IFWG

INTERGOVERNMENTAL FINTECH WORKING GROUP

FINTECH WORKSHOPS

03/04 September 2019

FIC Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Contents

Acronyms and abbreviations

ABIS	Automated Biometric Identification System
AI	Artificial Intelligence
API	Application Programming Interface
ASISA	Association of Savings and Investments South Africa
CBDC	Central Bank Digital Currency
CDD	Customer Due Diligence
CSIRT	Computer Security Incident Response Team
DCDT	Department of Communication and Digital Technologies
DHA	Department of Home Affairs
DLT	Distributed Ledger Technology
EFT	Electronic Funds Transfer
EU	European Union
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
Fintech	Financial Technology
FSPs	Financial Services Providers
FSRA	Financial Sector Regulatory Act
GSMA	Global System for Mobile Communications Association
HANIS	Home Affairs National Identity System
ICT	Information and Communication Technology
ID	Identity
ID4D	Identification for Development
Insurtech	Insurance technologies
IFWG	Intergovernmental Fintech Working Group
IR	Incident Response
ISFTOV	Irrevocable, Simultaneous, Final Transfer of Value
KYC	Know Your Customer
mPOS	Mobile Point Of Sale devices
MSMEs	Micro, Small, and Medium Enterprises
PASA	Payments Association of South Africa
PMJDY	Pradhan Mantri Jan-Dhan Yojana
PSD2	Payment Services Directive
SADC	Southern African Development Community
SARB	South African Reserve Bank
SSI	Self-Sovereign Identity
UIDAI	Unique Identification Authority of India
STEM	Science, Technology, Engineering and Mathematics
UK	United Kingdom
US	United States
USD	United States Dollar

Foreword from the IFWG

In April 2018 the Intergovernmental Fintech Working Group (IFWG) hosted its inaugural workshop, an outreach that signalled the importance of financial technology (fintech) to South Africa and South African regulators. At this workshop there were two outcomes we undertook to pursue: the first being another IFWG workshop during 2018, as well as an innovation policy framework during 2019. The IFWG, in the 2018 workshop, put its focus on obtaining inputs on three significant topics, namely crypto assets and Initial Coin Offerings (ICOs), financial inclusion and innovation facilitators.

We are pleased to report that we have made good progress based on those undertakings. In 2018 the IFWG hosted a focussed industry workshop on crypto assets and in January 2019 issued the first crypto assets paper which is to be followed up during the first quarter of 2020 with a policy framework positioning how South African regulators propose to deal with crypto assets into the future.

This post-workshop booklet documents the important conversations and input from the sector on a range of fintech issues which formed the basis for six different workshops hosted by the IFWG at the Sandton Convention Centre on 3 and 4 September 2019. One of those workshops was on innovation where the IFWG reported back on the second undertaking on an innovation facilitation framework made at the 2018 workshop. The IFWG expended significant effort, between the 2018 inaugural workshop and the September 2019 set of workshops in designing an Innovation Hub for South Africa, a cross regulator capability to support inclusion and innovation for growth and the design of the IFWG Innovation Hub was launched at the workshop with very positive response from delegates.

The fact that the 2019 event was broken up into six different workshops is indicative of the pace and scale of change and the wide range of issues facing the sector and regulators. Whilst we were not able to deal with all fintech issues we selected those that we believe to be a priority in terms of their potential to reshape the financial services industry by removing market inefficiencies.

Engagement with delegates throughout the workshops highlighted other fintech areas for discussion and focus and these will be borne in mind for future IFWG engagements which we undertake to continue to host to enable responsible regulation with meaningful input from the sector.

A lot of work goes into planning an event of this nature and the IFWG would like to thank the event organisers, the communications and branding teams and each one of the workshop leaders for all your input and effort in ensuring the success of the workshops. Sincere gratitude is also extended to all presenters, panellists and discussants for their expert input and their willingness to be forthright and open during the sessions. Without your contributions, the sessions would not have been a success. We have made every effort to document herein all-important actions which are important to follow through on and on which financial regulators should pay attention to in the forthcoming year and in formulating policy positions and regulatory frameworks.

Introduction

South Africa's financial services sector is internationally recognised for its sophistication. Although the financial technology (fintech) sector is still small relative to international fintech hubs, fintech developments have accelerated in recent years, and have the potential to change the face of South Africa's financial services sector. Innovators are not the only stakeholders disrupting the financial services sector; industry incumbents are also pursuing the potential opportunities offered by new technologies. Regulators are investigating ways to improve how they engage with the sector and how to incorporate new technologies to improve competition and access to financial services for all South Africans.

This relentless technology march requires an equally relentless regulatory march. A clear and coordinated regulatory response is necessary to manage the risk and opportunities that the infusion of technology and finance create. The system’s operational resilience, as well as its susceptibility to cyber and financial crime, are becoming much greater matters of concern for firms and regulators alike. In recognition of these potential challenges, it is important that regulators take a balanced view on risks and to craft regulation and supervision in a way that ensures risks are appropriately mitigated.

At the same time, regulatory responses to manage risk need to avoid creating barriers to responsible innovation as these technologies present significant opportunities for improved efficiency, reduced costs, and better coverage of underserved customers. However, South Africa's start-ups face a number of barriers, including a limited funding environment and difficulty in navigating the financial sector's regulatory requirements. Providing clarity on regulatory requirements and addressing the regulatory barriers experienced by start-ups and incumbents will allow South Africa to fully leverage the potential benefits of developments in financial technologies.

Workshops overview and objectives

Recognising that the pace of change and scale of impact of fintech requires a coordinated approach, the Intergovernmental Fintech Working Group (IFWG) was formed at the end of 2016 as a joint initiative between South Africa's financial sector regulators and policy makers. The overall objective of the IFWG is to foster fintech innovation while ensuring a continued efficient functioning of financial markets, financial stability, and protecting the rights and interests of customers and investors.

As part of this approach, the IFWG hosted its 2019 workshops on 3 and 4 September 2019, which provided a platform for regulators, policymakers, industry incumbents and product innovators to engage on emerging fintech developments and what they mean for South Africa. Much of the dialogue centred on the potential of fintech to promote financial inclusion and enable South Africa to achieve its broader development objectives, including the policy and regulatory responses necessary to facilitate and manage the risks associated with this process.

Ultimately, the workshops aimed to provide clarity on the priority areas on which to focus regulatory responses to emerging fintech innovations, and how regulators and supervisory bodies can develop a coordinated, holistic, and enabling regulatory framework. To this end, the workshops consisted of six full-day workshops, including three sessions per day over two days and covered the following themes:

1. **Innovation for economic growth in the digital future:** this session aimed to create dialogue around fintech innovations and how stakeholders can partner to facilitate innovation in South Africa. The session reviewed key barriers to innovation and how regulatory and policy changes can address barriers.
2. **Digital identity:** delegates explored how to develop and implement seamless and secure ways to accurately identify customers served via digital channels. It was acknowledged that it is fundamental to protect the system against cybercrime and fraud. A key consideration of this discussion was how to add a layer of authorisation and authentication without opposing the rising customer expectations for fast, frictionless digital services.
3. **Harnessing Artificial Intelligence (AI) for economic growth:** this session facilitated dialogue around the existing and planned applications of AI technology, how these technologies can support the financial services sector and developmental objectives more broadly, as well as the governance frameworks and security processes necessary to protect consumers.
4. **Cybersecurity:** during this session, delegates discussed the global threat of cybersecurity and South Africa's experiences to date. A focal point of the discussion related to measures that financial institutions and government can take to prevent, detect and respond to cyber threats.
5. **Central Bank Digital Currency (CBDC):** CBDCs are a rapidly evolving area for innovation. This session investigated the potential benefits and risks associated with CBDCs in general, as well as the feasibility and appropriateness of issuing CBDCs in the context of South Africa.
6. **Open banking:** open banking is forcing banks to reconsider the way they think about financial services and is poised to reshape banking as it’s understood today. During this session, delegates reviewed global shifts towards open banking, and South Africa's experiences to date.

IFWG

INTERGOVERNMENTAL FINTECH WORKING GROUP

FINTECH WORKSHOPS

03 September 2019

Innovation for economic growth in the digital future

Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Innovation for economic growth in the digital future

Investing in and supporting innovation is important to ensure global competitiveness and economic growth. In this workshop, delegates began by questioning appropriate definitions to capture the true meaning of innovation. Armed with a shared understanding of innovation, delegates then explored innovation trends, both globally and in the context of South Africa. This conversation revealed advancements in financial technologies to date, emerging opportunities, as well as the critical barriers that South Africa needs to address in order to continue supporting innovation. Finally, delegates agreed that there is a need for more stakeholders to come to the table, both from the public and private sector, to create an enabling environment for innovation in South Africa.

At a glance

The innovation workshop created a space to discuss the enablers of, and barriers to, innovation in South Africa. The workshop revealed the following:

- While South Africa has a world class financial sector, fintechs struggle to navigate the complex regulatory environment.
- To support fintechs and enable innovation, South Africa is developing a multi-regulator Innovation Hub.
- However, other barriers remain, including limited skills and financing for innovation.
- Delegates agreed that stakeholders need to coordinate and leverage resources to facilitate innovation in South Africa.
-Ultimately, innovations aim to solve for human needs. This was a common thread throughout the workshops.

Definitions and frameworks

The rate of financial services innovation has prompted incumbents, regulators and disruptors alike to reflect on what exactly is innovation. In the (draft) White Paper on Science, Technology and Innovation, South Africa's Department of Science and Technology defined innovation as, *"the implementation of a new or significantly improved product (good or service) or process, or a new marketing method, or a new organisational model in business practice, workplace organisation or external relations."*[1]

While this definition is reasonable, delegates expressed that too often innovation is thought of as a *new* solution, overlooking the way in which innovation includes the application of existing products or processes in new contexts or in response to different challenges. Instead, thinking should be focused on the fundamental need that the innovation aims to address and consider different mechanisms to address those needs. In doing so, South Africa will be well placed to deliver innovative solutions to social challenges and ensure economic growth in the digital future.

Fintech innovation: What is happening globally

According to a study by Accenture, global investment in fintech ventures more than doubled from 2017 to 2018, increasing from USD 26.67 billion to USD 55.33 billion. During this period, the number of investments increased by 18.5% to 3,251.[2]

While governments globally have made an effort to introduce policies and regulations to respond to the increase in fintech innovation, legislative changes have been unable to keep up with the pace of change in the fintech industry. However, delegates argued that Facebook's Libra announcement (a proprietary crypto currency managed by the Libra Association, which Facebook forms part of) has accelerated national governments' responses to innovations in fintech[3]. On this, an Executive of the European Central Bank was quoted as saying, *"Libra is a meaningful fintech development which should not be allowed to enter into a regulatory void. The market is evolving quickly, and regulators must respond."*

[1] Department of Science and Technology, Republic of South Africa. Draft White Paper on Science, Technology and Innovation. 2018. Available: https://www.gov.za/sites/default/files/gcis_document/201809/41909gon954.pdf.

[2] Accenture. (2019). Global Fintech Investments Surged in 2018 with Investments in China Taking the Lead, Accenture Analysis Finds; UK Gains Sharply Despite Brexit Doubts. Available: https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm

[3] Since the workshop, a number of developments have brought into question the viability of Libra. Notably, the Group of Seven (G7) countries have warned that Libra is unlikely to receive regulatory approval as it poses a risk to the global financial system. Payments giants Visa and Mastercard have since withdrawn their support for the project. Szu Ping Chan. Facebook's digital currency dealt another blow. BBC. 14 October 2019. Available: https://www.bbc.com/news/business-50037223.

For example, following the Libra announcement, China announced that it will be launching its own CBDC (Central Bank Digital Currency). China's response to fintech innovations is discussed further in the case study below.

Case study 1: China's response to fintech innovations

China has been at the forefront of fintech growth in the past decade, enabled by the country's protectionist policies as well as the regulator's 'wait and see' approach[4] to fintech innovations.

Peer-to-peer (P2P) lending is one fintech innovation that flourished in China due to the open regulatory environment and demand for credit among small and medium enterprises. As a result of ongoing turbulence in this industry, however, delegates noted that China has undergone a regulatory overhaul in the P2P industry.

Digital payments have also experienced significant growth in the Chinese market, with non-bank payment systems making up the majority of transactions. One delegate argued that this growth in non-bank payments is one of the factors that prompted the Chinese government to explore CBDC, as traditional methods of monitoring the financial system no longer provided a good picture of what is happening in the Chinese economy.

Facebook's Libra announcement has further accelerated the Chinese central bank's research into creating its own digital currency, due to concerns over monetary policy and financial stability. CBDCs are discussed further in the Central Bank Digital Currencies section below.

