic value added. Digital currencies and blockchain have the potential to speed up transactions exponentially—particularly for P2P payments—but they also may be more opaque than other kinds of digital transactions.

The inevitable consequence of all of this increased speed, of course, is increased risk. Fraud or cybercrime can now occur more quickly than law enforcement and other authorities can react, with tens or hundreds of millions of pounds moving in minutes—or even seconds—while investigations after the fact can take weeks, months or even years.

7.4.2 Financial Support for Small and Medium-sized Enterprises

For our purposes, we can segment SMEs as:

- sole proprietors;
- micro businesses (2–20 employees);
- small businesses (21–100 employees); and
- medium-sized businesses (101–1,000 employees).

These businesses are conventionally underserved by traditional financial

services. More than 95 per cent of the world's small businesses are underbanked or unbanked—a figure that is troubling. It is all the more so when partnered with the fact that small businesses create four out of five new jobs—jobs badly needed in Africa and Asia, where 600 million new jobs need to be created in little more than a decade to stave off poverty and improve people's lives.³¹

While SME finance is one of the most wide-reaching mechanisms with the most far-reaching potential to drive societal change and economic growth, there are barriers to its success. Credit underwriting and analysis of small businesses is challenging, for example, with few alternative data sources and poor-quality credit modelling. Among questions remaining are the following:

- How can we ensure equal access?
- How can we manage risk across a portfolio of small business loans?
- What securitisation opportunities exist to free up more liquidity to expand the loan book more rapidly while limiting risk exposure?
- How do we determine the ultimate beneficial owner (UBO) of any SME or in any given transaction and ensure that we comply with AML/KYC rules? (With even fewer reliable methodologies to ensure data quality, the identity challenges described elsewhere in this Toolkit are compounded in relation to SMEs.)

Central banks should therefore be encouraging further investment and experimentation, while regulators and policy-makers can address SME finance in

collaboration with private industry through a variety of mechanisms, from offering attractive rates through the discount window to sandboxing new lending models.

Endnotes

- 1 Much of the content of this section on financial inclusion was first published in Thomason J, Bernhardt S, Kansara T, Cooper N (2019). *Blockchain Technology for Global Social Change* (Hershey, PA: IGI Global) and is reprinted with permission. See: www.igi-global.com/book/blockchain-technology-global-social-change/221876#table-of-contents
- 2 Demirgüç-Kunt A, Klapper L, Singer D, Ansar S, Hess J (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf>
- 3 *Ibid.*
- 4 McKinsey & Co. (2016). *Digital Finance for All: Powering Inclusive Growth in Emerging Economies* [online]. Retrieved from: www.mckinsey.com/-/media/McKinsey/Featured%20Insights/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx
- 5 UN General Assembly (2015). *Transforming Our World: The 2030 Agenda for Sustainable Development*. A/RES/70/1, 21 October [online]. Retrieved from: www.refworld.org/docid/57b6e3e44.html
- 6 Häring N (2017). 'Modi, Yunus and the Financial Inclusion Mafia'. *Money and More*, 26 March [online]. Retrieved from: <https://norberthaering.de/en/war-on-cash/modi-yunus/>
- 7 Bauchet J, Marshall C, Starita L, Thomas J, Yalouris A (2011). *Latest Findings from Randomized Evaluations of Microfinance* [online]. Retrieved from: www.cgap.org/sites/default/files/CGAP-Forum-Latest-Findings-from-Randomized-Evaluations-of-Microfinance-Dec-2011.pdf
- 8 Central Bank of Kenya, Kenya National Bureau of Statistics, FSD Kenya (2019). *Inclusive Finance? Headline Findings from FinAccess 2019* [online]. Retrieved from: <https://s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2019/07/24171523/19-07-26-FinAccessPolicy-Document-Web.pdf>
- 9 Bright J (2020). 'Visa and Kenya's Safaricom partner on M-Pesa, payments and tech'. *Techcrunch*, 30 April [online]. Retrieved from: <https://techcrunch.com/2020/04/30/visa-and-kenyas-safaricom-partner-on-m-pesa-payments-and-tech/>
- 10 Demirgüç-Kunt A, Klapper L, Singer D, Ansar S, Hess J (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf>
- 11 International Finance Corporation (2019). *Blockchain: Opportunities for Private Enterprises in Emerging Markets* [online]. Retrieved from: www.ifc.org/wps/wcm/connect/2106d1c6-5361-41cd-86c2-f7d16c510e9f/201901-IFC-EMCompass-Blockchain-Report.pdf?MOD=AJPERES&CVID=mxYj-sA
- 12 Accenture, CARE International (2015). *Within Reach: How Banks in Emerging Economies Can Grow Profitably by Being More Inclusive* [online]. Retrieved from: www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_23/accenture-banking-withinreach.pdf#zoom=50
- 13 McKinsey & Co. (2016). *Digital Finance for All: Powering Inclusive Growth in Emerging Economies* [online]. Retrieved from: www.mckinsey.com/-/media/McKinsey/Featured%20Insights/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx
- 14 Bridge (undated). 'What We Do: Tech' [online]. Retrieved from: www.bridgeinternationalacademies.com/

- 15 Osafo-Kwaako P, Singer M, White O, Zouaoui Y (2018). *Mobile Money in Emerging Markets: The Case for Financial Inclusion* [online]. Retrieved from: www.mckinsey.com/industries/financial-services/our-insights/mobile-money-in-emerging-markets-the-business-case-for-financial-inclusion
- 16 Costa M (2016). 'Economies shared'. *Medium*, 20 June [online]. Retrieved from: <https://medium.com/atlas-together/economies-shared-4e14a6e93d0f>
- 17 Atlas (2018). *About* [online]. Retrieved from: <https://atlas.money/about>
- 18 Knowledge@Wharton (2018). 'How the Blockchain Brings Social Benefits to Emerging Economies', 28 November [online]. Retrieved from: <https://knowledge.wharton.upenn.edu/article/blockchain-brings-social-benefits-emerging-economies/>
- 19 Osafo-Kwaako P, Singer M, White O, Zouaoui Y (2018). *Mobile Money in Emerging Markets: The Case for Financial Inclusion* [online]. Retrieved from: www.mckinsey.com/industries/financial-services/our-insights/mobile-money-in-emerging-markets-the-business-case-for-financial-inclusion
- 20 Pande S, Medikepura Anil A [2018]. 'South Asia Can Become an Innovation Hub: Here's How'. *Qrius.com*, 20 November [online]. Retrieved from: <https://qrius.com/south-asia-can-become-an-innovation-hub-heres-how/>
- 21 Foundation for Development Cooperation (2019). *The Inclusion Imperative: A Call to Action* [online]. Retrieved from: www.ada-microfinance.org/download/5530/fdc-the-inclusion-imperative-a-call-to-action.pdf
- 22 *Ibid.*
- 23 *Ibid.*
- 24 *Ibid.*
- 25 *Ibid.*
- 26 *Ibid.*
- 27 *Ibid.*
- 28 ING (2018). 'Know Your Customer and Anti Money Laundering Measures at ING'. Press release, 4 September [online]. Retrieved from: www.ing.com/About-us/Compliance/KYC-and-anti-money-laundering-measures.htm
- 29 Hoffman A, Munsterman R (2018). 'Dreyfus Teams with Banks for First Agriculture Blockchain Trade'. *Bloomberg*, 22 January [online]. Retrieved from: www.bloomberg.com/news/articles/2018-01-22/dreyfus-teams-with-banks-for-first-agriculture-blockchain-trade
- 30 See, e.g., Al Jazeera (2018). 'Hacked: The Bangladesh Bank Heist'. 24 May [online]. Retrieved from: www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html
- 31 Van Trotsenburg A (2018). 'More and Better Jobs for Developing Nations'. World Bank, 11 May [online]. Retrieved from: www.worldbank.org/en/news/opinion/2018/05/11/more-and-better-jobs-for-developing-nations

Chapter 8

Considerations



Considerations

Key points

- Commonwealth member countries are diverse in terms of population size.
- **Small states** benefit from agility in that they are able to make decisions swiftly and hence several Commonwealth countries have already embraced fintech. While smaller developing economies have historically been limited by resource constraints, a new paradigm suggests that population size may not be a constraint to digital transformation—as evidenced by the actions of countries including Bermuda, Dubai and Mauritius. Imagination, agility and aspiration all may allow small states to leapfrog others and become leaders in a new digital economic order.
- Larger and wealthier countries may benefit from more resources and/or larger populations across which to amortise the costs of investment in new technologies, but larger nations are typically slower to make decisions and to implement solutions. Indeed, wealthier nations are more likely to have ‘legacy’ systems—that is, older technology that will need to be upgraded or replaced if the nation is to take advantage of fintech.
- In addition, the needs of countries that neighbour one another may be shared, while they may differ from the needs of countries in other regions.

8.1 Introduction

In any effort to develop policy interventions for Commonwealth nations, it is necessary to evaluate their diverse needs. While there are small nations with abundant resources (e.g., Singapore) and there are larger countries that are yet developing economically (e.g., Nigeria), it is generally helpful to understand the constraints and opportunities offered by countries segmented by size. Indeed, among Commonwealth states, island nations have been particularly progressive in experimenting with and adopting fintech and fintech-related policies, and this may be because of their small size, whereby a handful of decision-makers can rapidly reach consensus.

8.2 Diversity among Commonwealth Nations

The Commonwealth countries have a combined population of 2.4 billion—almost

a third of the world's people. Population sizes are diverse within the Commonwealth, however, ranging from India at more than 1 billion, Pakistan, Nigeria and Bangladesh with more than 100 million, 33 countries with fewer than 10 million and 26 at fewer than 1 million. Economic development is also uneven in Commonwealth economies, with financial inclusion remaining a major problem in many countries.

Developed economies in the Commonwealth feature large, well-established, traditional enterprises filling business and consumer needs in markets with sound infrastructure and well-developed regulatory regimes. In Commonwealth emerging markets, by contrast, growth is often fast, but needs may be unmet, infrastructure poor and compliance patchy—to the benefit of innovation enabled by digital technologies. Characterised by a lack of legacy systems, emerging markets are more likely to embrace

new technologies. In emerging markets, digital technologies enable entrepreneurial businesses to overcome long-standing barriers and reach new potential customers. Fintech and the digital economy can enable small businesses, women and other disadvantaged groups to take part in trade and connect around the world. For some Commonwealth economies, then, disruptive change may deliver a unique opportunity to 'leapfrog' the legacy issues that advanced economies confront—and the rewards can be transformative.

8.3 Small States: Opportunity and Challenge

Thirty-three of the Commonwealth member countries have populations of fewer than 10 million and have traditionally been hampered economically by size, talent and geography. Digital technologies provide these small states with a transformative opportunity.

Artificial intelligence (AI) and blockchain allow small states to overcome the barriers of distance, talent and isolation. They are more agile and can be more responsive; they are often less inhibited by legacy systems and, in many, the pressure to meet people's needs is more acute. While larger states are still debating the promise of new technologies, many smaller jurisdictions are already embracing them.

Small states are moving quickly:

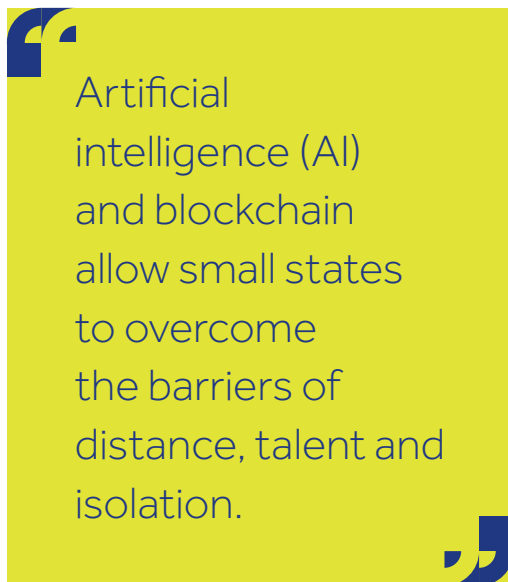
- Bermuda announced its new regulations on initial coin offerings (ICOs) on 13 July 2018, describing minimum required information for ICO projects and establishing compliance measures for companies to conduct an ICO;
- Jersey's Financial Services Commission launched Jersey's ICO guidelines on 12 July 2018;

- Estonia has already established itself as a world leader in digitisation;
- Switzerland and Singapore are early adopters and leaders in blockchain;
- Dubai is implementing a mandate for government services to go paperless on blockchain;
- in February 2018, the Government of Gibraltar announced its intention to proceed with token regulation;
- on 4 July 2018, the Maltese Parliament officially passed three bills into law—reportedly, the first regulatory framework for blockchain, cryptocurrency and distributed ledger technology (DLT); and
- the East African island nation of Mauritius is seeking to brand itself as a regional haven for blockchain innovation.