Whereas China previously adopted a 'wait and see' attitude, the overwhelming pace of change in fintech innovation has since prompted a more proactive approach from the Chinese government. Many delegates argued that South Africa should learn from China's experience and similarly adopt a proactive response to innovations in the fintech sector.

Fintech innovation: South Africa

South Africa has a small but fast-growing fintech industry.[5] In recognition that understanding this industry is an important first step in developing evidence-based policies and facilitating solutions-oriented engagements between stakeholders, the South African National Treasury and World Bank commissioned a fintech scoping study in South Africa. The World Bank presented the preliminary findings from this study at the workshop.

There are an estimated 218 active fintech[6] companies operational in South Africa, across eight market segments. These segments include: payments, lending, savings and deposits, insurtech, investments, financial planning and advisory, capital raising, and business-to-business tech providers. The payments segment is the most mature of these segments, with 30% of the active fintechs operating in this market segment.

According to the study, some of the key challenges experienced by fintechs include: limited communication avenues with regulators; a challenging environment to test and scale fintech ideas; limited peer-to-peer collaboration; the lack of support structures; and challenging licencing requirements. Regulatory-specific requirements are discussed further in the section below. When the World Bank asked the audience whether any of these findings were surprising, or any important points were missing, the audience confirmed that the findings were consistent with their experience of the

[4] The 'wait and see' approach is a watchful approach whereby regulators observe and learn about emerging innovations to understand potential consequences for regulation. This is done while innovations remain, "sufficiently immature that we are not placing our objectives, stability, protection and integrity, at risk by not taking action." Securities Finance Monitor. ESMA's approach to fintech, 'wait and see' on DLT and crypto assets. 2018. Available: https://finadium.com/esmas-approach-to-fintech-wait-and-see-on-dlt-and-crypto-assets/.

[5] In this study, fintechs were described as those which, "were founded in the last 11 years, are not born out of the corporate structures of any incumbent financial services provider, and currently, have a physical presence to serve South African clientele." Staatssekretariat fur Wirtschaft (SECO), The World Bank, South Africa National Treasury, IFWG, Genesis Analytics. Fintech Scoping in South Africa. (Forthcoming).

[6] In this context, fintechs are considered as start-up companies that were formed outside of corporate structures post 2008 and are technology innovators building products for use in financial services.

sector. As this sector continues to grow, it is important that policies and regulations keep pace to sustain an enabling environment for innovation.

South Africa’s current regulatory framework

Fintechs are subject to financial regulations which ensure that financial transactions are secure and ultimately aim to protect consumers and prevent systemic risk. These regulations are technology agnostic and targeted at the underlying financial activity. Some of the key regulation and licencing requirements in the financial sector include:

- Financial Sector Regulation Act 9 of 2017;
- Financial Advisory and Intermediary Services Act 37 of 2002;
- National Payment Systems Act 78 of 1998;
- National Credit Act 34 of 2005;
- Banks Act 94 of 1990;
- Insurance Act 18 of 2017; and
- Financial Markets Act 19 of 2012.

Start-ups face many resource constraints which limit their ability to navigate this regulatory environment. Some of the fintechs at the workshop noted that it can be challenging to access reliable and cost-effective legal advice on the licencing requirements to go to market, which ultimately limits their ability to quickly go to market and to attract good investment. As a result of this complex regulatory framework, it is challenging for new and small innovative players to enter the sector, which ultimately exacerbates frustrations toward regulators. Delegates argued that government should strike a better balance between protecting consumers and regulations that ultimately embed incumbents and set up barriers to entry for new, innovative businesses.

On the other hand, regulators are mandated with protecting consumers and predicting and managing potential negative second order consequences of legislative changes. The IFWG was formed at the end of 2016 in order to foster fintech innovation while ensuring the continued efficient functioning of financial markets, financial stability and protecting the rights and interests of customers and investors.

Guided by international best practice, the IFWG is currently in the process of developing a *multi-regulator* Innovation Hub. The Hub aims to facilitate innovation and will include a Regulatory Guidance Unit, an Innovation Accelerator, as well as a Regulatory Sandbox. Whilst the Innovation Hub is still under development, a number of objectives have been identified for each unit within the Hub.

The Innovation Hub will be made up of **Regulatory Guidance Unit**, **Regulatory Sandbox** and an **Innovation Accelerator**. The Regulatory Guidance Unit will provide informal, non-binding information to steer entities requesting assistance and clarity in navigating the financial services regulatory landscape. The Regulatory Sandbox will be a controlled environment that offers regulatory relief to test innovative products and services within predefined parameters and timeframes. The Innovation Accelerator will focus on exploring innovation that can improve the regulatory environment as well as innovation that can transform the broader financial services landscape. Regulators will continue to develop an Innovation Hub to advance responsible innovation that supports consumer protection, market integrity and stability.

Ultimately, these mechanisms aim to bring regulatory clarity and appropriately regulated financial services enabled by innovative technologies. On this, one regulator noted, "*Importantly, the sandboxing and innovation accelerator will allow us to understand how and where regulations could be creating a barrier, which can show where [regulatory] changes are necessary."*

While the Innovation Hub and IFWG represent material steps toward creating an enabling environment for innovation in South Africa, legislative changes are necessarily slower moving, in comparison to the 'fail fast' ethos of innovators. Increased collaboration and transparency between these stakeholders may reduce the divide, and the workshop created a venue for learning and exchange of ideas. Start-ups provided suggestions to regulators in order to improve the process of change around the Innovation Hub. For example, delegates argued that taking the Innovation Hub to market at a minimum viable product stage, and then learning and adapting based on experience, may help the Hub embody the ethos of the innovators it is aiming to facilitate.

Gaps and barriers to fintech innovation in South Africa

Bridging the skills gap

Delegates expressed concern as to whether South Africa's education ecosystem is equipping individuals with the knowledge and skills necessary to take advantage of emergent opportunities. Micro-credentialing institutions offer opportunities for accelerated, demand-driven learning and present an opportunity to close the skills gap. However, micro-credentialing institutions are not recognised under the national qualification framework or Sector Education and Training Authority accreditation framework. This limits the opportunity for South Africans to quickly build their digital skills in a way that is not prohibitively expensive for lower income groups.

According to these delegates, increasing emphasis on Science, Technology, Engineering and Mathematics (STEM) disciplines in schools and expanding accreditation frameworks are important in ensuring that South Africans have the knowledge and skills necessary to leverage emerging opportunities in the digital age.

Financing for innovation is limited

The amount of financing available for start-ups is limited in South Africa and is largely geographically limited to companies in the Western Cape and Gauteng province. Due to funding limitations, investors must focus on fewer, quality opportunities with a higher probability of success. This often diverges from the more enabling seed stage funding provided in the developed markets, where even companies that do not have a clear probability of success can receive funding. As a result of limited resources at the seed stage, many start-ups either fail entirely or are unable to achieve the scale necessary to access more traditional forms of capital.

While the Section 12J tax incentive has encouraged new funds with venture capital investments in start-ups, it excludes investments in financial services and advisory services companies. As a result, fintechs are restricted from accessing financing through this channel. Additionally, it has been difficult to maintain momentum in investing in start-ups. This is largely due to the lack of economic and policy stability necessary to assist in attracting both local and foreign capital.

Conclusion: the role of government in facilitating innovation

Given the constraints and opportunities for fintech innovation in South Africa, how best to facilitate innovation was a key focal point for much of the discussion during the Innovation session. Rather than taking a 'wait and see' approach, which is reactive in nature and delays regulatory change until emerging trends are fully understood, delegates emphasised a resounding need for government to be proactive in creating an enabling environment for fintech innovation. There was overwhelming agreement that the Innovation Hub is a promising example of proactive government action to ensure that regulation keeps pace with emerging innovations.

At the same time, however, delegates recognised that regulators cannot facilitate innovation independently; regulatory authorities and policy makers are at risk of being overloaded by the extent of activities necessary to facilitate innovation in the long term without support from other stakeholders. To create an enabling environment in South Africa and take advantage of opportunities, private and public sector actors need to collaborate and pool human and financial resources in order to facilitate innovation. Delegates argued that while isolated efforts are taking place, stakeholders need to identify complementarity capabilities and pool resources to leverage opportunities and drive a greater innovation agenda. In this context, the government can play a critical coordinating role:

> *"The state must understand the leadership necessary in each context, and how to crowd in relevant stakeholders. Then, like playing music in an orchestra, the state should determine how the actors can play off the same sheet, and be the conductor indicating when to make the music required of them. The entrepreneurial state is the conductor of innovative and entrepreneurial activity."*

IFWG

INTERGOVERNMENTAL FINTECH WORKING GROUP

FINTECH WORKSHOPS

03 September 2019

Digital identity

Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Digital identity

Being able to prove one's identity is increasingly recognised as the basis for participation in economic, social, political, and cultural life. Digital identification (digital ID) can be authenticated unambiguously through digital channels. As a result, digital identity presents the opportunity of unlocking access to banking, government benefits, education, and many other critical services for communities, that have traditionally been un/underserved, in developing countries.

While South Africa has started a journey to a digital ID system, countries across the continent are at different stages of developing out their national identity systems. From the workshop, it became clear that in order to harness the potential of digital identity, countries need to work on having secure national identity systems that cover the population from birth to death. These are necessary in order to make it easier for incumbent and new financial and non-financial service providers to on-board and better serve new and existing customers. Finally, both public and private organisations also need to work together to promote an interoperable identity ecosystem that supports innovation but also maintains the privacy and safety of customer data.

At a glance

During the digital identity workshop, delegates explored the benefits and challenges related to digital identity, and global progress in this regard.
- While identity systems enable access to economic and financial services, traditional paper-based methods are subject to error. Digital identity can solve for this challenge.
- South Africa is among a number of governments worldwide that are pursuing or have fully implemented digital identity systems.
- However, governments need to investigate means of ensuring privacy and data protection for these centralised systems.

Box 1: Defining digital identity[7]

Digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities.

A person's digital identity may be composed of a variety of attributes, including biographic data (e.g. name, age, gender, address) and biometric data (e.g. fingerprints, iris scans, hand prints, facial recognition) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual. When these data points are collected and verified, they can be used to identify a person by answering the question ("who are you?"). These attributes, along with credentials issued by the service provider (e.g., unique ID number, e-Document, e-ID, mobile ID) can then also be used as authentication factors to answer the question ("are you who you claim to be?").

The global challenge of identity

Legal identity is defined by the World Bank as an identity that carries a legal status, usually issued by governments to their citizens. Although there are no globally accepted identifiers, these types of identity tend to include basic identifying information such as a person's name and date of birth. Typical examples include birth certificates, voter registration cards, social security numbers, and national identity cards, documents, and numbers.

Despite the importance of being able to uniquely identify oneself, the World Bank Identification for Development (ID4D) database estimates that over a billion people globally lack any form of officially recognised identity. The remaining 6.6 billion people have some form of identification, but over half cannot use it effectively in today's digital ecosystems. This problem disproportionally impacts on rural residents, poor people, women, children, and other vulnerable groups. Without a secure way to assert and verify their identity, a person may be unable to, for example, open a bank account, vote in an election, access education or healthcare, receive a pension payment, or file official petitions in court. Furthermore, poor identification systems mean that states will have difficulty collecting taxes, targeting

[7] The World Bank, 2016, Digital Identity: Towards Shared Principles for public and Private and Private Sector Cooperation

social programmes, and ensuring security. Achieving inclusive development therefore requires a sustained effort to address the world's identity gap, as reflected in the new Sustainable Development Goals.

Digital identity, combined with the extensive use of digital channels such as mobile devices in the developing world, offers a transformative solution to this global challenge and provides public and private sector entities with efficient ways to reach the poorest and most disadvantaged.

The importance of identity in promoting financial inclusion

The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system. On this, one delegate noted, *"There are currently no standards for digital identity, except for some form of identity that is kept in the cloud (the internet)."*

The need for greater adoption of a publicly available, national (even global) directory of legal identities is clear. Financial services businesses invest significant amounts of time, money, and resources into the basic task of identifying people and legal entities as they on-board new clients in line with the Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (The FATF Recommendations) regarding Customer Due Diligence (CDD). It also has to be kept in mind that entity verification processes do not stop with the conclusion of the on-boarding process. The client data must be maintained up-to-date throughout the business relationship, which includes regularly verifying business information and changes to the ownership structure. Therefore, as long as countries are not using a standardised, widespread legal identity, it will continue to be a long and laborious process, which can discourage financial services providers from expanding their offerings to previously unserved consumer segments. It will likewise discourage consumers due to the onerous processes.

Lack of identity also limits the development and delivery of efficient, secure, digital-based fintech offerings, and is currently a critical pain point for fintech innovators. Many of these innovators are trying to deliver pure digital offerings, but the process of identifying users consistently forces them to use physical channels. These fintech innovators now see the development of a new generation of digital identity systems as being crucial to continuing innovation and delivering efficient, secure, digital-based fintech offerings.[8]

Transitioning from paper-based to digital identities

Traditional paper-based systems can be an inefficient means to prove a person's legal identity – subject to errors, fraud, and damage.[9] As the general population veers more and more in the direction of a digital economy, there is an opportunity for national governments to leapfrog traditional outdated paper-based systems and offer more inclusive methods of proving legal digital identities. New technologies, such as the increasing use of digital registration systems combined with biometric data collection (fingerprinting, iris scanning, and facial recognition), result in official identities that are more robust and credible as well as being more portable and accessible.

Developed and developing countries alike are increasingly moving to adopt digital identity systems, and some examples are shown in Figure 1 below. In addition, many developing countries are exploring innovative ways to offer further services online, including e-Government services such as payment of school fees, taxes, land registration and social payments. Despite the move towards digital identity, countries in regions such as Sub-Saharan Africa still have low citizen registration levels.

[8] World Economic Forum, 2016, A Blueprint for Digital Identity

[9] GSMA, 9 October 2017, Definitions of Identity – Legal/official Identity [https://www.gsma.com/mobilefordevelopment/programme/digital-identity/definitions-identity-legalofficial-identity/]: accessed 11 September 2019

Figure 1: Examples of countries that have adopted digital ID[10] [11]

SecureKey Concierge, Canada

(~50% adoption)
- Federated system launched in 2012 led and operated by financial institutions
- Enables authentication only with a range of public and private sector institutions through online login

UK Verify, UK

(<10% adoption)
- Federated system launched in 2016 by public sector, with private identity providers
- Enables authentication only with a set of public sector departments through online login, with plans to expand to private sector institutions

BankID, Sweden

(~75% adoption)
- Launched in 2003 by financial institutions, now recognised by the government
- Enables digital authentication and signature with limited data sharing for use with public and private sector institutions through smart card or digital device (mobile or computer)

e-ID, Estonia

(90+% adoption)
- Launched by public sector in 2000, with over 940 public and private sector institutions connected today
- Facilitates authentication, data storage and sharing, and digital signature through chip based card or digital keys

Digital Identification System (SID), Argentina

(<10% adoption)
- Recently launched by government in coordination with private sector
- Will enable remote biometric authentication across public and private sector services

National eID, Nigeria

(<10% adoption)
- electronic ID card launched by public sector in partnership with Mastercard in 2014
- Enables authentication through chip based card and data sharing for KYC, with potential additional future use cases under consideration

Aadhaar, India

(90+% adoption1)
- Launched in 2009 by agency established by public sector
- Enables biometric digital authentication, as part of broader digital ecosystems with additional functionality
- Key use cases include direct transfer of benefits to bank accounts, e-KYC, digital document storage

Mobile Connect, global

- Launched in 2014 by the GSMA, and now provided by 52 mobile operators across 29 countries
- Enables mobile operator-facilitated, user-controlled, authentication and data sharing functionality, with applications including e-commerce, e-government, and banking

As shown in Figure 1 above, India is one of the countries that have adopted a digital ID system. Despite piloting multiple national identity projects over the decade prior to 2008, the government of India had not only been unable to firmly establish a foundational national ID, but the average Indian resident held several functional forms of identity, each of which served a different purpose, followed a different application process, and generally reached different segments of society. For example, the four major identification programmes – passports, voter IDs, Permanent Account Number cards and ration cards – only covered about half of the population, and fraudulent versions of these documents were widespread. India's experience in adopting a national digital ID is described in Case study 2 below.

[10] Mckinsey Global Institute, 2019, Digital Identification: A key to inclusive growth.

[11] The Global System for Mobile Communications Association (GSMA) is a trade body that represents the interests of mobile network operators worldwide. Approximately 800 mobile operators are full GSMA members and a further 300 companies in the broader mobile ecosystem are associate members.

Case study 2: India’s Aadhaar programme

With an estimated 1.2 billion inhabitants, India is currently the world’s second-most populated country, and is expected to overtake China as the most populated nation within the next few years.[12] In addition to the sheer size of its population, India is also characterised by a high level of diversity; a person can identify themselves on the basis of their region, religion, language, caste, creed, gender, sect, occupation, political involvement, etc. The country is home to over 2,000 ethnic groups and more than 1,600 ‘mother tongues', twenty-nine of which have over one million speakers.[13] These realities made national identity particularly difficult for the country.

In the absence of a national identity with universal coverage, service organisations in India (e.g. mobile network operators, financial institutions, health care centres, and government) would typically set and follow their own processes for establishing the identity and entitlement status of Indian residents in order to provide them with services. This presented a number of challenges. For example, government was spending nearly USD 60 billion a year on its various social security programmes reaching 600 million people. According to Rajesh Bansal, the entire funding pipe leaked from the time it left the Federal Treasury to when it reached the 600 million recipients of the programmes. There was often some form of gaming the system – e.g. a person claiming more than once, and people creating separate identities. The leakages were estimated between 10% - 40% of the total spend.

In 2009, the Indian government established the Unique Identification Authority of India (UIDAI), giving it the mandate to provide a unique ID to each of India’s residents. Its objective is to collect the biometric and demographic data of residents, store them in a centralised database, and issue a 12-digital unique identity number called Aadhaar (Foundation) to each resident.

Since 2010, 1.25 billion biometric IDs have been issued, making Aadhaar the world’s largest biometric database and the first online biometric-based identity system in the world. The system has also expanded to include iris authentication. The impact of Aadhaar has to be viewed in conjunction with the other two initiatives introduced under the JAM Trinity (acronym for Aadhaar, Jan Dhan Yojana bank accounts and Mobile number).

- Jan Dhan Yojana: Pradhan Mantri Jan-Dhan Yojana (PMJDY) is India's National Mission for Financial Inclusion to ensure access to financial services for every household in an affordable manner. The campaign was launched by the Prime Minister of India Narendra Modi on 28 August 2014 and has since led to more 300 million bank accounts being opened in five years.
- Mobile number: PMJDY strongly focused on use of mobile/internet banking especially in the areas where physical branches cannot be established. These channels were viewed as an important tool for increasing access to internet and improving service delivery. As a result, more than a billion SIM cards have been issued, there are 500 million smartphone subscribers, and India has some of the lowest mobile data tariffs in the world.

Because Aadhaar is built on an open platform, external organisations are able to re-engineer its application programming interface (API) to create new, connected services. These ‘layers’ of services, known as the ‘India Stack', have helped create a digital infrastructure that provides presence-less (no need for physical authentication), paperless and cashless service delivery from anywhere in India.

Through the India stack, organisations can now leverage Aadhaar to digitally authenticate new customers (e-KYC); send payments directly to a users’ bank account (Aadhaar Payments Bridge); sign documents online (e-sign); allow users to transfer money via mobile (Unified Payment Interface); or share documents such as bank statements, utility bills, etc. with other service providers who need to authenticate a users’ identity (Digital Locker).

Some of the notable successes from Aadhaar and the India Stack include 32 billion authentications,

[12] R. Gladstone, 29 July 2015, ‘India Will Be Most Populous Country Sooner Than Thought, U.N. Says’, New York Times [https://www.nytimes.com/2015/07/30/world/asia/india-will-be-most-populous-country-sooner-than-thought-un-says.html?_r=0 ,] accessed 09 September 2019

[13] Bioethics in India: Proceedings of the International Bioethics Workshop in Madras: Biomanagement of Biogeoresources, 16-19 Jan. 1997, http://eubios.info/index.html .

7.47 billion e-KYC, and over 800 million uniquely banked individuals verified through Aadhaar since its launch.

During the workshop, when asked to quantify the savings that have been made from the JAM Trinity, Rajesh Bansal mentioned that the digital identity infrastructure reduced the cost of opening an account to about a fifth of what it used to be.

However, a number of challenges were raised during the workshop that still need to be addressed. These included:

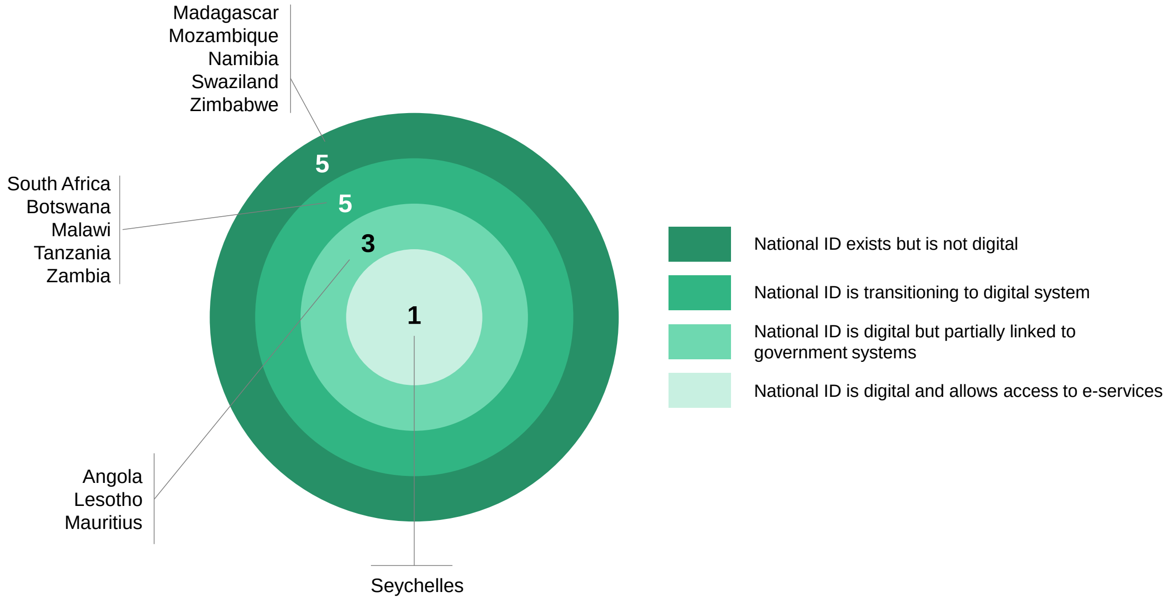
- Ensuring records are up to date: Despite having set up over 35,000 physical stations for people to update records regarding changes in address and death, keeping fully up to date records is still a challenge.
- No laws for privacy and data protection: In the absence of data privacy laws in India, UIDAI has worked to establish its own stringent security and data privacy policies to ensure that the information collected from residents is secure. Despite these protocols, there are still concerns regarding the legal framework around UIDAI's activities and their ability to ensure that personal data – collected and transmitted by private companies and stored in one central database – is kept private and secure.

As shown in Figure 2 below, the case study above details how programmes employing this relatively new technology have had mixed success to date. Many have struggled to attain even modest levels of usage, while a few have achieved large-scale implementation. Despite these challenges, delegates saw great potential, and agreed that well-designed digital ID not only enables civic and social empowerment, but also makes possible real and inclusive economic gains.

Digital identity in South Africa and the continent

According to the World Bank ID4D 2018 database, Sub-Saharan Africa accounts for half of the world's unregistered population. Though there is a widespread push to introduce national ID systems in the region, there remains a large variation in the extent of development of the national ID and registration systems. It is no surprise then that only a few countries have been able to introduce digital ID systems.

Figure 2: Level of digitisation of national ID systems in the Southern African Development Community (SADC) region[14]



In South Africa, the Department of Home Affairs (DHA) started the journey towards digital identity with the introduction of the Smart ID card in 2013 under the Home Affairs National Identity System (HANIS). South African financial institutions such as South African Banking Risk Information Centre (SABRIC)

[14] World Bank State of ID country briefs & ID4D 2017 dataset

member banks use HANIS to biometrically verify the identity of their customers. This online service provides the SABRIC member banks the opportunity to verify certain information of a client with information stored on HANIS and is recognised by the Financial Intelligence Centre (FIC) as an alternative procedure to verify the identity of a client as required in terms of the FIC Act (FICA). The progress towards 100% coverage of the Smart ID card has been slow, with only 13 million out of 41 million eligible individuals (about 32%) having registered. The rate of adoption is expected to speed up with an expected 90% coverage by year 2021.

DHA is now working to replace HANIS with the Automated Biometric Identification System (ABIS), a real-time centralised data source of customer information that will identify and verify people through fingerprints, facial recognition and IRIS technology. DHA's aim is that HANIS will run in parallel with ABIS and will be decommissioned once ABIS is in full production around March 2021.