While not a comprehensive list, this clearly points towards a new paradigm whereby small populations are not a constraining factor for digital transformation; rather, imagination, agility and aspiration may enable small states to leapfrog others and take the lead in a new digital economic order.

Small states will nonetheless also face a number of challenges—notably, costs and access to talent—and may need to collaborate with other countries to access the resources and capital that they require. Regional collaboration can help countries to address regulation and standards, examine the regulatory fitness of legislation for a digital economy, and support the sharing of best practices in areas such as change management.

To build capacity, regional platforms could support the sharing of experiences,



trigger collaboration and joint investments with relevant partners, explore common approaches to regulatory problems, and facilitate workforce reskilling and recruitment to allow small states to meet the needs of the digital age.

8.4 Advanced Economies and Legacy Systems

There is evidence that integrating digital technology into the design and delivery of public services yields efficiency and productivity gains for both government and industry, increasing public value and driving broad public sector modernisation, as well as promoting greater openness, transparency, public engagement and trust in government.¹ In 2016, the UK government estimated that introducing digital tools into government service delivery could save between £1.3 billion and £2 billion annually as quickly as by 2020.² Similarly, in a 2015 report commissioned by Adobe, Deloitte found that the cost savings for the Australian government of digitising consumer transactions could be as much as AU\$17.9 billion per annum by 2025.³ Despite this evidence, many advanced economies are

moving slowly to implement new technology systems because changing legacy systems at the institutional and structural levels is a massive undertaking that can take years—or even decades.

8.5 Developing Economies

In developing economies,⁴ the lack of trusted and effective infrastructure means that new technologies are a welcome arrival: they do not demand change to the status quo, but signal the arrival of a functional resolution to a long-standing problem. Developing economies are almost exclusively cash-based: nearly 90 per cent of economic activity is conducted traditionally, because trust in local financial institutions is poor, and because an average of 40 per cent of people do not have bank accounts.⁵ Few people and small businesses in developing economies fully participate in the formal financial system; some 2 billion individuals and 200 million small businesses lack access to formal savings and credit.⁶ Thus emerging markets are constantly innovating in the field of payments, promoting an increasing shift to digital services.⁷ The lack of trust in local financial institutions means, however, that preference for cash prevails and indeed continues to increase.

By 2016, the amount of cash in circulation had increased to 9 per cent of gross domestic product (GDP) compared with 7 per cent in 2000, yet digital payments were expected to reach a record 726 billion by 2020, with emerging markets leading this trend at a rate three times that of developed economies.⁸ Digital payments in developing markets were expected to have a compound annual growth rate of 23.5 per cent between 2017 and 2022, compared to an expected 7.1 per cent rise in mature markets over the same time period.⁹ In 2017, non-cash payments in Asian emerging markets were projected to grow by almost a third

(30.9 per cent) over the coming decade, led by China and India.¹⁰ Accordingly, there is likely to be rapid change in the payments landscape, building on accelerating growth in electronic payments and the advent of new and disruptive markets.

Developing economies will be at the forefront of this transformation, for they are currently the locus where demand meets the ability to supply: millennials respond well to digital-first service delivery and desire financial inclusion, and the legislative environment supports the introduction of a wider array of financial services. Concerted efforts are being directed towards introducing and promoting innovative retail e-payment instruments and systems including e-wallets, mobile payments and one-click payments. For example, in Nigeria, the use of mobile-based payment systems has increased as access to mobile phones has become more widespread, both for customer and merchant processes. In India, the central automatic teller machine (ATM) switch that processes all retail ATM transactions has been revamped in preparation for expected demand increase.

One of the most commonly cited examples of leapfrogging is the Safaricom M-Pesa mobile payment system in Kenya and Tanzania, launched by Vodafone in 2007, which enabled phone-based banking in the national currency, abandoning traditional banking methods to create a mobile banking revolution. It is now used by more than 17 million Kenyans, with approximately 25 per cent of the country's gross national product (GNP) flowing through it.¹¹ M-Pesa has boosted economic development by enabling relatively poor farmers to send and receive payments reliably and affordably, fostering economic growth by lowering transaction costs (see Case Study 10.2).

The global mobile industry connected more than 5 billion people in 2017.¹² The Global System for Mobile Communications (GSMA), the industry's non-profit trade association, predicts that the number of unique mobile subscribers will reach 5.9 billion by 2025—equivalent to 71 per cent of the world's population.¹³ Developing countries will drive that growth—particularly India, Pakistan and Bangladesh, as well as sub-Saharan Africa.

To overcome the preference for traditional cash-based transacting while supporting rapid growth, it is especially important for economic structures in emerging markets to integrate with local culture. The large financial services institutions that are common in mature markets are incongruous here and therefore likely to be ineffective. Small—sometimes homegrown—collectives achieve social traction because they adopt systems of operation that are locally trusted. For example, CrowdForce Solution is an Africa-based start-up that uses Ethereum to incentivise trusted local and community retailers to act as banks and offer financial services.¹⁴ It offers utility payments, cash deposit and withdrawal accounts, cryptocurrency exchange, and crypto-fiat exchanges on a PayForceMobileApp. This means there is no need for a banking structure; the only start-up capital required is for agent retailers to fund their wallet, with agents earning commission on transactions.¹⁵

We noted in Chapter 7 that shallow banking infrastructure accelerates the adoption of blockchain in developing economies. Not only does the lack of financial infrastructure mean reduced social and institutional resistance and lower transition costs, but it also means that regulators and existing financial institutions in emerging markets are more open to blockchain-based new entrants.¹⁶ In fact, international payments

and trade finance frontrunners have high transaction and verification costs that blockchain can reduce by improving the speed, transparency and process. In 2018, well-established multinational Western Union partnered with newcomer Ripple to test the speed and economy of blockchain-based cross-border payments.¹⁷

8.6 Regional Considerations

In addition to considering the factors distinguishing large and small nations, as well as advanced and developing economies, it is also important to understand how regional variations across the Commonwealth can affect the development and adoption of fintech. We have divided the countries into four basic regions: Africa; the Americas; Asia Pacific; and Europe.

8.6.1 Africa

Africa is in the midst of a technology transformation on a continental scale. In 2016, more than 700 million smartphone connections were expected on the continent by 2020, with 20 per cent of the continent's population already able to access a mobile broadband connection—a figure expected to triple by the end of 2021.¹⁸ Low-cost devices, such as low-end Android models, have accelerated this trend towards digital inclusion at a large scale.

The costs of mobile services remain a rate-limiting factor in the ability of poorer African peoples to take advantage of digital financial services. A number of developing economies in Africa, however, have sought to leapfrog legacy-laden advanced economies by deploying next-generation systems and solutions that are less readily available in the latter.

8.6.2 The Americas

The Commonwealth countries in the Americas range from the wealthy and

established Canada to an array of Caribbean islands that are working on financial inclusion. Canada has been progressive in embracing pilots of fintech, from AI to digital identity. In the smaller island nations, the Caribbean Community (CARICOM) has served as a forum for the exchange of ideas that has been helpful in fostering progressive policies and opportunities. The Inter-American



Developing economies will be at the forefront of this transformation, for they are currently the locus where demand meets the ability to supply: millennials respond well to digital-first service delivery and desire financial inclusion, and the legislative environment supports the introduction of a wider array of financial services.

Development Bank (IDB) has also been exploring thought leadership and idea exchange around progressive solutions to regional issues such as inclusion.

Unfortunately, identity theft remains a key issue in developing economies in the Americas and, as a result, rates of 'false declines' (legitimate credit card transactions that are not allowed to process) remain high, which inhibits financial inclusion.

8.6.3 Asia Pacific

While inclusion rates vary considerably within the Asia Pacific region, connectivity has been quite good in a number of Commonwealth countries. This, in turn, has facilitated critical policy goals such as financial inclusion, which then enable other more advanced fintech offerings to be provided to the market, such as alternative lending.

Just under two-thirds of the populations of Singapore and Malaysia, for example, are fully banked, while in each country another 20–30 per cent are underbanked (i.e., able to access some services, if not to the same degree as the fully banked).¹⁹

In India, the Aadhaar project has driven a massive increase in the number of bank accounts held, with ever-more government subsidies being paid into those accounts (driving utilisation). Between 2014 and 2017, India increased its banked population from 53 per cent to almost 80 per cent, and the World Bank has found that the growth is continuing.²⁰ Financial literacy remains an opportunity area, however, and the financial services offered to the newly banked remain modest: loans are still difficult to get, for example.

Other Asia Pacific nations, such as Papua New Guinea and Samoa, are at an early stage of their inclusion journey and—with

the support of the Asian Development Bank (ADB) and other bodies—are aiming to leapfrog, with new technologies that empower their population with access to financial services.

Looming over all of the countries in the region are three powerful platforms originating in the People's Republic of China (PRC): Baidu, Ali Baba and Tencent (known as the BATs). These companies have integrated communications data with financial data, which provides them with powerful predictive insights into individuals.

8.6.4 Europe

The three European members of the Commonwealth (the UK, Cyprus and Malta) have been experimenting with and adopting regulation around an array of fintech activities. Malta and Cyprus continue to develop solutions within the context of European Union (EU) regulation, while the UK has been developing parallel and analogous, but different, regulations (e.g., open banking versus the EU revised Payment Services Directive, or PSD2²¹). The UK's multitier licensing of and engagement with new financial institutions (with e-money, 'halfway' banking and a full banking licence, in addition to a regulatory sandbox) remains a gold standard for supporting fintech innovation.

8.7 Conclusion

It is essential that all Commonwealth governments learn how to engage with the new digital issues that cannot be regulated universally across member countries. Digital literacy will prove to be a key skill for citizens, politicians and industry leaders alike. Likewise, both small and large states need information on fintech policy, regulatory approaches and applications, such as digital identity and anti-money-laundering (AML) and know your customer (KYC) rules, the digital issuance of bonds

and treasury notes, the resilience of digital payment systems, digital cash supply and trade finance, etc.

Meeting these needs is challenging territory because there is a shortage of world-class digital experts globally. Commonwealth nations may therefore consider collaboratively investing to develop an elite task force of digital experts who can help multiple governments to develop fintech.