As a centralised data source, ABIS will capture all data related to civic status and identity for South Africans as well as immigration and identity for all foreign nationals. This system will therefore seek to integrate with other relevant systems, inside and outside Home Affairs, to allow for one holistic view of the status of clients. It will serve as a single source for biometric authentication of citizens and non-citizens across state institutions and private sector entities.

As a result of the DHA's efforts to expand digital identification, and the potential advancements for financial inclusion, one delegate noted, *"Home Affairs is the backbone of the economy. It is not only responsible for security but also has an economic function."*

Identity and financial inclusion in South Africa

The sophistication of South Africa's financial system, as well as a well-covered national identity system, has led to a highly banked population. At the workshop, Nikki Kettles, Head of the SADC Financial Inclusion Programme at FinMark Trust, noted that more than 80% of South African adults over the age of 16 have a bank account. Although the South African population is highly banked, usage of bank accounts is low.[15] Additionally, the financial system is not equally accessible for micro, small, and medium enterprises (MSMEs) and migrant workers, as many are unable to provide proof of address or valid ID documentation required by financial institutions as part of their Know Your Customer (KYC) processes. For example, customers are often required by financial institutions to provide proof of address not older than three months. These restrictions limit the level at which the informal economy and cross-border remittances can move from cash to digital.

> *"A centralised digital KYC for specific use cases in SA and the region would make a huge difference. From an economic perspective, from reducing cost, and also considering the benefit to the user who no longer has to do KYC with various providers."*

Since 2003, the FIC has been relaxing the FICA rules in line with the FATF standards to make it easier for potential customers to open low-value accounts. Most recently in 2017, the FIC Amendment Act moved to a full risk-based approach (in line with the revised FATF standards) to Anti-Money Laundering and Countering Financing of Terrorism, and other SADC countries are expected to follow. In terms of this approach, anonymous transactions will not be allowed, but financial institutions will be left with more choice of which documents they rely on to verify identity of potential customers. This creates opportunity for agreements among accountable institutions to standardise their approach to identity proofing and verification.

Despite relaxed rules and the fact that financial institutions are not required to use an address as a unique identifier, KYC and challenges around proof of address dominated discussions amongst workshop delegates. Many expressed that financial institutions have yet to test methods of conducting KYC that do not require proof of address. Many agreed that there is a need for a paradigm shift within the financial sector from depending on documented proof of address as a critical means of verifying customers.

[15] FinMark Trust, 2016, Why use accounts? – Understanding account usage through a consumer lens

Many companies, including more agile financial institutions like fintechs, have been developing digital identity solutions to support their work and exploring ways to work around documented proof of address. These include using GPS coordinates, social media, and other types of data points which have been used in markets such as Brazil.

These innovations are fragmented and bespoke to specific institutions, with no linkages to the national ID system. As a result, delegates emphasised the need to investigate ways in which DHA's systems can be integrated with others that exist in the market. Although these conversations are yet to take place, DHA is said to be working on a new e-Identity policy which could help facilitate greater engagement between DHA and those companies.

> *"The big challenge we have is that the CDD in the FIC Act has not been properly embedded. We are still in the tick-box exercise. We need to introduce a certain level of authenticity and uniqueness of the individual… supplementary information is the space where we need to apply our efforts. "*

Privacy and data protection in the age of digital identity

While digital identity and increased interconnectedness through the internet provide several benefits, potential data breaches, cyber threats, and other criminal activities present risks to information security. This risk becomes more significant when data is centralised. Although ABIS is reportedly protected through cutting edge authentication and security protocols, delegates expressed concerns about the risk of centralised data systems. As a result, delegates explored the viability and benefits of decentralised identity solutions, such as through the use of blockchain.

> **"***The internet was not built with a layer of identity. It is difficult to prove you are you online."*

Blockchain has facilitated the idea of having Self-Sovereign Identity (SSI). SSI is the concept that people and businesses have ownership of their digital and analogue identities, and control over how their personal data is shared and used. This adds a layer of security and flexibility allowing the identity holder to only reveal the necessary data for any given transaction or interaction. What makes blockchain unique, relative to other systems, like public key infrastructure, is the ability to be uncensored or controlled by a central authority. Blockchain also enables data interoperability across potentially thousands of distributed applications. This has the potential to completely change the way we use identities to connect to different online services. On this, one delegate noted, *"The emerging model of decentralised digital identity will ultimately replace the identity you talk about today."*

The concept of SSI is relatively new in South Africa. However, the financial sector has shown growing interest, with identity blockchain networks such as the Sovrin Network and Ethereum working with financial institutions to build credential issuance and verification. The Sovrin example is discussed further in Case study 3 below.

Case study 3: The Sovrin Foundation and Sovrin Network

The Sovrin Foundation is a non-profit organisation established to administer the Governance Framework governing the Sovrin Network, an open source decentralised global public network enabling SSI on the internet. The Sovrin Network is operated by independent Stewards and uses the power of a distributed ledger to give every person, organisation, and entity the ability to own and control their own permanent digital identity. With recent advancements in digital identity standards, Sovrin provides a secure and private network for identity holders to collect, manage and share their own verifiable digital credentials.

To date, the Sovrin Network is operated by more than 75 Stewards around the world. The Sovrin Foundation expanded the open source community to include more than 200 developers with over 15,000 code contributions.

Given the budding nature of the SSI concept in South Africa, there are still a number of challenges that limit organisations’ ability to adopt this technology as noted by presenters from the South African Financial Blockchain Consortium. These include the struggle to get started without a clear strategic plan and goals; a steep learning curve to doing it yourself and skilled developers being rare in the market; potential vendor lock-in due to a small pool of suppliers; and unclear overall governance; and lack of data standards and lack of an ecosystem.

Conclusion: bringing stakeholders together to facilitate digital identity

Digital identification enables citizens to access critical government and economic services and presents an important opportunity to promote financial inclusion. However, developing digital ID systems is a time-consuming process and also presents a new security risk due to potential cyber threats. These types of threats can further exacerbate vulnerability among the traditionally un/underserved population.

The South African DHA introduced a Smart ID in 2013 and is in the process of developing a more advanced, integrated digital ID system. For South Africa to successfully harness the benefits of digital identity, and manage potential risks, workshop delegates put forward the following suggestions for public and private sector stakeholders to consider:

1. There needs to be better interoperability of different identity platforms whereby government engages with the private sector to explore how the different identity solutions being piloted can be integrated with the national ID system. On this, one delegate noted, “Platform interoperability is key, as organisations will have to be able to issue credentials into identity wallets being used by customers. Initially we see the use in a few separate and narrow industry verticals, but the technology implemented must plan for much broader use.”
2. As innovation continues to take place, customer information privacy and protection needs, and cybersecurity need to be ensured and maintained, which requires a robust and collaborative regulatory framework.
3. Service providers, particularly financial service providers, need to leverage the flexible risk-based approach in terms of FICA to explore alternative identifiers to proof of address in order to better serve target markets such as informal businesses and migrant workers.
4. There is need for better understanding and engagement of centralised versus decentralised identity systems, more especially the concept of SSI.
5. Consumers need to be better educated and empowered to protect and manage their data.

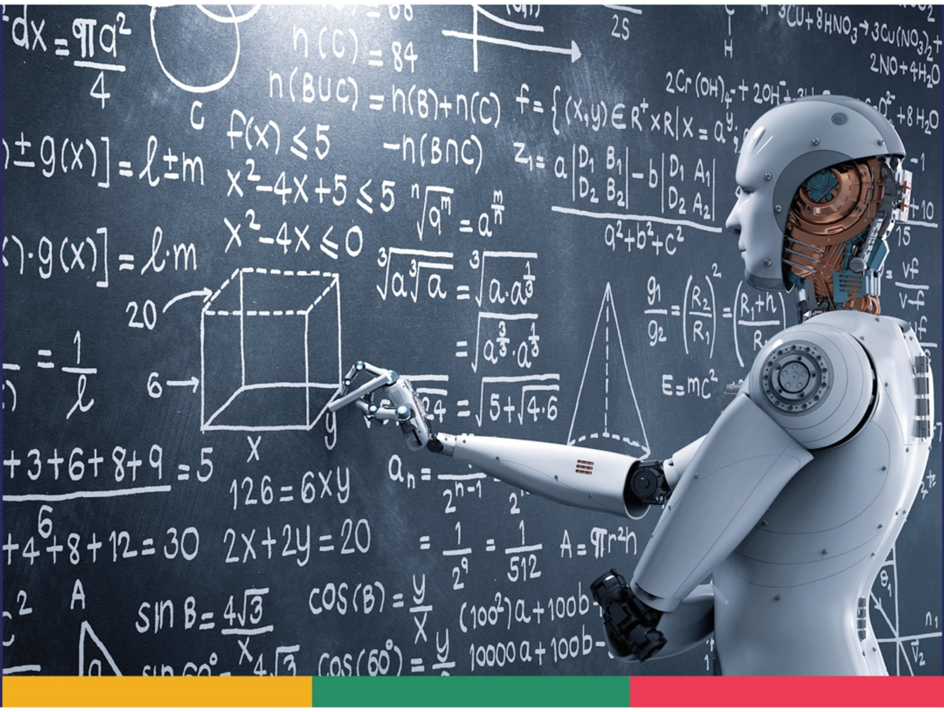
IFWG

INTERGOVERNMENTAL FINTECH WORKING GROUP

FINTECH WORKSHOPS

03 September 2019

Harnessing AI for economic growth



Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Harnessing Artificial Intelligence for economic growth

In the summer of 1956, a group of leading academics spent time at Dartmouth College to discuss the possibilities of computers processing intelligence. The vision of the workshop was to "proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it."[16] It was at this event that the term Artificial Intelligence (AI) was coined, and the field was founded.

Since this meeting, there have been considerable global advancements in AI. Governments worldwide are investigating and implementing policies and strategies to support innovations in AI technologies. These technologies are also being used in South Africa and the rest of the continent, in the financial services, agriculture and healthcare sectors, among others. While AI offers tremendous opportunity to improve lives and support economic growth, there are also potential negative political, social, legal and ethical consequences associated with these technologies which should be anticipated and managed. Government has a critical role to play in developing policies and regulations to harness AI for economic growth, while also introducing measures to minimise potential negative second order consequences of these technologies.

At a glance

The Artificial Intelligence workshop explored global and local applications of AI.
- While governments such as China are aggressively pursuing AI technologies, others are taking a cautionary approach due to the ethical risks associated with these technologies.
- Applications in South Africa and the rest of the continent are solving for human needs in the financial services, agriculture and healthcare sectors.
- While AI presents new solutions, there are a number of risks associated with these technologies, including ethical, legal and political risks. AI makes decisions in complex ways and understanding and correcting for these when errors occur can lead to exaggerated shocks.
- As AI becomes increasingly common, regulators and policymakers need to consider and manage the impacts on labour markets as technology may displace workers.

Defining AI

The concept of processing large amounts of data to find patterns and insights has been around for a long time. However, advancements in mathematics and computer processing capacity, as well as increased data generation and availability have enabled the field to flourish. Delegates referred to this period as the "golden age of artificial intelligence."

As linear thinkers, it is difficult for us to comprehend the rate at which we can grow and develop this field. Speakers referred to Moore's law[17] to frame the rate of exponential development in this space. The rate of computer processing power and data storage capabilities has increased exponentially, while becoming increasingly more affordable.

AI tech is defined by four types of machines, with the first being the most basic and type four being the most advanced:

- **Reactive machines:** The most basic AI system which is purely reactive and does not have the ability to form memories or to use past experiences to inform current decisions. A machine is given context and rules on which to base decisions. An example of this is IBM's Deep Blue machine, a chess-playing machine that beat international grandmaster Garry Kasparov.
- **Limited memory:** These machines use some amount of past data for machine learning. Self-driving cars are an example of this technology, where data points such as lane markings, traffic lights and other important elements, like curves in the road, are pre-programmed to help the car make decisions. This data is only transient, and experiences are not saved for the car to learn from in the way that human drivers learn from their driving experience.
- **The theory of mind:** Machines of the future will be able to understand that people, creatures and

[16] John McCarthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. 1955. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. *AI Magazine*. Vol. 27, No. 4. 2006.

[17] In short, this law states that processor speeds, or overall processing power for computers will double every two years. Investopedia. Moore's law definition. Available: https://www.investopedia.com/terms/m/mooreslaw.asp.

other robots have thoughts and feelings that impact on their behaviour.

- **Self-awareness:** The final AI development will be to build machines with consciousness. Conscious beings are aware of themselves, know about their internal states, and are able to predict feelings of others. However, this type of AI is not yet in existence.

Speakers described the last two types of AI as the “holy grail", where machines are able to have memories, learn from situations and base decisions on past experiences.