Endnotes

- 1 Organisation for Economic Co-operation and Development (2016). *Digital Government Strategies for Transforming Public Services in the Welfare Areas* [online]. Retrieved from: www.oecd.org/gov/digital-government/Digital-Government-Strategies-Welfare-Service.pdf
- 2 Andrews E, Thornton D, Owen J, Bleasdale A, Freeguard G, Stelk I (2016). *Making a Success of Digital Government* [online]. Retrieved from: [www.instituteforgovernment.org.uk/sites/default/files/publications/IFGJ4942_Digital_Government_Report_10_16%20WEB%20\(a\).pdf](http://www.instituteforgovernment.org.uk/sites/default/files/publications/IFGJ4942_Digital_Government_Report_10_16%20WEB%20(a).pdf)
- 3 Deloitte Access Economics (2015). *Digital Government Transformation*. Retrieved from: www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-digital-government-transformation-230715.pdf
- 4 Much of the content of this section on developing economies was first published in Thomason J, Bernhardt S, Kansara T, Cooper N (2019). *Blockchain Technology for Global Social Change* (Hershey, PA: IGI Global) and is reprinted with permission. See www.igi-global.com/book/blockchain-technology-global-social-change/221876#table-of-contents
- 5 Down M (2018). 'How Blockchain Technology Can Serve Emerging Market Economies'. Hackernoon, 12 September [online]. Retrieved from: <https://hackernoon.com/how-blockchain-technology-can-serve-emerging-markets-a7585ca2ff43>
- 6 Osafo-Kwaako P, Singer M, White O, Zouaoui Y (2018). *Mobile Money in Emerging Markets: The Case for Financial Inclusion* [online]. Retrieved from: www.mckinsey.com/industries/financial-services/our-insights/mobile-money-in-emerging-markets-the-business-case-for-financial-inclusion
- 7 Jones H (2018). 'Cash Is Far from Dead and Use Is Rising'. *Reuters*, 11 March [online]. Retrieved from: [www.reuters.com/article/us-bis-report-cash/cash-is-far-from-deadand-use-is-rising-bis-idUSKCN1GN0PS;PricewaterhouseCoopers \(2018\). 'Emerging Markets: Driving the Payments Transformation' \[online\]. Retrieved from: www.pwc.com/gx/en/industries/financial-services/publications/emerging-markets-driving-payments.html](http://www.reuters.com/article/us-bis-report-cash/cash-is-far-from-deadand-use-is-rising-bis-idUSKCN1GN0PS;PricewaterhouseCoopers (2018). 'Emerging Markets: Driving the Payments Transformation' [online]. Retrieved from: www.pwc.com/gx/en/industries/financial-services/publications/emerging-markets-driving-payments.html)
- 8 Bech M L, Faruqui U, Ougaard F, Picillo C (2018). 'Payments Are A-changin' But Cash Still Rules'. *BIS Quarterly Review*, March [online]. Retrieved from: www.bis.org/publ/qtrpdf/r_qt1803g.htm
- 9 Capgemini (2019). 'Non-cash Payments Volume' [online]. Retrieved from: <https://worldpaymentsreport.com/non-cash-payments-volume/>
- 10 Brown R (2017). 'Digital Payments Expected to Hit 726 Billion by 2020—But Cash Isn't Going Anywhere Yet'. *CNBC*, 9 October [online]. Retrieved from: www.cnn.com/2017/10/09/digital-payments-expected-to-hit-726-billion-by-2020-study-finds.html
- 11 Berman A (2018). 'Western Union Considers Crypto, Partners with Ripple to Test Blockchain Payments'. *Cointelegraph*, 20 December [online]. Retrieved from: <https://cointelegraph.com/news/western-union-considers-crypto-partners-with-ripple-to-test-blockchain-payments>
- 12 GSMA (2017). 'Number of Mobile Subscribers Worldwide Hits 5 Billion'. Press release, 13 June [online]. Retrieved from: www.gsma.com/newsroom/press-release/number-mobile-subscribers-worldwide-hits-5-billion/
- 13 *Ibid.*
- 14 Babayan D (2018). 'Ethereum Adoption in Developing Countries Rising Exponentially: Lubin'. *NewsBTC*, 2 December [online].

- Retrieved from: www.newsbtc.com/2018/12/02/ethereum-adoption-in-developing-countries-rising-exponentially-lubin/
- 15 Down M (2018). 'How Blockchain Technology Can Serve Emerging Market Economies'. Hackernoon, 12 September [online]. Retrieved from: <https://hackernoon.com/how-blockchain-technology-can-serve-emerging-markets-a7585ca2ff43>
 - 16 International Finance Corporation (2017). *MSME Finance Gap: Assessment of the Shortfalls and Opportunities in Financing Micro, Small and Medium Enterprises in Emerging Markets* [online]. Retrieved from: <http://www.ifc.org/wps/wcm/connect/03522e90-a13d-4a02-87cd-9ee9a297b311/121264-WP-PUBLIC-MSMEReportFINAL.pdf?MOD=AJPERES&CVID=m5SwAQA>
 - 17 Berman A (2018). 'Western Union Considers Crypto, Partners with Ripple to Test Blockchain Payments'. *Cointelegraph*, 20 December [online]. Retrieved from: <https://cointelegraph.com/news/western-union-considers-crypto-partners-with-ripple-to-test-blockchain-payments>
 - 18 Rice-Oxley M, Flood Z (2016). 'Can the Internet Reboot Africa?'. *The Guardian*, 25 July [online]. Retrieved from: www.theguardian.com/world/2016/jul/25/can-the-internet-reboot-africa
 - 19 Soriano M *et al.* (2019). *The ASEAN FinTech Ecosystem Benchmarking Study* [online]. Retrieved from: www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-ccaf-asean-fintech-ecosystem-benchmarking-study.pdf
 - 20 Demirgüç-Kunt A, Klapper L, Singer D, Ansar S, Hess J (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution* [online]. Retrieved from: <http://documents.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf>
 - 21 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 23 December 2015, OJ L 337/35.

Chapter 9

Action Framework for Creating an Enabling Environment for Fintech



Action Framework for Creating an Enabling Environment for Fintech

Key points

Through consultation with the Commonwealth Central Bank Governors (CCBGs), academics and subject-matter experts from the private sector, the Commonwealth has devised an 'action framework' outlining:

- how to build an effective national or regional fintech task force;
- the steps that governments and that task force can take to create an enabling environment for fintech and fintech applications, from first establishing context through to public launch; and
- the ways in which governments and other stakeholders can support one another to build on success.

9.1 Introduction

Developed in response to calls from and in consultation with Commonwealth Central Bank Governors (CCBGs), as well as academics and subject-matter experts from the private sector, the Commonwealth Fintech Toolkit aims to help government policy-makers and regulators to take practical steps to create an enabling environment for fintech. It stands alongside other international efforts such as the Bali Fintech Agenda, which the International Monetary Fund (IMF) launched in association with the World Bank late in 2018.¹

In Part I of the Toolkit, we looked at tech topics. In Part II so far, we have considered the policy outcomes and other considerations that might lead a government to pursue fintech initiatives. We look now at an 'action framework' that will support

governments and other stakeholders in creating an environment that will enable those initiatives and improve the likelihood that they will be successful.

The best practice gathered in this chapter is drawn from both primary and secondary research (see Appendix 2), including interviews with representatives of Commonwealth governments and other fintech stakeholders. We directly quote some of these participants in this chapter to provide context and insights based on their practical experience.

At the outset, the Deputy Secretary-General of the Commonwealth Secretariat helped to define the work needed to convert the concepts which we have looked at so far into the actions that create an enabling environment for fintech in a country or a region:

There are several questions to be answered ... What regulations and policies do we need in this area? What is working and what is not working? What institutions are necessary for a fintech-friendly system and how do they work together as one? What infrastructure is needed? And last, but not least, do we have adequate human resources?

Dr Arjoon Suddhoo, Deputy Secretary-General, Commonwealth Secretariat

Because Bermuda has been at the forefront of developing fintech policy, enacting a series of enabling regulations and organising government offices to sponsor fintech

initiatives, the Honorable E David Burt, JP, MP, Premier of Bermuda, and members of his government played a key part in shaping the action framework:

We all recognise that fintech is a very open and collaborative industry. Bermuda's experience of working with some of the thought leaders in this space has helped us to develop our legislative and regulatory framework, which is the foundational pillar of our ecosystem. Bermuda is of the position that, since this was an emerging and disruptive technology or space that could present risk to our existing financial ecosystem and our reputation, it was important to create laws first so that people could have fair, safe and a well-regulated space [in which] to innovate, create and develop ideas.

Honorable E David Burt, Premier of Bermuda

The action framework therefore outlines:

- how to build an effective national or regional fintech task force;
- the steps that governments and that task force can take to create an enabling environment for fintech and fintech applications, from first establishing context through to public launch; and
- the ways in which governments and other stakeholders can support one another to build on success.

9.2 Building an Effective Fintech Task Force

An effective fintech task force at the country or regional level will be critical to building,

delivering and continuously improving any enabling environment for fintech.

The most successful task forces tend to comprise individuals from the public and private sectors, as well as so-called captains of industry, under the supervision of and support from a fintech champion in government (*see later in the chapter*).

To build an effective task force, we first need to identify the necessary skill sets and backgrounds that individuals need to bring to the table, and which interests need to be represented. This is most likely to emerge as part of the sense-making work we do in the initial stages of creating an enabling environment for fintech: when establishing context and during analysis. These skills sets, backgrounds and interests will

necessarily differ from country to country and region to region, and it is with these clearly defined person specifications that government leaders can identify, recruit and benefit from the expertise of specific individuals as part of the fintech task force.

Once convened, the task force must establish a regular schedule of meetings, set clear goals and practicable timetables, and distribute minutes to all participants to fuel continuity and accountability.

More broadly, a country's or region's fintech task force may wish to co-ordinate with other international bodies, to ensure that it can respond to issues that may arise in a globally connected financial system.

One such issue is cybersecurity: should an attack occur in one country or region, its effect might be contagious across many. Should a country's financial system—or even a single institution within that system—be hacked, for example, the proceeds of cyber theft might flow through multiple

other national systems (as was the case for the Bangladesh Bank cyber heist²). Another example is in the domain of central bank digital currencies (CBDCs), where questions of interoperability arise if CBDCs are to be realistic alternatives to conventional currencies.

The UK has long recognised that co-ordinating international standards and other efforts can drive a more effective response to systemic risk (also known as contagion risk) events. As such, the UK is involved in the work of the Committee on Payments and Market Infrastructures (CPMI), International Organization of Securities Commissions (IOSCO), the G7 cyber experts group, and the work of the Financial Stability Board (FSB).

For Barbados, a regulatory sandbox was the solution to mitigating risk as it began to experiment with fintech, offering a safe environment in which start-ups could test new technologies without risk of harm to consumers or to the country's financial system:

Our response has been centred around the development of a regulatory sandbox to better engage with start-ups that require greater regulatory clarity and to allow the Central Bank of Barbados (Bank) to better understand these new business models and their product offerings. ...

Most of the Bank's work related to fintechs has been structured by way of an internal cross-departmental work group that was established to leverage the differing perspectives from Legal, Bank Supervision, and Operations department. Some of this work has been relevant to the undertakings of the [Caribbean Community] CARICOM Fintech Work Group that Barbados chairs. This regional group has been focusing on issues such as the regulatory framework for digital currency, the efficiency of digital cross-border settlement and data protection provisions to enable greater digital payments. There are some similar realities across the region and as such, it makes sense to evaluate the varied regulatory approaches to fintechs, [acknowledging] what can be standardised and the potential efficiency gains.

Michelle Doyle-Lowe, Adviser, Central Bank of Barbados

9.3 Creating an Enabling Environment for Fintech

The work outlined in the appendices has allowed us to build consensus around a set of steps that governments can take to create an enabling environment for fintech and fintech applications. While these will be championed from within government and led by the fintech task force, participants agree that continuous stakeholder consultation is essential not only to inform the decision-making process, but also to ensure that the outcomes are more swiftly and more broadly adopted.

The six steps—or stages—through which governments and regulators

should progress when seeking to foster an enabling environment for fintech are as follows.

1. Establishing context
2. Strategic analysis
3. Project planning
4. Resource acquisition
5. Early implementation
6. Public launch

[T]echnology is moving at a phenomenal pace and revolutionising our way of life, work and even play. However, when we discuss technology in the context of development, [we] should not lose sight of the social and environmental issues. There are many demands and expectations from our diverse range of member countries and, to that end, the Secretariat views technological innovation as a catalyst for growth and development, particularly in the arena of ... financial technology ... Although the Toolkit is not yet comprehensive, it focuses on the core tech products and themes in the financial technology space. It provides case studies to showcase how fintech is being utilised for development.

Dr Arjoon Suddhoo, Deputy Secretary-General, Commonwealth Secretariat

9.3.1 Establishing Context

At the very outset, any government must reflect on *why* it is seeking to create such an

environment—that is, it must establish the context in which it aims to facilitate fintech:

In 2019, The Bahamas ... experienced one of the largest hurricanes to ever blow through the region and almost 100% of the banks were thoroughly destroyed. At the moment, the banks are still not fully operational, which really frustrates a lot of residents there. They have no means to send money, to receive money or even [to] commercialise with dignity. At the moment, a lot of residents are left with no money because prior to the hurricane they had been storing physical cash in their homes. It is a very sad realisation where we have discovered some newfound meaning to establishing [a CBDC]. There are true, meaningful and tangible ways to use and propagate this agenda. Obviously, it is also used to strengthen our national defences against [money laundering] as well as other illicit activities that are being carried by cash today and also [to] reduce the reliance on cash usage in the domestic market.

Chaozhen Bobby Chen, Assistant Manager E-Solutions, Central Bank of The Bahamas

As it does for all of its policy-making, the government will engage in this sense-making by:

- attending industry events to understand current trends;
- compiling and dissecting research reports;
- meeting with industry, academic and consultative experts;
- commissioning a study of the market and country-specific opportunities; and/or
- convening one or more multistakeholder working groups that span the public and private sectors and reflect the country's or region's strengths.

Motivation

Any government seeking to facilitate fintech must clearly define and communicate its motivation for doing so. For example, it might see fintech as a solution to one or more policy goals. It might be responding to market behaviour or demand. It might be trying to align itself more nearly with its trading partners.

For the Eastern Caribbean Central Bank (ECCB), the motivation was a need to remedy financial exclusion and to lower the high costs to consumers of doing business with commercial banks in the Caribbean region. It recognised the opportunity that a new, real-time payments system offered in terms of affordability and accessibility, and it was eager to harness that system to fuel financial inclusion:

DXCD Caribe is a secure, accessible, real-time payment system in the Eastern Caribbean Currency Union [ECCU] ... [W]hen we look at the DXCD Caribe, we have to consider the ultimate objective we are trying to achieve. We ask questions such as: why are we building this product? What platform capabilities are desired? Who are the players who are going to use the system? How are we going to interact with the platforms?

Sharmyn Powell, Chief Risk Officer, Eastern Caribbean Central Bank

Having recognised the potential of fintech to deliver a powerful policy outcome, the ECCB next assessed what technology it should use. Should it base the system on older technologies that were proved and stable, or on newer developments such as blockchain that would offer

transformational cost and performance improvements, but introduce technology risk?

The ECCB actively pursued a disciplined approach to this question, weighing up risk and benefit in the context of its goals:

... Once we are able to answer those questions, we are able to determine the best solutions we can use to deliver this product. We have chosen a blockchain product. Based on our research, we think this is best suited to deliver the product we want to provide our citizens.

Sharmyn Powell, Chief Risk Officer, Eastern Caribbean Central Bank

Bermuda, meanwhile, assessed its own financial services strengths and decided to root its enabling environment on both

'vertical' sector knowledge (of industries such as insurance or tourism) and 'horizontal' competency around regulatory equivalence:

It was decided to leverage Bermuda's reputation as a top jurisdiction for financial services, reinsurance and insurance to build an ecosystem for the fintech industry. We have regulatory equivalence along with Switzerland, which means that an insurance company that is domiciled in Bermuda can write business anywhere in the [European Union] or North America as if they were physically domiciled in those jurisdictions, but the company is in Bermuda. We want to do the same thing for the fintech industry as we try to create this kind of ecosystem or environment, where companies can set up their businesses here and benefit from our established reputation in tourism, international business and reinsurance, in financial services.

Major Allan Wayne Smith, Head, Fintech Business Unit, Government of Bermuda

If we understand acutely why we want to establish a robust fintech-enabling environment, we will be well placed to align our subsequent strategy, policy, planning and implementation towards a successful outcome.

Ownership

Understanding our context is only one part of the puzzle, however; if we intend to translate that understanding into action, we must be certain to attribute ownership.

Government must take clear ownership at the outset, identifying and empowering someone to champion the initiative. The fintech champion may be the head of state, a cabinet minister, a central bank governor or an equivalently placed individual. With sponsorship at a senior level in government, the fintech task force will be more likely to overcome organisational inertia, to maintain momentum, to secure sufficient resources, and to successfully co-ordinate action among governments and/or between the public and private sectors.

In some countries that have focused on enacting progressive regulations (e.g.,

Bermuda and Malta), the fintech initiative is sponsored by both the premier or prime minister's office and a governing regulatory body, such as the financial regulator or the central bank. In others, the regulator or central bank is driving fintech focus and its chief executive is the champion. Examples include the Monetary Authority of Singapore (MAS) and the Financial Conduct Authority (FCA) or the Bank of England in the UK, which collaborates with the Department for International Trade (DIT) and Her Majesty's Revenue and Customs (HMRC), among other partners.

When a government initiative in a complex, multi-stakeholder domain such as fintech is pushed from below only by industry professionals and without solid sponsorship at a senior government level, the story is invariably the same: the initiative struggles to achieve traction and fails.

9.3.2 Strategic Analysis

Once we have established our context, we must analyse that context strategically. While there are myriad tools that a government or the fintech task force can use to that end, we will look at only the most common—namely:

- SWOT analysis;
- PESTLE analysis;
- gap analysis; and
- systems mapping.

SWOT Analysis

Any government proposing to create an enabling environment for fintech must first analyse its strengths, weaknesses, opportunities and threats (SWOT). Such analysis—SWOT analysis—is a common tool in developing strategy, and in this context it will focus keenly on the nation’s financial services capabilities. For example, one nation might have a strong insurance industry. Another might have greater capacity in payments or an attractive business tax regime. Yet another might have strengths in asset management or in outsourced software development. Few, if any, nations are equally effective in all aspects of financial services and, by establishing those areas in which it excels, the government will expose the strongest foundation on which it might build an enabling fintech ecosystem.

Any SWOT analysis is typically set out as a 2 x 2 grid (see Figure 9.1), each segment of which is populated with key bullet points that allow the stakeholder to explore the factors at play.

PESTLE Analysis

Another familiar framework for strategic analysis of the context in which we intend to introduce the fintech initiative is PESTLE analysis—that is, analysis of the political, economic, social, technological, legal and environmental (PESTLE) factors at play.

To some extent, the Toolkit itself has already explored a wide range of such factors, but

Figure 9.1 SWOT analysis.



the extent to and ways in which they impact on any given country or region and relate to a proposed initiative will vary. The government or fintech task force must take care to narrow its focus and analyse most closely those factors that are relevant to its own specific context.

Gap Analysis

A systematic gap analysis is a tool that the government and fintech task force can use to explore its current context, to identify existing shortcomings and to craft solutions that meet those needs.

At its simplest, a gap analysis comprises four steps—or, more properly, four questions:

1. Where are we now?
2. Where do we want to be?
3. What is the gap between where we are now and where we want to be?
4. How can we close that gap?

The ECCB conducted gap analysis when developing its blockchain payments system:

... [W]hat we did was undertake an analysis of our existing information security policies against the requirements of DXCD Caribe to see what gaps there were and what new policies [we] would need to implement. To date, we have updated our information security policy paying special attention to [anti-money laundering] AML industry standards, not only for blockchain, but [also for] the entire system, in terms of the best security practices we need to have internally to deliver the product that would best serve the people of the region.

Sharmyn Powell, Chief Risk Officer, Eastern Caribbean Central Bank

Systems Mapping

Finally, and in the most detail, systems mapping allows us to visualise multiple stakeholders and understand how they relate to one another in the established context.

That systems map then informs systems thinking, revealing new opportunities—potential collaborators—and allowing us to militate against unintended consequences.

For example, one government with which we spoke had tried to manage the costs of new fintech to consumers by putting in place interest rate caps—a policy tool that some World Bank economists believe to be ineffective (see Chapter 1). These caps meant that it was no longer economically

viable for some lenders to participate in the market and they withdrew, leaving consumers with fewer choices, reducing competition and diminishing innovation.

In that case, while the government swiftly tried to correct its course, had it constructed a systems map and engaged systems thinking before implementing the measure, it could have avoided this outcome. Had it identified the risk, the government would have facilitated dialogue among stakeholders and found an alternative intervention.

Bermuda describes its nuanced risk management framework:

Some jurisdictions have taken the view that they can take existing case law or legislation and try to shoehorn these new innovative, disruptive companies into global legislation. That does not work. It is not what they need and will not encourage innovation and drive good options. It will not allow these companies to come and set up and create in a free manner. We take the view that it is about understanding the risks and establishing rules and laws around them.

The four types of risk that we have identified are business risks, custody risks, cybersecurity—many of you will have heard that it is not a question of if but when you will be hacked, so it is important for companies to develop strong cybersecurity policies—and compliance around [know your customer] KYC, know your customer's customer (KYCC), anti-terrorist financing and AML to ensure that your business plan and operating principles and methods are positioned so that the company is sound and can avoid these types of risk.

Major Allan Wayne Smith, Head, Fintech Business Unit, Government of Bermuda

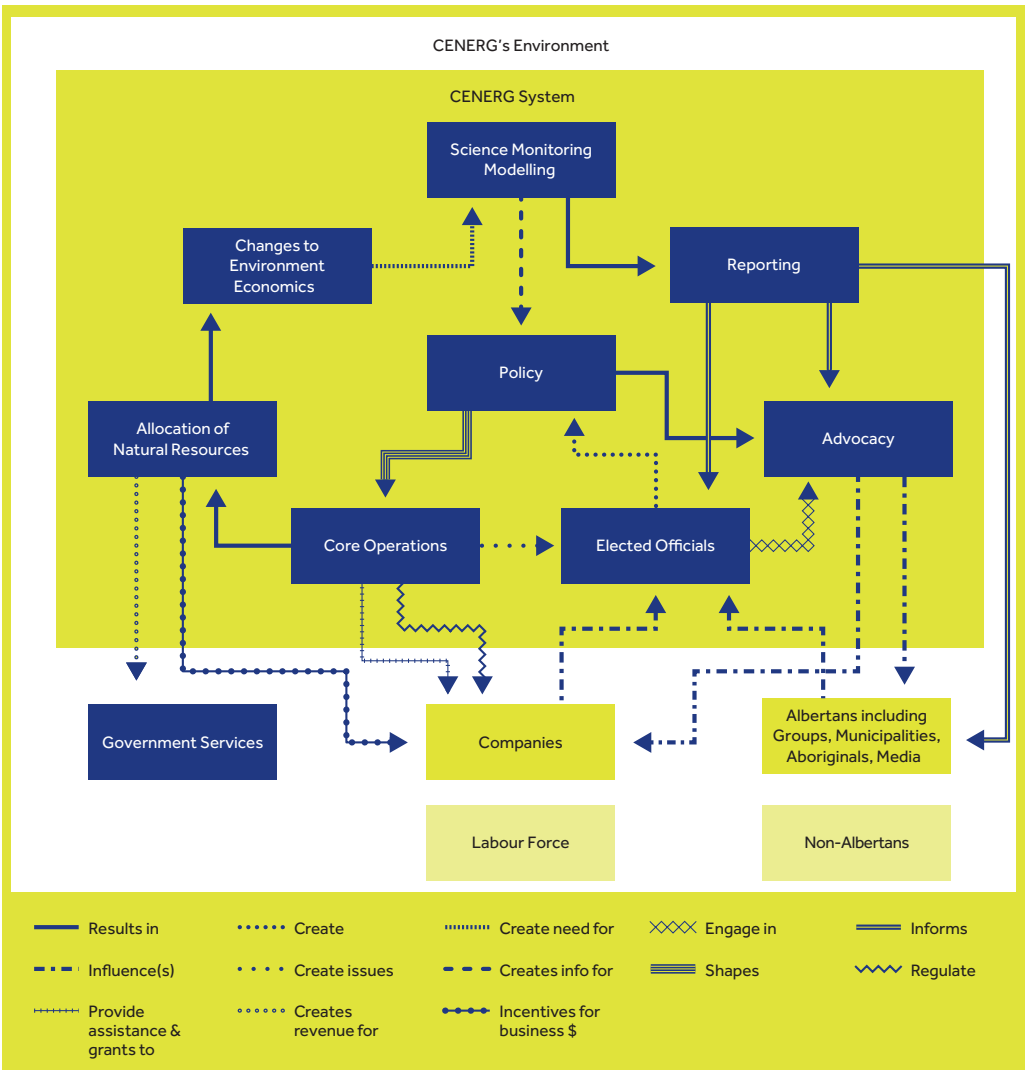
Figure 9.2 is an example systems map illustrating a policy-driven clean energy ecosystem for the government of Alberta, Canada.