Global Investments in AI

The Harvard Business Review estimates that AI will add USD 13 trillion to the economy over the next decade.[18] A few countries are expected to be at the forefront of these investments, including China, the UK and the US.

The Chinese government has ambitious plans to be the world’s AI leader by 2030. China has a centralised AI strategy endorsed by the highest level of government and plans to invest billions of dollars in research and development.

The UK is another market aggressively pursuing AI technology with a thriving AI start-up market. The government has invested GBP 1 billion to support the development of the AI industry and academia. The investments focus on four thematic areas – leadership, skills, adoption and data.[19]

In the US, venture capital investment in AI has grown phenomenally. In 2012 venture capitalists funded USD 282 million of AI initiatives; that number has grown to USD 5 billion in 2017 and USD 8 billion in 2018.[20] Also in North America, while the Canadian government was the first to develop a national AI strategy, and is making a concerted effort to enhance AI capabilities,[21] Canadian investors are taking a more cautious approach. Adoption of AI technologies comes with a host of potential ethical and cybersecurity risks, and investors recognise the need to understand and mitigate these risks before aggressively pursuing AI technologies.[22]

AI applications in South Africa and the rest of the continent

There are already a number of exciting AI technology applications in the South African and African context. While some of these applications were first developed in other markets, AI is creating more efficiencies in production processes and has the potential to fuel economic growth on the continent. Harnessing the potential of AI technology will help drive development goals and the reduction of poverty in Africa. There are a few key industries where we are already seeing the positive impact of AI technology, namely financial services, agriculture and healthcare.

Financial services

A healthy and inclusive financial services sector is a key driver of economic growth and development. Financial service providers are keen to embrace the productivity and efficiency benefits of technology and use innovation to improve the customer experience and reduce the exposure to risk.

A delegate representing Capitec bank, a large retail bank focusing on lower income individuals in the South African market, described how the bank is using AI technologies to increase revenue opportunities by providing customers with better insights on their financial positions, improving customer experience, as well as identifying areas for growth and retention. The bank is also reducing costs by

[18] Harvard Business Review; The AI Powered Organisation, July-August 2019

[19] Wendy Hall, “In 2019, despite everything, the UK’s AI strategy will bear fruit,” *Wired UK*, December 27, 2018; Gov.uk, “World-leading expert Demis Hassabis to advise new Government Office for artificial intelligence,” press release, June 26, 2018.

[20] These numbers were recorded in Statistica: Artificial intelligence (AI) funding investment in the United States from 2011 to 2018 (million U.S. dollars)

[21] United Nations Educational, Scientific and Cultural Organisation, “Canada first to adopt strategy for artificial intelligence.” November 22, 2018. Available: http://www.unesco.org/new/en/media-services/single-view/news/canada_first_to_adopt_strategy_for_artificial_intelligence/.

[22] Deloitte Insights. Future in the balance? How countries are pursuing an AI advantage: Insights from Deloitte’s State of AI in the Enterprise, 2nd Edition survey. May 1, 2019. Available: https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/ai-investment-by-country.html.

developing more efficient, automated processes, and improving risk management by supporting risk and compliance processes such as transaction monitoring and anti-money laundering.

Some of the most notable examples of AI technology being investigated and used by South African financial services providers included:

- **Prediction analysis**: AI offers financial service providers the opportunity to analyse customer data to identify patterns in behaviour and transactions. Predictive models can then be used to support banking processes such as *retention*, by predicting that a customer will move to another service provider; *credit scoring*, by predicting likelihood of default; and *fraud detection*, by identifying unusual transaction behaviours.
- **On-boarding**: AI technology can be used to authenticate identities, process applications and supporting documents in real time, and support KYC checks by aggregating data from external data sources. Chatbots also allow these processes to be conducted on digital channels, improving the customer journey. For example, Strider, a South African fintech company that focuses on AI and automation in financial services, confirmed that an on-boarding process using AI technology can be conducted in under two minutes using AI and alternative data.
- **Advice:** Robo-advice platforms are using technology to provide cost effective ways to offer customers advice on topics ranging from suitable products to discretionary asset management services. For example, South African firm CLEVVA offers a platform that companies can use to build and deploy front-office digital workers used to deliver consistent, compliant and context-relevant sales, service and support across staff-assisted and digital channels (also refer to Case study 4 below).
- **Supervision and regulation:** Regulators are also using AI technology to improve the quality of supervision of financial services markets. The South African Reserve Bank is investing in infrastructure that will allow the regulator to extract data from financial service providers. This technology will also analyse large granular data sets to support predictive models that will identify potential risk areas. This is aligned to a global shift towards risk-based supervision that sees regulators play a more proactive role in identifying risk factors and working with the financial services sector to take mitigating actions.

Case study 4: CLEVVA as explained by CEO Ryan Falkenberg

Within the future digital workforce, there are different specialists emerging. There is the Natural Language chatbot called 'boff' which specialises in free-flowing conversations; the Data Reader (optical character recognition) that specialises in extracting information off PDF documents and Images; the Predictor (AI), that specialises in predicting outcomes from huge sets of data; the System Processor (robotic process automation - RPA) that specialises in capturing information into different legacy systems; and the Process Navigator (CLEVVA) that ensures the right questions are always asked, the right information is always gathered, the right answers are always given and the right actions are always triggered. Plus, there is a compliance report to prove it.

"CLEVVA allows low-code teams to build, deploy and maintain the entire front-office digital workforce," Falkenberg explained. “Our digital workers are process compliance specialists. They ensure your front-office logic is consistently and correctly applied to every situation, across every channel. Their logic works a bit like a GPS, adjusting the engagement journey to the context and the specific set of choices made.

For staff, they act like digital co-workers, guiding them through real-time customer engagements, much like a GPS guides a driver through unfamiliar roads. For customers, they act like a digital specialist at their fingertips, offering compliant, intelligent self-service via mobile, web, social media, or instore kiosk.

They also ensure that the decisions made, and information gathered is then automatically actioned. They do this by Integrating directly to targeted back office systems or to a RPA bot for processing. This ability to 'close the last mile' means that customers are never left with the task of solving their problem out for themselves. Being offered a link to 'helpful' Information is not what CLEVVA digital workers consider as service. Service means getting the job done right, first time, every time.

CLEVVA digital workers enable a number of financial companies to automate their customer on-boarding, financial need analysis, customer service and operational compliance.

Differences in sectors are starting to disappear as companies begin to realise that to succeed, they need to become data businesses – using data to understand their customers better, provide better customer experiences, find efficiencies and better manage business risks. Financial service providers are no different.

“Data is the new oil and is allowing new businesses to compete with incumbents more efficiently and effectively.”

Agriculture

Agriculture is a critical sector in Sub-Saharan Africa. The sector is currently the largest source of employment on the continent and a key contributor to economic growth. However, there are a number of challenges facing farmers on the continent, including increasing pest resistance, climate change and its impact on weather patterns, poor soil quality and its impact on crop yields. These challenges not only threaten food security but the livelihoods of millions of Africans.

AI technologies provide potential solutions to some of these challenges, such as by predicting weather patterns and pest outbreaks, and monitoring harvest levels. For example, Microsoft and the International Crop Research Institute for Semi-Arid Tropics have developed a Sowing App that helps farmers achieve optimal harvests by advising on the best time to sow, taking into account weather and soil conditions which can lead to higher crop yields.

Blue River Technology has developed See & Spray technology to manage crops at a plant level. Usually all plants in a crop are treated the same; however, See & Spray technology uses computer vision and AI to allow growers to detect, identify, and make management decisions about every single plant in the field individually.

Healthcare

Examples of AI in healthcare include technologies that encourage people to live healthier lives and detect disease earlier and more accurately. These innovations are improving medical diagnosis and even extend to complex surgical robots that can either assist a surgeon or perform operations themselves.

Sophie Bot is an example of an African healthcare innovation. Developed in Kenya, this chatbot[23] answers questions on sexual and reproductive health in a society where talking about sexual health is often taboo. Sophie Bot provides anonymity and credible answers in a conversational manner. Users are able to interact with the platform using popular messaging apps, such as Twitter.

Seeing AI is a Microsoft project which uses AI to describe surroundings for the visually impaired. Using the camera to 'see' a person's surroundings, Seeing AI then provides a verbal description of anything that appears in front of the camera. Seeing AI is able to describe people, text, currency, colours, and objects.

AI still has areas of concern

The power of AI technology lies in vast amounts of data that is aggregated to find patterns and predict future behaviours. Delegates expressed a number of concerns around ensuring data quality, biases with the underlying algorithms and models, security of data, legal concerns and the ethics of AI.

Delegates agreed that there are issues around data quality and that poor data, or data with inherent biases would lead to unfair or biased outputs. Businesses therefore need to understand the importance of collecting, acquiring and using quality data when implementing AI technology.

Financial Service Providers (FSPs) deal with sensitive customer data and this would need to be taken

[23] A chatbot is a “programme that uses instant messaging (IM) as an application interface… Because the bot uses artificial intelligence (AI), the end user has the feeling he is talking to a real person and is apt to forget that he is really just querying a database.” TechTarget. IM bot. September 2005. Available: https://searchdomino.techtarget.com/definition/IM-bot.

into consideration when transferring customer data to third party partners for analysis or via APIs[24] to support additional products and features. However, one delegate, involved in the development of AI tools for banks and other FSPs, felt that once data had been modified or 'vectorised'[25] as an input to AI technology, it is often less useful to anyone outside the organisation as it would likely be out of context.

Delegates acknowledged that algorithms and analytical or mathematical models developed by humans could be susceptible to human biases that may potentially exclude segments of the market. For example, advisory models are built using pre-determined, defined rules and prescribed logic, and are reliant on context. As a result, these models can reflect the bias of the individual designing the model. One suggested way to overcome this was to programme instances where the results of the model would be manually verified to ensure the quality of the model.

Delegates agreed that there is an inherent risk that models could become opaque to the point where the "decisioning logic would be difficult to explain and could lead to exaggerated financial shocks." This is because as the algorithm learns, it sorts pieces of data into constellations of data that would take time for humans to break down and understand. If a financial shock occurs, the time taken to break down and address the model could increase the severity of the financial shock. Despite this, delegates felt that governance around AI technology should be centralised within an organisation and not at a regulator level.

Many of the areas of concern raised by delegates relate to the ethics of AI, including moral, socio-economic and legal concerns. Some of these concerns have been discussed above, such as risks associated with AI bias. However, delegates expressed other second order consequences, including the potential to exacerbate inequality and malicious use of AI by political adversaries.

To date, some bodies such as the European Union (EU) Commission have begun to address issues around developing guidelines for trustworthy AI technology. For example, the EU High-Level Expert Group on AI has presented Ethics Guidelines for Trustworthy Artificial Intelligence.[26] However, there is more work to be done that will need the collective input of civil societies, governments, multilateral organisations, private sector and academia. Delegates noted that further research is necessary to identify the potential risks and harms of AI technology; develop national strategies that identify human rights in relation to interactions with robotics; to understand the role of law; and develop ways to implement policies to ensure fair, ethical and transparent behaviour in the use of technology.

Conclusion: The role of the regulator in harnessing AI

Returning to the South African context, delegates and speakers alike felt that regulators have a role to play in ensuring that advances in technology do not exacerbate or create new areas of exclusion.

Many raised concerns that AI will eliminate jobs and potentially worsen inequality, impacting on the most vulnerable in society. Some delegates argued that cost efficiencies from automation can lead to high profit margins, ultimately benefiting business owners or owners of capital rather than ordinary South Africans. Delegates noted that AI is often used to automate manual processes, a pain-point in developed markets with high costs of labour. However, technology solutions for the South African market should not focus exclusively on automation as our markets have more cost-effective labour forces and our economy needs job creation. While most delegates acknowledged that some jobs will disappear as a result of automation, many felt that there may be more opportunities to generate jobs requiring different skill sets more focused on supporting the technology industry.

Policy makers have a role to play in facilitating labour market policies to help connect displaced workers with new employment opportunities, as well as providing access to training opportunities so that workers are better placed to succeed in new types of employment. As part of this, government needs to re-think elements of the national education systems. National curriculum should include more focus on

[24] An API defines how software components should interact. Petr Gazarov. What is an API? In English, please. freeCodeCamp. 16 August 2016. Available: https://www.freecodecamp.org/news/what-is-an-api-in-english-please-b880a3214a82/.

[25] Vectorisation is, "the process of converting an algorithm from operating on a single value at a time to operating on a set of values at one time." Quantify. Vectorization, Part 2: Why and What? 22 June 2017. Available: https://www.quantifisolutions.com/vectorization-part-2-why-and-what.

[26] European Commission. Ethics guidelines for trustworthy AI. 8 April 2019. Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

mathematical skills, critical thinking and technology to equip learners to enter the workforce and be able to participate in the AI economy and even contribute to AI advancements. The importance of this objective was also discussed in the Innovation section above.

Many also emphasised that investments in information and communication technology (ICT) infrastructure, 5G connectivity in particular, is necessary to facilitate advances in AI and data analytics in South Africa.

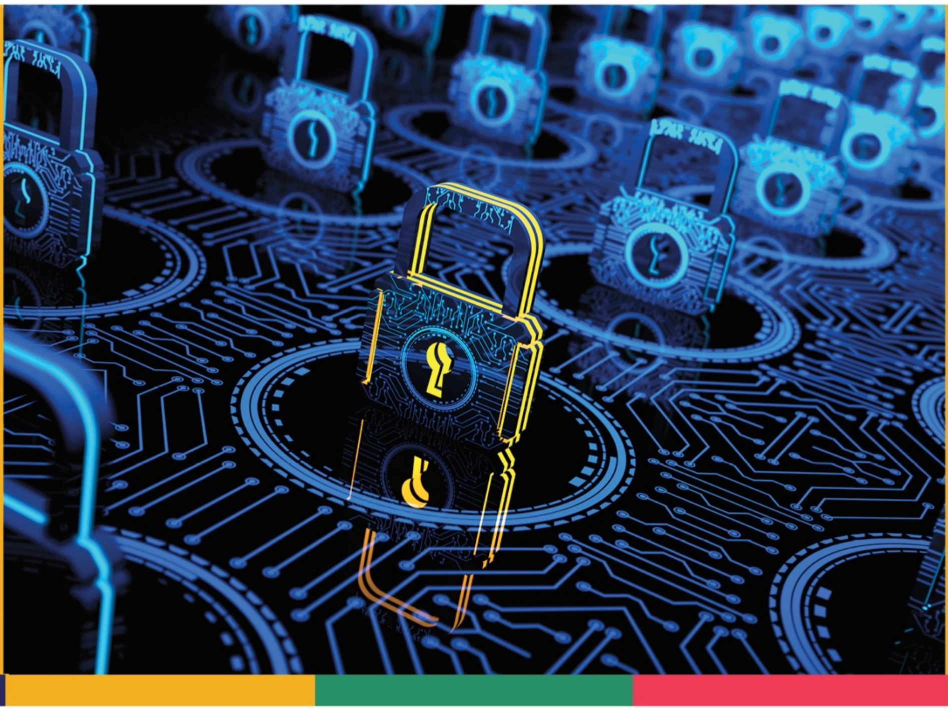
Technology will continue to gather pace; devices, objects, organisations and organisms will become increasingly interconnected. Machines will become more 'intelligent' as they start drawing on past experiences to inform future decisions – how this will impact humans is unknown. But with the right governance and guidelines in place there is potential to use this technology to significantly improve lives across the continent.

IFWG FINTECH WORKSHOPS

INTERGOVERNMENTAL FINTECH WORKING GROUP

04 September 2019

Cybersecurity (Collaborate • Coordinate • Execute)



Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Cybersecurity

As technology continues to evolve, new opportunities and challenges also emerge. The sections above have described how digital connectivity plays a pivotal role in unlocking innovation and prosperity around the world. However, increasing cyber threats present a material obstacle to the progress possible through technological advancements. Cybercriminals take advantage of a borderless playing field and the lack of adequate measures by governments, corporations, and global law enforcement to launch targeted attacks, with limited risk and retribution. These threats are just as relevant for South Africa, especially as the country continues on its path towards the 4th Industrial Revolution and greater digital connectedness to the world. This IFWG workshop crystallised the need for greater collaboration and information sharing at a sector and cross-sector level in order to effectively prevent, detect, and respond to and recover from cyberattacks.

At a glance

The workshop revealed a number of cybersecurity-related concerns introduced by technology-driven innovations.
- Cybersecurity threats have further become more prominent with increased interconnectedness and pose significant economic costs.
- South Africa has a number of mechanisms to prevent, detect and respond to and recover from cybersecurity threats.
- However, delegates noted that more work is necessary in this regard, including increased information sharing for threat detection and strengthening the legal framework for government bodies to coordinate their cybersecurity activities.

Cybercrime[27] is a global issue

According to Danny Myburgh, Association of Certified Fraud Examiners' Cyber Forensic Forum for South Africa, the most dominant types of cyber threats encountered are a combination of computer incidents and fraud. This includes:

- **Business email compromise**: where attackers compromise a person's online mail account and change account details. There is often a case of illegal access, such as through phishing[28] or when an attacker breaks in and there is no dual factor authentication.
- **Ransomware**: this is currently the biggest cyber threat to an organisation. The more sophisticated attack is where attackers physically insert ransomware into the server. In a number of these attacks, it is either revengeware or where attackers are trying to cover their tracks.
- **Illegal access or hacking**: which is often a result of weak password controls. IBM estimates that the average cost an organisation incurs per security breach in South Africa is ZAR 4.3 million. These attacks can go more than 200 days unnoticed by the organisation.

The World Economic Forum's Centre for Cybersecurity reports that the global economic loss due to cybercrime is predicted to reach a staggering USD 3 trillion by 2020. The GozNym malware, for example, managed to steal over USD 100 million since 2016[29] – demonstrating both the grand scale of cyberattacks and the devastating consequences for their victims. This is discussed further in Case study 5 below.

Case study 5: The GozNym malware

GozNym is a hybrid of two other pieces of malware, Nymaim and Gozi. Nymaim is known as a 'dropper', a type of software that is designed to sneak other malware on to a device and install it. Gozi has been around since 2007; over the years it has resurfaced with new techniques, all aimed at stealing financial information.

The new computer malware targeted 22 websites that belonged to banks, credit unions and e-commerce platforms based in the US, and two that belong to financial institutions from Canada. Unsuspecting citizens thought they were clicking a simple link – instead they gave hackers access to their sensitive data. The suspected ringleader used GozNym malware and contracted different cyber-

[27] Criminal activities carried out by means of computers or the internet.

[28] Phishing is a cybercrime in which individuals are targeted via email, telephone or text message. The perpetrator poses as a legitimate institution (such as the target's bank) in attempt to obtain sensitive data such as passwords and credit card details.

[29] Europol, 2019. Goznym malware: cybercriminal network dismantled in international operation [https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation] accessed

crime services to control more than 41,000 computers and enable cyber criminals to steal and whitewash an estimated USD 100 million from victims' bank accounts.

In May 2019, Europol reported to have dismantled the cybercrime network behind the GozNym. The 10 members were from five different countries have since been charged. However, five of the members remain on the run – including the developer of GozNym malware who oversaw its creation, development, management, and leasing to other cybercriminals.

As the internet has become more complex, digitally fuelled innovation has outpaced the ability to introduce adequate safeguards. Current efforts to contain cybercrime, while important, remain largely insufficient as the global impact of cyber threats continues to grow. Figure 3 below provides details on the risks and costs imposed by cybersecurity threats.

Figure 3: The global cybersecurity threat in perspective[30]

6.4 billion The number of fake emails sent worldwide – every day	**1,464** The number of government officials in one state using "Password123" as their password
50% The number of local authorities in England relying on unsupported service software	**2 million** The number of stolen identities used to make fake comments during a US inquiry into net neutrality
1,946,181,599 The number of records containing sensitive data compromised from Jan 2017 - Mar 2018	**USD 729,000** The amount lost by a businessman in a scam combining "catphishing" and "whaling"
550 million The number of phishing emails sent out by a single campaign during the first quarter of 2018	**USD 3.62 million** The average cost of a data breach

Cybersecurity in South Africa

Prevention is better than a cure

Customer information is ranked by financial institutions as the top most valuable information to cyber criminals, followed by financial information and strategic plans. It is no surprise then that amongst the emerging cyber risks over the next five years, data-related risk is viewed by financial institutions as the main risk to anticipate. This is because data is increasingly seen as an important strategy driver by Boards and executives. One delegate noted, "If I contaminate that data, I can contaminate your strategy and send you on a wild goose chase."

As a result, financial institutions clearly recognise the risk of cybersecurity threats. However, delegates emphasised that South African banks and other financial institutions are still struggling to prevent and detect sophisticated attacks. The first challenge in this space is that it is difficult to identify the right advanced threat prevention and identification tools — organisations struggle with the nuance of why one solution is more suitable than another.

During his presentation, Samresh Ramjith, Deputy Chief Information Security Officer at ABSA Group challenged cybersecurity practitioners to engage with business units to improve effectiveness as well as business outcomes. In his experience, cybersecurity teams are moving from 'command & control' authorities in centralised businesses to having to cope with federated structures that exist in an ecosystem of providers, at both the infrastructure & application levels. In these aggregate organisations, cybersecurity is experiencing a sharp learning curve to align with the dynamic business environment

[30] Ernst & Young, EY Global Information SecuritySurveySecuritySurveySecuritySurveySecuritySurveySecurity Survey 2018–19

and add security features to business processes while considering the implications for efficiency, customer experience, and revenue impact. Historically, business executives were briefed on market risks and issues, but in future, success will be measured on performance improvements over time, as the board's focus shifts to wanting to understand emerging cyber risk scenarios, their potential contextual impact on the business and the organisations' ability to manage these eventualities – board awareness alone will not suffice. In his view, cybersecurity practitioners could do more to work closely with business units, understand the business drivers and work to ensure that cyber solutions are both business focused and cost optimised, rather than technology or vendor focused.

> *"Cybersecurity is a negative deliverable – measuring something that does not happen. It is about how we communicate cybersecurity. Often the cyber function reports to the Chief Financial Officer, which places a view on role of cyber – e.g. Return on Investment, which can create issues around drivers."*

Delegates referenced the FirstRand Bank's approach to prevention as one which works well. FirstRand Bank established an external and separate red team[31] that works on ensuring adequate protection against material risks. These include risks that have serious financial implications for the bank such as affecting share price. Unlike conventional cyber teams that report to business units, the team reports directly to the Chief Risk Officer, and they run various clandestine scenario tests on how quickly the bank is able to detect and control an attack. These are only known by top management and primarily, not known by business teams.

Adequate preparation cushions the cost of an attack and is in the best interest of an organisation given that it is cheaper to secure a service provider before an incident occurs rather than when it is happening. On this, one delegate noted, *"When it comes to cyberattacks, it is not if, but when. So, it is all about preparation, preparation, and preparation."*

Delegates reflected on how attackers do not wait until an organisation is ready for the incident. Instead, they strategically select to attack on weekends and odd times, such as at midnight. The attackers take ample time to understand the cycle of a business, know different sequences and seasonality. Therefore, organisations need to anticipate and plan responses to possible attacks, train for responses, and implement incident reporting strategies accordingly.

From the workshop discussions, it is comprehensible that there are various methods financial institutions can apply to prevent cyber breaches. However, the success of these different methods can be strengthened by some key principles, including:

- Continuous insight versus spot check-audits;
- A reality versus hypothetical view;
- Control frameworks that correspond to the modern threat landscape; and
- Translating cyber risk to a language that the board will appreciate and can act upon.

The role of government and regulators in preventing cyber breaches

Government and regulators play an important role in helping the private sector prepare for and prevent cyberattacks. The potentially systemic nature of this risk necessitates a targeted regulatory response, and a lot of guidance can be gleaned from international best practice. It is therefore important to make sure the risks do not trigger other vulnerabilities in the system.

The Cybersecurity Hub was established by the Department of Communication and Digital Technologies (DCDT) under the mandate of the National Cybersecurity Policy Framework in 2012. The Cybersecurity Hub is South Africa's National Computer Security Incident Response Team (CSIRT)[32] and its

[31] Red teams are focused on penetration testing of different systems and their levels of security programmes. They are there to detect, prevent and eliminate vulnerabilities. A blue team is similar to a red team in that it also assesses network security and identifies any possible vulnerabilities. What makes a blue team different is that once a red team imitates an attacker and attacks with characteristic tactics and techniques, a blue team is there to find ways to defend, change, and re-group defense mechanisms to make incident response much stronger.