In Figure 9.2, the inner box defines the core system, while the outer box spans the whole of the relevant environment. In a systems map of a country's fintech

environment, the central bank, finance ministry and even a technology ministry might be part of the core system, while fintech start-ups and incumbent banks might be part of the broader environment.

This type of systems mapping was integral to the approach that Bermuda took in considering its approach to fintech:

Figure 9.2 An example systems map.



Source: A Ryan, M Leung (2014). 'Systemic Design: Two Canadian Case Studies'. *FormAkademisk*, 7(3) [online]. Retrieved from: <https://journals.hioa.no/index.php/formakademisk/article/view/794>. Used under Creative Commons licence: <https://creativecommons.org/licenses/by/4.0/>

... [W]e are trying to look at where fintech is going. That is where blockchain starts to fit in. When we look at what is really happening in the long term, it is taking that traditional, vertically integrated stack, where you had innovations on payments, remittance and those layers, and the innovation happening on it, traditional fintech with Square and Alipay. We are seeing, because of these open distributed ledgers, the ability to start separating out the base core function of a bank, which is custody, and have open interoperability on top of it, in terms of accounts.

That allows us to generate data insights and have access to information, which means that, instead of having to build that vertical stack, like you saw with Square, of payments, point of sale and then lending, we could have multiple players sharing and interoperably driving the same data, to drive new services and innovations that do not require a whole stack. It can be more narrowly focused on a specific area of business, but with a much more global scale. We are going to see more innovation in lending that takes a global approach and can drive more efficiency and apps that specialise in each one of [the] areas leveraging the core infrastructure of custody, combined with open standards and interoperability. Back to that parallel of what happens when we digitise and can drive more insights, how do we drive control and leverage this kind of innovation?

Denis Pitcher, Chief Fintech Adviser to the Premier, Bermuda

9.3.3 Project Planning

The next stage, project planning, will necessarily be based on the results of strategic analysis.

Planning will involve identifying the specific actions that the government, fintech task force and other stakeholders must

take to implement the approach on which they have decided based on that analysis. It includes scheduling the project and developing a timeline, with key milestones, contingencies and gate reviews, and it demands that we anticipate the resources necessary, as well as the metrics that will be indicative of our success:

Contingency planning means you can then expand the horizon of risk taking as you are gaining assurances that the idea is moving along.

Marcelo Ramella, Director, Financial Stability Department, Bermuda Monetary Authority

Governments must carefully consider such metrics. For example, some countries have measured the success of fintech initiatives aiming to tackle financial inclusion by means of the number of bank accounts as a percentage of the total population. They swiftly recognised, however, that this was a worthless measure of nothing more than newly created

zero-balance, zero-activity bank accounts. Subsequent efforts in these and other countries have gone on to measure not only account ownership, but also activity within the account, with some countries now drilling down to add value by measuring whether core household spending runs through the account or only select and discretionary spending.

Crucial to planning for some governments will be the statutory time frame for introducing new legislation or expanding existing fintech mandates.

For example, Australia had granted few new banking licences in 20 years,³ but when the government decided to target greater competition in the market, it formalised a consumer data right (CDR) to facilitate open banking, and it introduced new regulations to facilitate choice and reduce costs for consumers.⁴ Likewise, when Kenya sought to enable the launch of M-Pesa and subsequently to adapt its evolving environment as more and more Kenyans began to use the mobile payment system in their everyday lives (see Case Study 10.2), it needed to develop a fintech-related legislation regime. Some states within and

outside the Commonwealth have even passed fintech-specific legislation after recognising that extant market activity fell outside the scope of existing laws.

The decisions made and the approach refined during the planning process will help to define the organisational mandate of fintech start-ups. Not only will the government, fintech task force and all other stakeholders, including start-ups, understand the scope of their powers and the expectations that they must meet, but also they will uncover those areas in which they need to work collaboratively—both among themselves and across jurisdictions.

Bermuda contemplated both risk and innovation in designing its fintech efforts as part of a global financial services system:

The key thing is looking at what your risk thresholds are and how you contain the risk but allow for innovation and what fits your jurisdiction. For us it is looking at how we embrace this innovation but constrain the risks well enough that we do not put our global industry at risk. For your own jurisdictions, it is looking at your own place. The biggest challenge ... is the potential to be excluded from correspondent banking and shut out of the global banking system.

How do we foster innovation? There have been a lot of moves with the interbank settlement network in trying to get around some of these problems and have other opportunities. How do we collaborate as jurisdictions to enable that, and how do we create environments that start building on some of this future vision that we are seeing globally around digital currencies and the potential?

Denis Pitcher, Chief Fintech Adviser to the Premier, Bermuda

9.3.4 Resource Acquisition

Building on project planning, resource acquisition demands that governments and the fintech task force gather the ingredients without which the initiative will fail. Resources, in this context, can be broadly defined and we will focus here on four key categories:

- funding;
- personnel;

- institutional capacity; and
- collaborators.

Funding is self-evidently a necessary ingredient in creating an enabling environment for fintech. Some of this may come directly from government sources, while some may be secured from international organisations such as the World Bank, the IMF, the Asian Development Bank

(ADB), the Inter-American Development Bank (IADB), the African Development Bank (AfDB), one or more export–import banks or private foundations, among others.

Personnel need to be recruited to the effort. Dedicated staffing is recommended, but it may be supplemented by full-time and/or part-time team members seconded either from within the central bank or finance ministry, or from across other government departments or agencies—noting that it is not always easy to identify or attract fintech professionals with the skills and backgrounds that will allow them to support the initiative effectively.

Governments may need to build **institutional capacity** around fintech. While professionals may be well versed in traditional banking and financial systems management, they may not have been exposed to the dynamics, technologies and participants in the fintech ecosystem. To remedy this, a government can draw on global expertise, diverse experiences and case studies by enrolling personnel in online learning with leading universities. Bespoke in-person workshops can also help governments to localise that learning to meet the specific needs of its own market.

Because fintech is a domain that spans disciplines, **collaborators** will help to

ensure the success of the initiative. Identifying, enlisting and co-ordinating collaborators from inside and outside of government is an essential component of resource acquisition. Government ministries (and corresponding industry representatives) ranging from education to information and communications technology are key players; economic development units are also likely to add value.

Collaboration has proved to be important in risk management and stimulating opportunity. For example, when Canada's federal government consulted on its efforts to streamline and innovate the Canadian payments system,⁵ that consultation in turn led private-sector actors to create Verified.me, an identity utility for the financial services industry, combining the experience of large incumbent financial institutions with start-up nimbleness to excellent effect.⁶

Collaborating across borders is another opportunity that effective resource acquisition will deliver. International groups and networks, such as the Global Financial Innovation Network (GFIN), the Finance Directorate of the Organisation for Economic Co-operation and Development (OECD), and the World Economic Forum (WEF) working groups, can be precious partners in new fintech initiatives:

[These partners] provide for private-sector concierge services for assisting new businesses looking to enter the market to establish themselves with key stakeholders and players in the jurisdiction.

Alex Marshall, Founder, BermudaChain

9.3.5 Early Implementation

Once we have established our context, analysed that context strategically, planned the project and acquired the necessary

resources, we can start to put 'flesh on the bones' with procedures and guidelines—the tools with which we will implement our initiative. Among them will be specific

guidelines and other materials to support government and personnel in delivering the initiative, as well as communications materials aiming to explain it to external stakeholders.

While not all governments will do the same, Bermuda focused first on embedding the legislative regime:

Developing a fintech ecosystem in your jurisdiction starts with legislation. You do not want the country to be the wild, Wild West and it could be like that if you do not have rules. Most human beings are creatures of habit and while we like to be creative, disruptive and anti-authoritarian sometimes ... it works better if we have rules because they make [for] fair play, as with any endeavour in life.

Major Allan Wayne Smith, Head, Fintech Business Unit, Government of Bermuda

Indeed, the legislative process offers opportunities for further consultation and public comment, which facilitates stakeholder voice and can include rounds of expert testimony or other formal comment mechanisms to ensure that critical input shapes the laws enacted. In this way, the early implementation stage can build buy-in and, carefully handled, can allow governments and fintech start-ups to

overcome stakeholder resistance before the final stage, launch.

To this end, Bermuda also thought critically about communicating the unique assets it would bring to the global stage with respect to fintech, noting candidly that no country is alone in seeking to offer attractive environments to new business and that a country's ability to differentiate itself rests on its strengths:

It is important to understand your economy proposition and what it is that you and your country can do. You must focus on your value proposition as you cannot be all things to all people. Identify what you can do and do that well, while marketing that to your internal and external stakeholders. ... One of the important tenets is stakeholder consultation and you cannot implement an effective policy if you have not done useful and collaborative conversations with your key stakeholders.

Major Allan Wayne Smith, Head, Fintech Business Unit, Government of Bermuda

9.3.6 Public Launch

With all of the necessary structures in place, the success of the final phase of the initiative—public launch—will depend on a robust communications strategy. Clear communications at this stage will continue

to share the benefits and opportunities of the fintech initiative with public and private stakeholders. A continuous engagement process aligned with the strategic objectives of the fintech initiative will be key, as Bermuda confirms:

You have to bring people along and communicate with internal and external stakeholders so that they know exactly what you are trying to accomplish. There is no point implementing an initiative that the whole country does not understand as they will not follow you or support the initiative ... That is ... where you can learn from our experience. We need to make sure that we devote the relevant resources and have a proper communication strategy with frequency of communication to deliver the messages to the entire country about what you are trying to accomplish to achieve buy-in.

Major Allan Wayne Smith, Head, Fintech Business Unit, Government of Bermuda

Moreover, maintaining that communications strategy *beyond* launch will help to secure continued support and a receptive audience for the fintech outcomes of the enabling environment we have worked hard to create.

9.4 Building on Success

In outlining these steps—from establishing context to public launch—we have set out best practices emerging from our research into and interviews with multiple individuals and governments, drawn both directly from experiences in launching fintech initiatives and from other government interventions.

When creating an enabling environment for fintech in any jurisdiction, a government must take into account all of the factors that are specific to it locally. If we simply mimic the activities of any other jurisdiction without tailoring the steps to meet our own needs, we set ourselves up to fail.

As governments within the Commonwealth apply this Toolkit, they will valuably gather their experiences and collate their learning, helping one another to refine the recommendations set out here and informing further iterations of the Toolkit itself—a collaborative spirit that the Bermuda Monetary Authority (BMA) models:

The Bermuda Monetary Authority (BMA) strives to maintain fit-for-purpose regulation. This type of iterative approach is often rare among regulators, but you will see it in Bermuda. Innovation is in the BMA's DNA and we know that a quick yet prudent response to the exponentially evolving market dynamics will help maintain Bermuda's position as a jurisdiction of choice. The Digital Asset Business Act was released in 2018, amended in 2019, and will likely be amended further if additional market innovations or events create the need for further requirements and controls. Our aim is to strike a balance between protection and pragmatism—upholding our high standards, particularly from a risk perspective, while acknowledging innovation and market needs. To accomplish this, we frequently engage with the local and international ecosystem, including our global regulatory counterparts, to benchmark progress and provide and solicit feedback on regulatory innovation. This collaborative spirit enables us to share best practices for the regulation of digital assets and digital finance technologies, as well as [to] conduct cross-border trials in a global sandbox.

Aqsa Zubair, Fintech Specialist, Bermuda Monetary Authority

This iterative process of continuous learning is one that governments in other jurisdictions, ranging from Kenya to Canada, practise, incorporating the lessons learned from early fintech experiments into refinements to legislation and regulation.

In the dynamic and ever-evolving arena of fintech, continuous learning is crucial. No single statute or regulatory regime can be both specific enough to suit current needs and yet general enough to withstand years of innovation. A robust working group of stakeholders can help a government to stay up to date with emerging technologies and emerging policy issues, allowing it to create and sustain a dynamic enabling environment for fintech that stays aligned with societal goals.