[32] A CSIRT is a team of dedicated information security specialists that prepares for and responds to information security incidents. When an incident occurs, members of a CSIRT can assist its constituency in determining what happened and what actions need to be taken to remedy the situation.

responsibilities are:

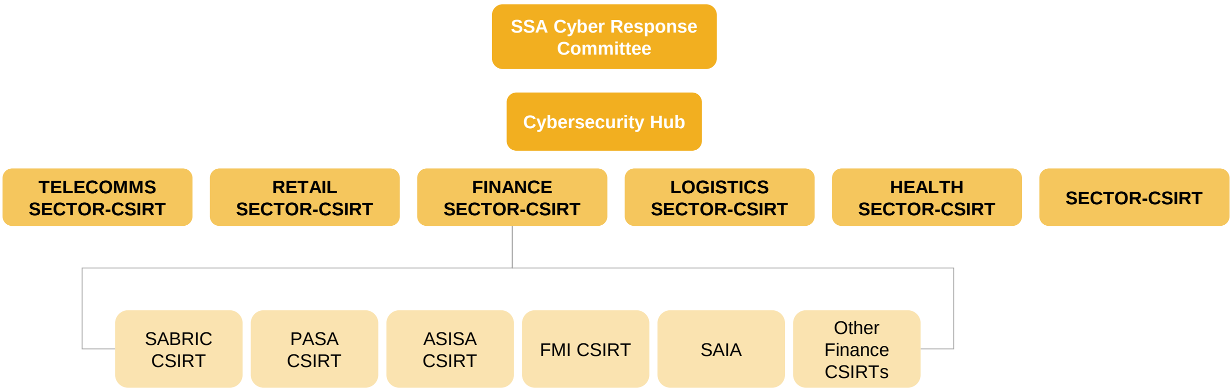
- **Consultation**: The Cybersecurity Hub consults between the Justice, Crime Prevention and Security cluster departments, the private sector and civil society regarding Cybersecurity matters;
- **Coordination**: Coordinate general cybersecurity activities; identifying stakeholders and developing public-private relationships and collaborating with any sector CSIRTs that may be established;
- **Dissemination of information**: Disseminate relevant information to sector CSIRTs, vendors, technology experts;
- **Providing guidance**: Provide best practice guidance on ICT security for government, business and civil society;
- **Promoting compliance**: Promote compliance with cybersecurity standards, procedures and policy and best practices; and
- **Creating awareness**: Initiate and run cybersecurity awareness campaigns.

While the Cybersecurity Hub is meant to be regulatory in nature, it is currently limited in that role. The Cybercrimes Bill, which will enable the Hub and DCDT to adopt sub-legislation, is currently before Parliament and is yet to be passed into law. Delegates expressed that passing the Bill is critical, because a legislative mandate may give more impetus for the Cybersecurity Hub to strongly encourage collaboration in the sector-based and national CSIRTs.

Among the various sector CSIRTs, delegates highlighted that the Finance Sector CSIRT is well represented and is driven by industry associations, including the South African Banking Risk Information Centre (SABRIC), the Payments Association of South Africa (PASA), South African Insurance Association, and the Association of Savings and Investments South Africa (ASISA). Financial markets institutions are also part of this CSIRT, including the Johannesburg Stock Exchange, Prudential Authority, BankservAfrica, and Strate.

Other sectors have their own CSIRTs, including the Internet Service Providers Association CSIRT (Telecomm sector) and the Consumer Goods Retail sector CSIRT (retail sector). This is depicted in Figure 4 below.

Figure 4: Illustration of South African CSIRT structures



Delegates noted that the sector-based CSIRTs are a valuable platform for organisations to collaborate on issues relating to cybersecurity. So far, however, there has been mixed levels of engagement within the sector-based CSIRTs and at a cross-sector level. Delegates also noted that one of the challenges limiting cross-sector collaboration is the lack of a legal framework for the Cybersecurity Hub to mandate CSIRTs to work together. However, there were mixed views in the workshop about how effective an enforcement model might be in encouraging information sharing.

> *"What is missing is that there isn't enough awareness and education cross-sector. Cross-sector pollination is not happening."*

Regulatory bodies also play an important role in preventing cyber threats. The Financial Sector Regulatory Act (Act 9 of 2017) defines specific roles for financial sector regulators. This includes protecting and enhancing financial stability, and if a systemic event has occurred or is imminent, restoring or maintaining financial stability. Financial regulatory bodies are also required to monitor status and take reasonable steps to prevent systemic events from occurring.

Jacques Henning, Head of Operational Risk and IT Risk at the Prudential Authority took workshop participants through various initiatives the Prudential Authority has undertaken in the financial sector (mainly with banks) relating to cybersecurity. These included a guidance note on outsourcing of functions within banks (2014); questionnaire on IT security and infrastructure risk (2016); flavour of the year with Boards on cybersecurity (2016); and a guidance note on cyber resilience (2017).

Effective detection

Similar to prevention, delegates agreed that detection activities require a holistic sector and cross-sector approach driven by regulators, industry associations, and private sector institutions. To enable effective detection, there should be concerted efforts to build cyber threat intelligence, information sharing, collaboration, as well as incident sharing.

So far, this collaboration and information sharing takes place within pockets of specific industry associations and sector CSIRTs, but it has not broadened to cross-sector and international level collaboration. SABRIC has, for example, built a platform for reporting cyber events. The platform is, however, still manual, making it difficult to manage the large volume of data and SABRIC is working on making it an automated process. SABRIC has also adopted a colocation model where people from different organisations can work in the same room and share learnings from time-to-time.

> *"What's missing is a sustainable model of sharing. Currently sharing happens in trusted circles between individuals and is based on informal relationships. The sustainability issue is important because if a personal contact leaves an institution, you no longer have a contact in that situation. We need a better model for sustainable information sharing."*

To increase its source of information, ASISA has also joined the Financial Services Information Sharing and Analysis Centre, a global financial industry resource for cyber and physical threat intelligence analysis and sharing.

One delegate suggested that detection efforts could potentially learn from the 'neighbourhood watch' model. Some of the tools that could be used in cyber threat detection based on this model include:

- **Volunteers**: There is a need for volunteers amongst practitioners and they need to do it for the greater good. We need people and financial institutions to step up and put their time on the line.
- **Tailored groups**: There may be people who want to share information, which is not always the same as that shared by others. We need to make sure the information is being discussed in the right group. When thinking of detection and sharing of information, we need to create those groups that are practicable. This could include setting up a technical group, operational group, etc.
- **Relevant content**: When we create these sharing groups, we do not want to re-share things that are already known. We therefore need to define the set of information that needs to be shared so that there is no information overload. SABRIC has done some work in this space and this can be learned from.
- **Shared analysis**: Once the information is shared, we need people who will start to connect the dots. A number of workshop participants questioned how this can be done. For instance, do you set up national or sector structures? The best approach is an important conversation to be had in determining the way forward.
- **Privacy settings**: The groups also need to define the privacy rules of the group – i.e. rules of engagement. As a principle, for example, the person sharing the information should be in control of how wide it goes. When setting up the groups, it is therefore important to consider how we create trusted groups in order to increase confidence that sensitive information can be pushed to those groups.
- **Dynamic groups**: There is often a tendency to think hierarchically, but delegates emphasised the importance of dynamic group set ups. For example, there may be room to create sharing groups for distilling information. There are communities that are quite similar that will want to share this information with each other. We should therefore be more flexible with how we create these groups.
- **Public partnerships**: It is important to use the national structures and partnerships such as the Cybersecurity Hub.
- **Reporting rules**: By reporting, there is an opportunity to push back into the regulatory machinery

and could lead to improved regulation. Although CSIRTs create structures and rules to deal with information in specific ways, there will always be systemic issues to share when they happen. We need to come up with ways where information can be shared anonymously.

Another delegate expressed a concern that anonymous sharing is a novel idea but difficult to implement in practice and it is unclear how it will work in practice. One potential approach to achieve this is to create a trusted institution that owns the potential database – not government – but a trusted party, where everyone contributes. The trusted party can conduct the analysis and flag when they find the hit and share with the relevant parties. This is where regulation can help to create an environment to share in order to ensure that the right parties are getting the relevant information.

Going forward, delegates also emphasised that there is a need to be clear on what is meant by information sharing. For example, the type of information that is shared in cybersecurity differs from what is shared when a cybercrime occurs. In other words, information should be viewed within the different contexts; there is a need for clarity regarding sharing information about a threat in comparison to different learnings about an incident.

An attack has happened – how do we respond and recover?

Effective response to and recovery from cyberattacks is dependent on the level of an organisation's and broader ecosystem's preparation. To be adequately prepared, organisations need to:

- Create an Incident Response (IR) policy and plan;
- Develop IR standard operating procedures to handle incidents;
- Define clear communication channels;
- Select IR team; and
- Define IR services.

Hendrik Nel, Head of the Financial Stability Department at the South African Reserve Bank (SARB), mentioned that the SARB plays an important role in guiding and coordinating finance sector response to events. In line with this, he noted that the SARB has conducted a number of crisis management simulation exercises in the financial sector, facilitated by external consultants through the Financial Sector Contingency Forum (FSCF). These exercises had cyber risk scenarios and showed that there is strong resilience in the sector. He emphasised the need to be able to estimate the cost of a potential systemic cyber event, which will help stakeholders understand the impact of the event.

The Governor of the SARB may determine that a specified event is a systemic event. Such a determination, announced publicly, will provide with SARB with additional powers to direct regulators to take certain actions and/or provide certain information. The SARB has developed a risk assessment matrix, through which systemic risks are identified, analysed and communicated to the Financial Stability Committee (FSC) for possible mitigating action. Cyber risk has been identified as one of four possible systemic risks, rated it in terms of the probability and impact of the event and the possible mitigating policy actions that can be taken to address the risk.

> *The Financial Sector Regulation Act 9 of 2017 also provides for the establishment of the Financial Stability Oversight Committee (FSOC) with the main aim of supporting the SARB in protecting and enhancing financial stability. The FSCF is another statutory forum to support the FSOC in identifying and mitigating risks to the financial sector. All the industry associations driving sector-based CSIRTS are represented in the FSCF. Responses to and recovery from cyber events could therefore be coordinated through the FSCF "We have a good feel of what's happening in the financial sector. But there is still some missing link around cross-sector collaboration."*

Conclusion: Collective actions to manage cybersecurity risks

The sections above have described how technology innovations introduce opportunities to fundamentally improve the lives of people across the globe. At the same time, however, cyber threats undermine progress in this regard.

The South African government has taken material steps to prevent, detect and respond to cybersecurity threats, and South African firms are likewise implementing measures in response to the risks posed by cybercrime. However, delegates agreed that there is a need for increased cross-sector engagement in addressing the cybersecurity risk. Specific actions included:

- Promoting greater collaboration amongst the different sector-based CSIRTs;
- Exploring ways to build a culture of information sharing beyond informal groups;
- Strengthening the legal framework for government and regulatory bodies to coordinate cybersecurity activities and encourage information sharing; and
- Investing more in campaigns to better educate the public on cyber risk and best practices for protecting one’s privacy and data.

By taking appropriate measures to manage cyber threats, South Africa will be in a better position to leverage and enjoy the benefits of emerging innovations for economic growth.

IFWG

INTERGOVERNMENTAL FINTECH WORKING GROUP

FINTECH WORKSHOPS

04 September 2019

Central bank digital currencies: evolution, revolution or distraction?

Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Central Bank Digital Currency

In recent years, CBDC has become a topic of interest in the minds of central bankers globally, igniting a global debate about whether CBDC is the future of money as we know it. South Africa is currently among the list of countries experimenting with CBDC to determine its relevance and viability. However, while some argue that this phenomenon is the new reality of central banking, others maintain that CBDC is a mere distraction.

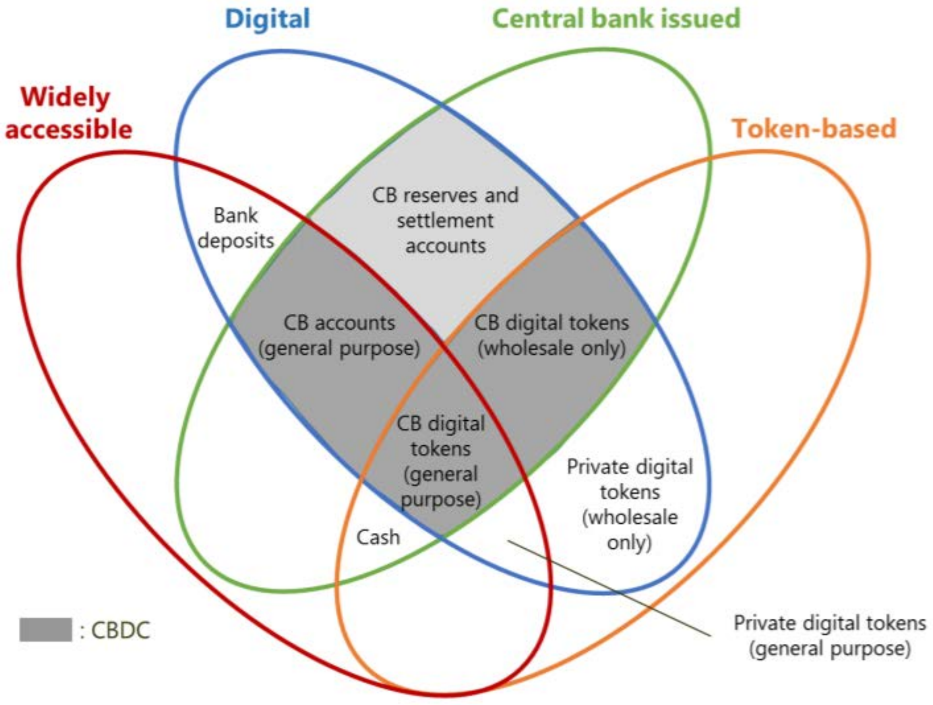
Understanding CBDCs

CBDC is not well-defined and an internationally agreed conceptualisation is elusive. The most common understanding of CBDC refers to an electronic central bank liability that is denominated in the national unit of account, which is different from balances in traditional reserve or settlement accounts[33]. CBDC can be for wholesale use, between banks only, or it can be for retail use, meaning it is open to the public. Retail CBDC allows for universal access and acceptance that is not necessarily blockchain-based. CBDCs may be interest bearing, private, account or token-based, and can be hosted on different technology platforms. Figure 5 below depicts a taxonomy of money, including traditional, digital and CBDC-based money.