Endnotes

- 1 International Monetary Fund (IMF) (2018). *The Bali Fintech Agenda*. IMF Policy Paper, October [online]. Retrieved from: www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda
- 2 Al Jazeera (2018). 'Hacked: The Bangladesh Bank Heist'. 24 May [online]. Retrieved from: www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html
- 3 Eysers J (2017). 'New Breed of UK Start-up Banks Force Licensing Rethink'. *Australian British Chamber of Commerce*, 26 April [Blog]. Retrieved from: www.britishchamber.com/blog/new-breed-uk-start-banks-force-licensing-rethink-james-eyers-afr
- 4 Finextra (2020). 'Australia Gets Ready for Open Banking'. 11 February [online]. Retrieved from: www.finextra.com/newsarticle/35264/australia-gets-ready-for-open-banking
- 5 Shinfield J, Murray B, Teolis J (2012). 'Canada: The Final Report of the Task Force for the Payments System Review Arrives'. *Mondaq.com*, 4 April [online]. Retrieved from: www.mondaq.com/canada/financial-services/170662/the-final-report-of-the-task-force-for-the-payments-system-review-arrives
- 6 Paddon D (2019). 'Canada's Big Banks Launch Verified.Me Network to Help Prevent ID Theft'. *CBC.ca*, 1 May [online]. Retrieved from: www.cbc.ca/news/business/canada-big-banks-launch-verified-me-network-dataidentify-theft-1.5118471

Chapter 10

Case Studies



Case Studies

Key points

The Commonwealth FinTech Toolkit closes with four case studies of fintech interventions promoting growth and development. In doing so, it aims to highlight the sensitivity with which governments should apply fintech in their own distinct contexts.

The case studies are as follows:

- **Case Study 10.1 The Journey of Emerging Technologies: Blockchain in Papua New Guinea**
- **Case Study 10.2 Pioneering Mobile Money in Kenya**
- **Case Study 10.3 Digital Assets Businesses in Bermuda**
- **Case Study 10.4 Malta's Support for Virtual Financial Assets**

Drawn from primary research in the form of interviews with representatives of Commonwealth governments (see Appendix 1), these case studies have been selected to highlight the use of fintech in developing economies and small states. Given that the vast majority of Commonwealth countries are developing, rather than developed, nations, the focus is on these. While nations such as the United Kingdom, Canada and Australia have taken sophisticated and highly evolved approaches to fintech (among them, digital banking in the UK, digital identity in Canada and digital assets trading in Australia), case studies of these would be unlikely to be applicable or portable to a small sub-Saharan African country or a Caribbean island nation.

These examples illustrate different types of fintech policy and implementation, across blockchain and digital identity, mobile money and digital assets. In addition, an effort was made to look both at mature policies and environments (such as Kenya's work with mobile money over ten years or

more) and at those on the cutting edge of emerging technology (such as Papua New Guinea's incorporation of biometrics and blockchain into a digital identity system).

Case Study 10.1 The Journey of Emerging Technologies: Blockchain in Papua New Guinea

10.1.1 Introduction

This case study relates to the Bank of Papua New Guinea (BPNG), the country's central bank, and its exploration of distributed ledger technology (DLT)—that is, blockchain—and the application of emerging technologies in its pursuit of financial inclusion.

10.1.2 Context

One of the pillars in the BPNG's 2016–20 Strategic Plan was the pursuit of financial inclusion for all PNG citizens.¹ As regulator of the economy, BPNG is duty-bound to investigate new and emerging technologies, to understand the impact that they have on banking regulations, and to develop a culture of embracing new and emerging technologies.

Quick Facts**Country:** Papua New Guinea (PNG)**Population:** 8.606 million**Gross domestic product (GDP), 2018:** US\$23.43 billion/£19.05 billion**GDP per capita, 2018:** US\$4,298.70/£3,494.90**Top three industries:** petroleum and natural resources; logging and agriculture; fisheries and marine**Source:** World Bank (2018). 'Papua New Guinea' [online]. Retrieved from: <https://data.worldbank.org/country/papua-new-guinea>**10.1.3 Challenges/Problems**

- PNG is one of the largest and most mountainous islands in the world, and these distances and terrain create telecommunications issues.
- There are approximately 8 million people in PNG, of whom only 18 per cent live in urban centres, making reaching all citizens difficult.
- There are more than 800 unique languages spoken in PNG, making basic interpersonal communications difficult.
- Some 85 per cent of the population do not have a bank account and hence the drive for financial inclusion.
- Birth registration is at less than 5 per cent and therefore identity is a major impediment to financial inclusion.
- Only 20 per cent of the population have access to electricity, while internet connectivity is poor, unreliable and not widely available.
- More than 75 per cent of the population have an SMS-capable mobile phone,

but less than 5 per cent of the population have a smartphone.

10.1.4 Policy Intervention

In late 2016, BPNG began to explore DLT and the potential impact that virtual currencies—especially Bitcoin—might have for the regulator.

Under the leadership of BPNG Governor Loi Bakani, a research programme was tasked with understanding these in more detail and investigating how DLT might be used towards greater financial inclusion. This included sponsorship of and participation in the Fintech Worldwide London Blockchain Conference and Hackathon in 2017—an event that led to the winning concept of a handheld, SMS-driven device. Initially labelled 'The Papuan Box', but later renamed 'IdBox', the device incorporated a biometric reader, ran on solar power and did not require internet connectivity—overcoming three challenges specific to digital identity in the PNG operational environment.

Field Trials

With funding from the Australian Department of Foreign Affairs (DFAT) and the Asian Development Bank (ADB), this and further iterations of the device and its successor were brought to PNG for field trials.

Successful proofs of concept emerged from trials in the villages of Lalaura, Abau District,

and Vesulogo, Bisiatabu District, both in Central Province (Exhibit 10.1).

Exhibit 10.1 Papuany Box field trials.



Notes: Solar power pack; IdBox identity device; fingerprint reader; SMS SIM card number; combined and encrypted
Source: Central Bank of Papua New Guinea

Exhibit 10.2 PNG Digizen prototype field trial.



Notes: Any Android device; scan and issue modes; encrypted card; KYC/e-KYC compliance; two-factor authentication; biometric-ready; no need for mobile ownership; online/offline capability; multipurpose card
Source: Central Bank of Papua New Guinea

A revised version using near-field communication, biometric and photographic recognition, and a trust-based hierarchy of know your customer (KYC) compliance (Exhibit 10.2) was the last to undergo final field trials before submission in January 2020 to testing in the BPNG regulatory sandbox—the first regulatory sandbox to be launched in the South Pacific.

The BPNG Regulatory Sandbox

The BPNG regulatory sandbox was expected to:

- provide an opportunity to test innovations in a safe environment;
- stimulate the interest of local and international innovators and investors in fintech; and

- protect consumers interested in trying new technologies.

In this way, the PNG government aimed to lower financial services fees and speed up processes, while insisting that those successful in the sandbox deploy their initiative in PNG within nine months of the trial ensures that PNG citizens reap the reward of the BPNG's investment.

In-house solution architects designed the BPNG sandbox, aiming to emulate—but not duplicate—many of the features found in the sandboxes of:

- the Australian Securities and Investment Commission (ASIC);
- Bank Indonesia;
- Bank Negara Malaysia;
- Bank of Thailand;
- Central Bank of Bahrain (CBB);
- Monetary Authority of Singapore (MAS);
- the UK's Financial Conduct Authority (FCA); and
- Hong Kong Monetary Authority (HKMA).

Technical advisers and subject-matter experts from the ADB provided quality assurance of this design. In addition, the BPNG entered into discussion with the six other members of the Pacific Islands Regional Initiative (PIRI) Financial Technology Regional Regulatory Sandbox (i.e., the central banks of Fiji, Samoa, Solomon Islands, Timor-Leste, Tonga and Vanuatu). As a result, the BPNG hopes that its own regulatory

sandbox will facilitate interoperability across jurisdictions in the future.

The BPNG will be welcoming interest in participation in its sandbox from any of the following, subject to their fulfilment of BPNG's entry criteria and principles:

- authorised financial institutions already active in PNG and hence already subject to BPNG's regulatory review;
- any institution not currently under BPNG's purview, but whose innovation is such that it may come to require licensing or regulatory approval;
- actors from outside the financial services sector who are developing solutions that can accelerate financial and social inclusion, in recognition of the relationship of financial services with industries such as technology, telecommunications and health care;
- local fintech developers, such as new entities in PNG that have developed or are developing solutions/concepts outside traditional business models with positive potential impact on inclusion; and
- overseas fintech developers, such as start-ups and other entities domiciled outside PNG that have developed or are developing solutions/concepts outside traditional business models that may represent new possibilities.

A communications and awareness programme was therefore targeted at members of PNG's National Payments Council first, then financial institutions and finally fintech developers.

To date, there has been no central government participation in the development of the BPNG regulatory sandbox.

10.1.5 Outcomes

Recognising its role in education, the BPNG has been active in ensuring that both government and industry engage with and are educated about key fintech concepts and their potential to drive financial inclusion. The BPNG convened and hosted the very first blockchain seminar in PNG and facilitated establishment of an industry body (the PNG Digital Commerce Association) in March 2019, which sponsored and facilitated the training of 24 locally recruited software developers in developing DLT-based solutions—another first for PNG.

In addition, the BPNG has attended and participated in two additional London blockchain hackathons and conferences, and been invited to speak at a large number of financial services forums across the world.

The BPNG regulatory sandbox originally and primarily targeted one of the Bank's key strategic business objectives: financial inclusion. In pursuing this objective, BPNG has aimed to:

- reduce financial transaction prices and service fees;
- provide a safe and protected environment for the design and testing of fintech innovations;

- make PNG more attractive to innovators and investors, and improve interoperability across jurisdictions; and
- protect consumers keen to use new technologies, but wary of risking their hard-earned savings.

Within nine months of the conclusion of successful testing in the sandbox, the BPNG requires participants to implement their solution in PNG. To do so, they must comply with PNG's regulatory framework, as would be the case had they not participated in the sandbox.

Applicants are then free to market their solution in any jurisdiction.

10.1.6 Conclusion

The BPNG takes pride in its leadership in exploring new technology for financial inclusion and is eager to push the boundaries and harness technology to improve financial inclusion in a challenging environment.

Case Study 10.2 Pioneering Mobile Money in Kenya

10.2.1 Introduction

This case study looks at Kenya's development of a mobile money solution known as M-Pesa, as a collaboration between both the public and private sectors, aiming to drive inclusion for its population.

Quick Facts

Country: Kenya

Population: 51.393 million

Gross domestic product (GDP), 2018: US\$87.908 billion/£71.470 billion

GDP per capita, 2018: US\$3,461.40/£2,814.10

Top three industries: agriculture; industry and manufacturing; services (wholesale and retail trade, transport, government, financial, professional and personal services)

Source: World Bank (2018). 'Kenya' [online]. Retrieved from: <https://data.worldbank.org/country/kenya>

10.2.2 Context

The Central Bank of Kenya (CBK) has set out a series of priorities around digital finance and the digital economy. These priorities emerged out of its work on promoting financial inclusion.

offered a prize of approximately £1 million for innovative solutions to the inclusion challenge. A consortium of private sector actors, including CBA Bank, Safaricom and various microfinance players, collaborated to propose M-Pesa.

10.2.3 Challenges/Problems

- When work on financial inclusion began, in the early 2000s, there was very limited access to formal financial services in Kenya: the country had a population of about 30 million, but only about 2.5 million had bank accounts.
- At that time, banks were closing branches and withdrawing entirely from rural areas, further restricting Kenyan people's access to financial services.
- In 2006, a financial access survey found that only 27 per cent of respondents had access to even basic formal financial services, such as for transferring money.

In the process of evaluating and creating the framework to support M-Pesa, CBK looked to the practices of a variety of other jurisdictions, including advanced economies such as the European Union, United States and Australia. The Bank found, however, that the situation in the Philippines was most closely analogous with its own and hence served as the most useful model in focusing on a similar set of issues with a similarly excluded population.

At the outset, the Kenyan government recognised that it did not yet have in place the regulatory framework necessary to support the solution. The government therefore enacted a package of legislation to create an enabling environment, including laws focusing on:

- anti-money-laundering (AML);
- consumer protection; and
- payments systems.

10.2.4 Policy Intervention

The Central Bank of Kenya (CBK) was initially supported in its efforts with seed funding from the UK's Department for International Development (DfID). In 2004–05, DfID

More recently, the government has moved to license many more players in the market to increase competition, promote interoperability between systems and most recently, in 2019, issue additional guidance regarding cybersecurity.

10.2.5 Outcomes

Financial inclusion in Kenya has soared from 27 per cent in 2006 to 82 per cent in 2019, according to the latest survey. The CBK also tracks, on a monthly basis, the number of accounts holding balances of mobile money, the number of agents helping to facilitate those accounts and other metrics showing that the intervention has actually integrated into daily life. In doing so, it takes care to look at meaningful activity rather than at 'zero balance bank account' inclusion—that is, at bank accounts held but not necessarily used.

The government has now begun to broaden the platform created by mobile money to align with other government objectives, such as digital finance and the digital economy. The enabling ecosystem and the CBK's supporting activities have evolved considerably over the years—and they continue to evolve. While the initial focus was on access, for example, the CBK is now looking at promoting usage and quality of service (QOS) while amplifying consumer protection.

10.2.6 Conclusion

Kenya's journey into mobile money revealed that the effective inclusion is not only about regulation and policy; both public and private actors must co-ordinate their efforts if inclusion is to be achieved. The public sector will create an enabling environment, but the private sector must invest in marketing, product development, distribution, consumer engagement and customer services, etc. The public sector

will take the lead on delivering digital infrastructure, while the private sector ensures continuous improvement of its products to meet continuously evolving customer needs.

As Kenya looks back at more than a decade of success and looks towards the next, it will be clear that mobile money is a foundation for a broader set of financial services. While the legacy focus has been on payments, a progressive plan will incorporate a broader set of higher-value financial services, such as credit, savings, insurance and pensions.

As this focus shifts, the needs that the products must meet become more sophisticated, reflecting more closely the everyday lives of Kenyans. For example, one of the biggest challenges for families is the concept of 'shocks'—that is, of unexpected events, such as a costly health emergency and/or long-term health issues that impact negatively on income. Traditional forms of health and other insurance are unlikely to meet the needs of those who have, until recently, been financially excluded; hence there is a need for public and private actors to explore financial flexibility and the potential ways in which fintech might be leveraged to deliver greater resilience to the household.

By looking more holistically at the framework, Kenya can now start to build on successfully established mobile money foundations to transform the lives of Kenyan citizens.

Case Study 10.3 Digital Assets Businesses in Bermuda

10.3.1 Introduction

This case study considers how the government of Bermuda has built a

supportive ecosystem in which businesses that focus on digital assets (such as

cryptocurrencies and other kinds of tokens built on blockchain) can thrive.

Quick Facts

Country: Bermuda

Population: 61,000

Gross domestic product (GDP), 2018: US\$6.127 billion/£4.981 billion

GDP per capita, 2018: US\$99,363/£80,783

Top two industries: international business (primarily financial services); tourism

Source: World Bank (2018). 'Bermuda' [online]. Retrieved from: <https://data.worldbank.org/country/bermuda>

10.3.2 Context

In 2017, Bermuda elected a premier who had a background in both information and communications technology (ICT) and economics. As one of his policy priorities, David Burt said that he wanted to make Bermuda more technology-friendly.

10.3.3 Challenges/Problems

Evaluating the Bermudian economy and finding space for diversification, the economic development arm of the Bermuda government began to explore new opportunities. Within the five years to 2017, token issuances had seen significant capital raised as the cryptocurrency market began to develop, but blockchain-related companies struggling to find jurisdictions friendly to these new types of security.

10.3.4 Policy Intervention

In September 2017, the Government of Bermuda established a task force dually focused on business development and policy, mandated with conceptualising ways

of helping fintech to develop. The premier and the minister of national security both attended Davos in January 2018, where they met with influential players, inviting several blockchain innovators to the island a few days later to map out the industry's needs.

A sandbox licence enables entrepreneurs to test an aspect of the business model if the entity is not yet sufficiently mature to seek a full licence.

In creating an enabling environment for fintech, Bermuda sought to leverage its long history in insurance and reinsurance. In that instance, the government had brought policy-makers, regulators and industry together to shape an environment to drive innovation and manage risk. It used this same approach to draft the Digital Assets Business Act 2018 (DABA).

The needs of the digital assets industry, on which the DABA centred, reflect the shifts that occur when new technology is applied to traditional finance. For example, new technology introduces cybersecurity risk, while new technology demands new approaches to compliance with global requirements such as know your customer (KYC) rules and rules countering the financing of terrorism (CFT). Custody risks that would formerly attach to traditional paper certificates are complicated by the unique characteristics of an asset that can be digitally copied or an asset that could be lost if cryptographic keys were lost.

The DABA anticipates that a business will contemplate business model risk, document its policies and procedures, and both (a) provide for risk mitigation and (b) respond effectively after a risk event occurs.

The DABA provides for a three-tier structure through which a digital asset business progresses.

At its apex is the **full licence**—available to a mature business such as Circle, which has been granted a full ‘Class F’ licence (one of five classes set out in the DABA).²

A **sandbox licence** is a modified licence with reduced scope and volume, granted to enable entrepreneurs to test an aspect

of the business model if the entity is not yet sufficiently mature to seek a full licence. An example would be a licence allowing a business to test its compliance policy under the close eye of the regulator.

In the very first instance, a business might participate in an **innovation hub**. At this stage, the business will not yet have fleshed out its business model or have proof of concept and while it wants to work closely with the regulator to develop both, it is not ready for the heavy constraints of the regulatory sandbox. The effect is that a start-up can begin to test its direction with the support and advice of the regulator, while minimising business model risk.

10.3.5 Outcomes

The DABA has been reasonably successful in generating interest from a number of companies. Several companies, including Circle, have successfully applied for licensing and the government has proposed amendments to the Act to bring derivative exchanges within its purview. While Bermuda came later to the fintech table than some jurisdictions, it has more confidence in longevity of the businesses that it is licensing because it has set a high bar in terms of risk management—a bar that is an industry benchmark.

10.3.6 Conclusion

Bermuda’s DABA is part of a multipronged fintech strategy that incorporates numerous elements aiming to foster growth within the financial services ecosystem. The government is already learning from its experiences, shaping amendments to the Act and consultation papers to refine the regulatory framework, on the one hand, and planning for other fintech-related initiatives, on the other.

Case Study 10.4 Malta's Support for Virtual Financial Assets

10.4.1 Introduction

This case study explores the series of regulations that Malta has passed

to support businesses engaged in the issuance and management of virtual financial assets (VFAs), such as cryptocurrencies.

Quick Facts

Country: Malta

Population: 483,530

Gross domestic product (GDP), 2018: US\$14.542 billion/€11.823 billion

GDP per capita, 2018: US\$42,567.20/€34,607.50

Top three industries: tourism; manufacturing; financial services

Source: World Bank (2018). 'Malta' [online]. Retrieved from: <https://data.worldbank.org/country/malta>

10.4.2 Context

Malta has been a notable banking centre for many years, offering the flexibility of a small state while complying with European Union (EU) regulatory standards. As digital assets such as cryptocurrencies emerged, the Maltese government sought to engage with this new segment of the financial sector to optimal effect.

10.4.3 Challenges/Problems

- Digital assets—or VFAs, as Malta terms them—are an emerging business and regulatory domain built on the technological innovation of blockchain.
- The international regulatory response to VFAs has been varied, with a high degree of uncertainty involved in the classification, regulation and oversight of the entities issuing these assets and the assets themselves.
- Entrepreneurs and investors have been seeking regulatory clarity and guidance

on compliance when working with VFAs.

10.4.4 Policy Intervention

On 30 November 2017, the Malta Financial Services Authority (MFSA) published a Discussion Paper on Initial Coin Offerings, Virtual Currencies and related Service Providers.³ This followed the general principles set out in a statement issued by the European Securities and Markets Authority (ESMA) on 13 November 2017.⁴ As the Discussion Paper explained, while certain initial coin offerings (ICOs), distributed ledger technology (DLT) assets—previously referred to as virtual currencies (VCs)—and related activities could fall within the scope of existing financial services legislation, others would be likely to fall outside that scope and hence be unregulated.

The Discussion Paper proposed a policy whereby the MFSA would create a high-level principles-based regulation—in line with the high-level objectives set out

supranationally—of ICOs and certain service providers (namely, intermediaries that act as brokers, exchanges, investment advisers and market makers) in relation to DLT assets that currently fall outside the scope of existing financial services regulation. The MFSA received ample positive feedback on the proposals and proceeded to draft the Virtual Financial Assets Bill. The Bill was enacted on 20 July 2018 and the Virtual Financial Assets Act came into force on 1 November 2018. The Act regulates the following activities when conducted in or from within Malta:

- the offering of a VFA to the public by an issuer;
- the application, by an issuer, for admission of a VFA to trading on a DLT exchange;
- the activity of a VFA agent; and
- the provision of VFA services.

On 4 July 2018, the MFSA published a Consultation Paper on secondary legislation to be issued under the Act (the Virtual Financial Assets Regulations), which set out detailed provisions on exemptions, fees, control of assets, and administrative penalties and appeals. The consultation closed on 20 July 2018 and, after feedback, the VFA Regulations were published on 2 November 2018.

Having set out the legislative and regulatory framework, the MFSA followed up with rules detailing its application to operators in this field of financial services. The MFSA's Virtual Financial Assets Rulebook comprises three chapters:

- Chapter 1 Virtual Financial Assets Rules for VFA Agents

- Chapter 2 Virtual Financial Assets Rules for Issuers of VFAs
- Chapter 3 Virtual Financial Assets Rules for VFA Service Providers

At the same time, the MFSA also consulted on achieving a higher degree of investor protection under the VFA Act and raising the bar for VFA agents.

One of the key points outlined in the MFSA's 2017 Discussion Paper was a Financial Instrument Test to determine whether a DLT asset, based on its specific features, is included in the scope of the existing EU legislation and corresponding national legislation or the VFA Act, or is otherwise exempt. In early 2018, the MFSA consulted on the test, which was to be applicable both within the context of an ICO and during the intermediation of DLT assets in or from within Malta.

When published on 13 April 2018, the Financial Instrument Test was accompanied by detailed guidance.⁵

Further guidance followed in 2019:

- Guidance Notes on Cybersecurity, as a minimum set of best practices and risk management procedures to be followed to effectively mitigate cyber risks; and
- Guidance for Credit Institutions, Payment Institutions and Electronic Money Institutions opening accounts for FinTechs.⁶

Anti-Money-Laundering (AML) and Countering the Financing of Terrorism (CFT) Rules

VFAs In relation to anti-money-laundering (AML) and countering the financing of terrorism (CFT) rules, VFA agents, issuers

and licence holders are all considered to be 'obliged entities' under Malta's Prevention of Money Laundering and Funding of Terrorism Regulations 2018 (PMLFTR).

The Maltese national framework goes beyond what is provided for under the EU's Fifth Money Laundering Directive (5AMLD).⁷ Whereas 5AMLD defines obliged entities as only (a) custodian wallet providers and (b) providers engaged in exchange services between virtual currencies and fiat currencies (leaving crypto-to-crypto exchanges outside of its scope), the Maltese framework defines obliged entities as VFA agents, VFA issuers and VFA service providers, including exchanges and service providers involved in VFA-to-VFA transactions.

The MFSA has introduced the role of VFA agent as an additional AML/CFT filter to ensure that the national financial system is secured. Indeed, those who can be appointed as VFA agents will already have a good understanding of these AML/CFT obligations, and will be able to guide both VFA issuers and VFA licence holders in terms of their legal obligations.

Forthcoming guidance will both explain how these different crypto asset operators are to meet their AML/CFT obligations and highlight particular risk factors and red flags that might emerge during risk assessment or when monitoring customer activity. For example, in relation to VFA, issuers and licence holders:

- must apply customer due diligence whenever interaction between a customer and a VFA issuer or licence holder is characterised by only occasional transactions; and
- must have systems in place to verify the origin of any VFAs they accept from

customers (e.g., to check whether these assets have ever been used on the dark Web or as ransomware).

As obliged entities, VFA agents, issuers and licence holders have ongoing obligations to monitor any business relationships they establish. Moreover, independently of that monitoring, all three also have reporting obligations to the Financial Intelligence Analysis Unit (FIAU) that are triggered whenever they suspect that:

- a transaction involves the proceeds of criminal activity or is related to the funding of terrorism; or
- a person may have been, is or may be likely to be connected with money laundering or the funding of terrorism.

DLT Assets Other than VFAs To the extent that a DLT asset does not qualify as a VFA but as either a financial instrument or electronic money, any provider of a related service (i.e., investment services and electronic money institutions) will also be considered to be an obliged entity. This means that they too must abide by the PMLFTR and submit reports to the FIAU.

Malta Digital Innovation Authority (MDIA)

Mandated by the Malta Digital Innovation Authority Act 2018, the Malta Digital Innovation Authority (MDIA) is an autonomous public body established with objectives that blend consumer protection and business development in the field of innovative technology arrangements and services (ITAS). The MDIA Act vests the MDIA with functions that include regulation, supervision, policy, education and business development. Within the context of the regulation of VFAs, the MDIA is the competent authority under the Innovative Technology Arrangements and Services Act

2018, which provides among other things for the authorisation of systems auditors, who have a specific role in ITAS cybersecurity.

As was the case with the VFA Act, a set of guidance notes aims to help ITAS providers when approaching the MDIA for registration and certification. The guidelines clarify and explain some of the processes, and reflect questions asked during public consultation, helping to increase stakeholder engagement.

10.4.5 Outcomes

While Malta's VFA activities are relatively new, they are stirring excitement among the blockchain entrepreneurial community, and some companies are either taking steps to domicile in Malta or contemplating registration and certification there, with positive potential impact on Malta's economy.

10.4.6 Conclusion

If small states are to take advantage of emerging market opportunities with meaningful financial corridors, they require a sophisticated regulator and a system of continuous improvement that allows them to respond as the emerging technology intersects with an emerging area of international regulation. Malta, in particular, is a model of best practice, straddling both the Commonwealth and the EU, and engaging in ongoing dialogue with regulatory bodies in each of these domains, as well as other authorities and international co-operating bodies (such as the Organisation for Economic Co-operation and Development,

or OECD), aiming to harmonise its response and regulatory framework with international standards.

Endnotes

- 1 BPNG (2014). *Strategic Plan: Bank of Papua New Guinea—2016–2020* [online]. Retrieved from: www.bankpng.gov.pg/wp-content/uploads/2014/06/Final-BPNG-Strategic-Plan-2016-2020.pdf
- 2 Pitcher D (2019). 'Premier Announces that Circle Has Achieved a Digital Asset Business License'. *FinTech Bermuda*, 22 July [online]. Retrieved from: <https://fintech.bm/premier-announces-that-circle-has-achieved-a-digital-asset-business-license/>
- 3 MFSA (2017). *Discussion Paper on Initial Coin Offerings, Virtual Currencies and Related Service Providers* [online]. Retrieved from: www.mfsa.mt/publication/discussion-paper-on-initial-coin-offerings-virtual-currencies-and-related-service-providers/
- 4 ESMA (2017). 'ESMA Alerts Firms Involved in Initial Coin Offerings (ICOs) to the Need to Meet Relevant Regulatory Requirements'. Statement, 13 November [online]. Retrieved from: www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf
- 5 MFSA (undated). 'Guidance' [online]. Retrieved from: www.mfsa.mt/fintech/virtual-financial-assets/guidance/
- 6 *Ibid.*
- 7 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, 19 June 2018, OJ L 156/43.

Appendix 1

Commonwealth Government Interviews

We conducted interviews in August and September 2019 with Commonwealth nations to ensure that the Commonwealth FinTech Toolkit meets the needs of its intended audience of policy-makers and regulators, with a focus on central banks. While interviews were typically with central bank officials, in some nations another body took the lead role in fintech, such as the Malta Financial Services Authority in Malta, so we interviewed these instead. Two Commonwealth Central Bank Governors (CCBGs) participated directly (Papua New Guinea and Namibia). A further discussion was held with British Overseas Territory Bermuda, leading to a case study that is incorporated into the full Toolkit document (Case Study 10.3). The Bahamas wished to participate, but had to deal instead with the effects of Hurricane Dorian and hence may be included in a future version of the Toolkit.

The participating countries were:

- Australia
- Bangladesh
- Barbados
- Botswana
- Canada
- Cyprus
- Eastern Caribbean Central Bank
- Mauritius
- Namibia
- New Zealand
- Papua New Guinea
- Samoa
- South Africa
- Trinidad and Tobago

- Kenya
- Malawi
- Malta
- United Kingdom
- United Republic of Tanzania

Generally speaking, the 19 participating countries expressed a great deal of enthusiasm, validating the need for the Toolkit and its proposed scope.

The interview cohort was diverse in terms of geography, size of country and stage of economic development. The relevant demographics (excluding Bermuda) are as follows.

- **Region** Seven African countries; four countries from the Americas (including the Caribbean); five Asia Pacific countries; three European countries
- **Population size** Ten countries with populations of <5 million and nine countries with populations of >5 million; a population range from 0.2 million (Samoa) to 163 million (Bangladesh), with a median population size of 5 million
- **Economic size** (in gross domestic product, or GDP) Ranging from US\$1.2 billion (Samoa) to US\$3.1 trillion (United Kingdom), with a median economic size of US\$18.6 billion (Botswana)

Most participants felt that the Toolkit, as proposed, would cover material appropriate for their needs. Some felt it would be useful

for building internal capacity, while a few felt that it would be useful to educate colleagues, not only within their agency or bank, but also in other government agencies and ministries. Almost three-quarters (74 per cent) expressed interest in blended learning on how to use the Toolkit—to be delivered at University of Oxford and online to different constituencies.

The remits of the participants ranged from monitoring and compliance (narrow focus) through to economic development and proactive ecosystem building (wide focus).

Sandboxes, digital financial services and digital currencies (including central bank digital currencies) stood out as topics that interview subjects requested and which were not originally contemplated for specific attention in the draft report.

Interview Questions

About You and Fintech

- 1 What are the top three to five strategic priorities at the central bank?
- 2 Have you engaged in a formal fintech policy process?
- 3 Do you have a fintech specialist and/or team within the central bank?
- 4 If you have set specific policy objectives with respect to fintech, what are they?
- 5 Has your team engaged in formal training regarding fintech policy? If so, which programme(s)?

- 6 If you have implemented policies with respect to fintech, what are they? Have they achieved the results you hoped for?

About the Fintech Policy Toolkit

- 7 Does the proposed Toolkit cover the key areas around which you have questions?
- 8 Are there topics that you want the Toolkit to cover that we have not proposed?
- 9 Who in your organisation do you feel would be best served by the Toolkit?
- 10 How involved do you want to be in the design process of the Toolkit?
- 11 If training is offered on implementing fintech policy and using the Toolkit, how many people from your organisation do you think you would want to participate?
- 12 Would you like training to be delivered (a) in person at University of Oxford, (b) digitally (online) or (c) both (for example, with more senior people receiving in-person training and more junior people getting digital training)?
- 13 Is there anything else you would like us to be thinking about as we build the Commonwealth FinTech Toolkit?

Appendix 2

Methodology

We conducted a combination of primary and secondary research.

Primary research comprised interviews with the Commonwealth Central Bank Governors (CCBGs) or their teams, as well as select other government authorities on a state-by-state basis (e.g., the discussion with Malta was held with the Malta Financial Services Authority).

We contacted 47 CCBGs by email and had a 35 per cent response rate. In total, we conducted interviews with 19 central banks or equivalent authorities.

Of these 19 interviews, 9 were of Commonwealth nations with more than 5 million population and 10 were of Commonwealth nations with less than 5 million population.

The geographic spread is as follows.

Region	%
Africa	36.8
Americas	5.3
Asia	5.3
Caribbean	21.1
Europe	10.5
Pacific	21.1

The populations of these nations ranged from 71,000 in Bermuda to 162 million in Bangladesh, and the economies (measured in GDP) ranged from US\$1.2 billion in Samoa to US\$3.1 trillion in the United Kingdom.

In this way, we gathered a wide range of perspectives and data from a representative range of Commonwealth nations. The list of interview questions used is set out in Appendix 1.

We conducted secondary assessments of academic research, corporate and think tank research reports, and information from thought leaders in the fintech and financial services areas. It should be noted that, given how relatively new fintech is and the rapid pace of change in the space, the information gathered from non-academic sources is valuable.

Appendix 3

Findings

The 19 Commonwealth countries interviewed demonstrated diverse approaches, capacity, resource allocation and focus around fintech. Some governments take a monitoring or evaluative approach, while most were developing some kind of policy response to or framework around fintech if they had not already taken meaningful policy action. Virtually all those interviewed felt that a Toolkit would be an important resource to help with their day-to-day work and some felt that it also could assist in building capacity in other government departments. The participants expressed desire to build capacity around the Toolkit in both digital and in-person formats.

Key statistics

% of the central banks who have engaged in formal fintech policy development

Yes	65
No	29
N/A	6

% of the central banks who have a fintech policy specialist

Yes	59
No	35
N/A	6

% of the central banks who have engaged in formal fintech policy/fintech-related training

Yes	29
No	65
N/A	6

In terms of building capacity around fintech generally and the use of the Commonwealth FinTech Toolkit in particular, 74 per cent of central bank respondents noted a preference for a blended learning approach to formal training. Some organisations believed that the Toolkit could be useful not only for building capability within the core fintech groups at the central bank or monetary authority, but also for educating a wider array of colleagues in multiple government departments on the issues, risks and opportunities of fintech.

% of the central banks who agree that the proposed Toolkit covers all key areas relevant to them

Yes	59
No	29
N/A	12

Contributors and Acknowledgements

Commonwealth Secretariat Sponsor

Senior Director: Prajapati Trivedi, Economic, Youth and Sustainable Development Directorate

Project Lead: Travis Mitchell

Secretariat Team Members: Heather Cover-Kus, Motselisi Matsela, Wonderful Khonje

Visionary Future

Visionary Future Commonwealth Ltd., a subsidiary of Visionary Future LLC, partners with governments and the private industry to build a better tomorrow through technology applications, with a particular focus on fintech (including blockchain), artificial intelligence, big data/big data analytics and cybersecurity. Visionary Future creates thought leadership, including online courses and books, conducts workshops and seminars, develops and implements strategic plans, and provides interim management capacity to support these activities. Clients have included the

European Commission, the Government of Dubai and various private companies. More information is available online at VisionaryFuture.com.

Project Lead: David Shrier, Managing Director, Visionary Future LLC

Project Contributors: Adele Jashari, Jane Thomason, Deborah Webster, Alfie van der Zwan

Acknowledgements

We would like to gratefully acknowledge the contributions of more than 50 leaders from central banks, government ministries, large incumbent financial institutions, fintech start-ups and academia who participated in the series of consultation workshops and seminars that led to the creation of this Toolkit.

We would also like to thank the Government of Australia, Department of Foreign Affairs and Trade for their generous financial support for this project.

The emergence of technology-enabled financial services (fintech) in the past two decades has profoundly impacted the production and delivery of financial services.

The Commonwealth FinTech Toolkit provides technical guidance on fintech and fintech applications. It sets out a framework for creating enabling environments for fintech, through legislation, regulation, institutions and policies. It also aims to build fintech capacity among government staff.

Part I considers the ways in which emerging technologies are transforming financial services. Part II explores how Commonwealth member countries can use those technologies to achieve their development goals.