At a glance

CBDC is an emerging trend globally, and countries such as South Africa are investigating its relevance and viability. Workshop delegates debated the benefits and challenges associated with this technology.
- Delegates debated as to whether CBDC is an effective monetary policy instrument, and whether CBDC can deepen financial inclusion.
- Successes from initiatives, such as Project Khokha in South Africa, have increased confidence that CBDC is technically feasible, but further analysis of the policy implications is required.
- Additionally, delegates noted that South Africa already has a sophisticated financial system and argued that introducing CBDC could result in financial stability implications.

Figure 5: The money flower: a taxonomy of money


Digital
Central bank issued
Widely accessible
Token-based
Bank deposits
CB reserves and settlement accounts
CB accounts (general purpose)
CB digital tokens (wholesale only)
CB digital tokens (general purpose)
Private digital tokens (wholesale only)
Cash
Private digital tokens (general purpose)
▨ : CBDC

Source: Bank for International Settlements

[33] https://www.bis.org/cpmi/publ/d174.pdf

Global trends in CBDC

Tunisia was the first country in the world to adopt a national cryptocurrency called the e-Dinar in 2015.[34] Then, in 2016, Canada began investigating the potential for a CBDC, in part due to the declining use of cash in the economy.[35] For a developed economy, such as Canada, it could be motivated by a number of factors, including:

- provide universal access to all citizens – especially those in rural areas;
- promote availability of a risk-free payment mechanism;
- improve competition in the payments sector;
- improve payments resilience; and
- maintain privacy for low value transactions.

While there are a number of potential benefits of introducing a CBDC in Canada, one delegate noted that there are also significant risks, such as potential security breaches. Additionally, while delegates discussed the use of CBDC as a monetary policy instrument, some questioned its relevance in this regard, noting that CBDC may be an ineffective tool for implementing negative interest rates. In investigating the viability of CBDC, and weighing up the potential costs and benefits, the Canadian central bank has yet to conclude in favour of a CBDC. In order to manage potential risks, the bank is considering the best design features to integrate in order for the electronic currency to yield the expected benefits.

By February 2019, 19 countries worldwide had investigated or were in the process of investigating the feasibility of a CBDC.[36] The list below presents the positions of certain countries around the world,[37] while Figure 6 below provides more information in this regard.

Adopters	Experimenters	Rejecters
Tunisia	Canada	Ecuador
Senegal	Dubai	Estonia
Marshall Islands	Kingdom of Eswatini	Switzerland
Venezuela	Iran	Hong Kong
	Singapore	Japan
	South Africa	
	Uruguay	

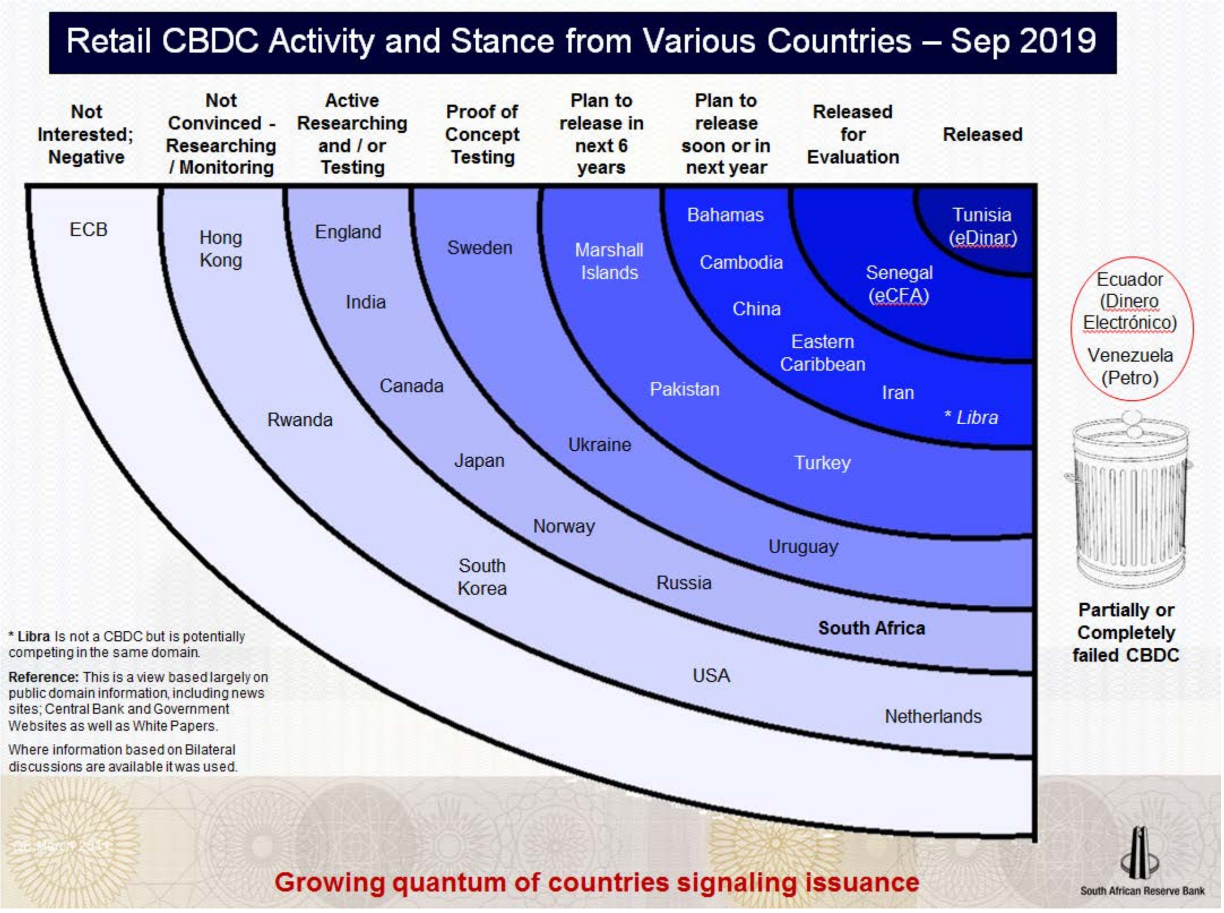
[34] CBDCs of the World: The Benefits and Drawbacks of National Cryptos, According to Different Jurisdictions, Stephen O'Neal, Jun 2019

[35] While the use of cash in the Canadian economy is on the decline, delegates noted that in countries such as Sweden the decline in the use of cash has been more marked.

[36] CBDC: 19 Countries Creating or Researching the Issuance of a Digital Decentralized Currency, L. Willemse, Feb 2019

[37] State-Issued Digital Currencies: The Countries Which Adopted, Rejected or Researched the Concept, Stephen O'Neal, Jul 2019

Figure 6: Retail CBDC activity and stance from countries



Retail CBDC Activity and Stance from Various Countries – Sep 2019

* **Libra** is not a CBDC but is potentially competing in the same domain.

Reference: This is a view based largely on public domain information, including news sites; Central Bank and Government Websites as well as White Papers.

Where information based on Bilateral discussions are available it was used.

Growing quantum of countries signaling issuance

Source: Johann Bence, SARB, Workshop presentation, Sep 2019

Looking at specific case studies, it is apparent that the CBDC approach is not 'one-size-fits-all'. Careful thought and testing is necessary to ensure the right decision is made for each country. Case study 6 refers to an example of a country which has chosen to adopt CBDC while case study 7 below refers to a country considering the implications of CBDC in its jurisdiction.

Case study 6: China, a CBDC-adopter

China has a large proportion of its population that rely on Facebook for daily communication. Since the announcement of the Libra project in June 2019, China has urgently focused on the development of its own digital coin in order to avoid banks being overtaken by the social media giant in the finance sector. The government had conducted a year and a half-long digital currency feasibility project and, in August 2019, announced the digital version of the yuan.

The digital yuan is intended to be a substitute for all coins and notes (M0) in circulation and is intended to boost circulation of the yuan locally and internationally.

The digital currency will be backed 1:1 by Renminbi fiat and will follow a two-tiered structured system with the bank, commercial banks, and retail market participants.

Case study 7: The Kingdom of Eswatini

The Kingdom of Eswatini is experimenting with digital currency. Eswatini has a high financial inclusion rate of 87% with four out of five adults possessing a bank account. The aim of the Eswatini CBDC trial is to allow more citizens access to the financial system and to be on-par with its regional partners should they also introduce CBDCs, as the country is highly integrated with its neighbours and trading partners.

The first findings from the research and consultative forum in Eswatini show the following:

- Both financial industry and regulatory stakeholders are keen to test the benefit of a CBDC, however, there are concerns regarding the policy implications and lack of understanding.
- There are concerns regarding whether the problem statement is well articulated and whether resource allocation is adequate, given the relatively small size of the country.

The country prefers to be at the forefront of developments than lag behind.

Germany has also investigated the feasibility of a CBDC and has decided not to pursue a digital currency at this juncture. As the country already has a well-functioning financial system, replacing it with a new digital currency would mean large investments into finding a suitable alternative that meets or exceeds the efficiencies of the current system. This is described in Case study 8 below. However, while the German Central Bank currently does not see any substantial benefit in the issuance of a retail CBDC in the euro area, there is acknowledgement of the potential benefits of Distributed Ledger Technologies (DLT) for the design of wholesale payment systems and, as such, the Bank will continue to carefully analyse the possible opportunities and risks of issuing a wholesale CBDC.

Case study 8: Germany remains cautious

The representative of the Bundesbank that addressed the audience agreed that there are potential benefits of having a CBDC, including the potential to avoid a single point of failure in technical infrastructure; 24/7 availability; supporting the consistency of delivery versus payment and payment versus payment payments when completing transactions.

However, to successfully implement a digital currency, critical design features should be in place. These include instant settlement finality; absolute and maximum security; and scalability. The scalability feature refers to the trade-off between decentralisation and throughput, which requires proof of work that systems will not fail at a large scale. Furthermore, introducing a digital currency requires training the country's resources on working with DLT, guaranteeing the legal status of a token and having sound governance structures for the currency.

For these reasons, the German Central Bank, Bundesbank, has decided not to introduce a wholesale or retail digital currency at this stage as the unknowns present risks that outweigh the benefits of having a stable, functioning financial system.

The South African context

South Africa is still in the experimental phase of its journey towards deciding whether to introduce a CBDC. In 2018, Project Khokha was launched to assess the performance, scalability, privacy, resilience and finality of a DLT solution for a clearing and settlement system under conditions as realistic as possible to those in the banking sector. It was designed, built and delivered in less than three months,[38] taking into account the South African context.

The project created a distributed ledger between participating banks for a wholesale payment system, backed by central-bank deposits, allowing participating banks to pledge, redeem and track balances of the tokenised sovereign currency (Rand) on the ledger. Each bank was responsible for the setup of its own node, and these nodes were then distributed. The whole system was set up using JP Morgan's Quorum network and other participants to monitor scalability, resilience, confidentiality and finality.

Project Khokha was recognised by the Central Bank Publication as the ***'Best Distributed Ledger Initiative'*** of 2018. It exceeded all milestones set, especially in terms of the number of transactions processed per period. However, it is not currently clear whether this pilot will work at national scale, and delegates agreed that there are numerous other issues to be considered prior to implementation. While some referenced Project Khokha's success as evidence that a CBDC is possible in South Africa, it should be noted that the pilot was for a *wholesale* CBDC, and must be distinguished from a *retail*

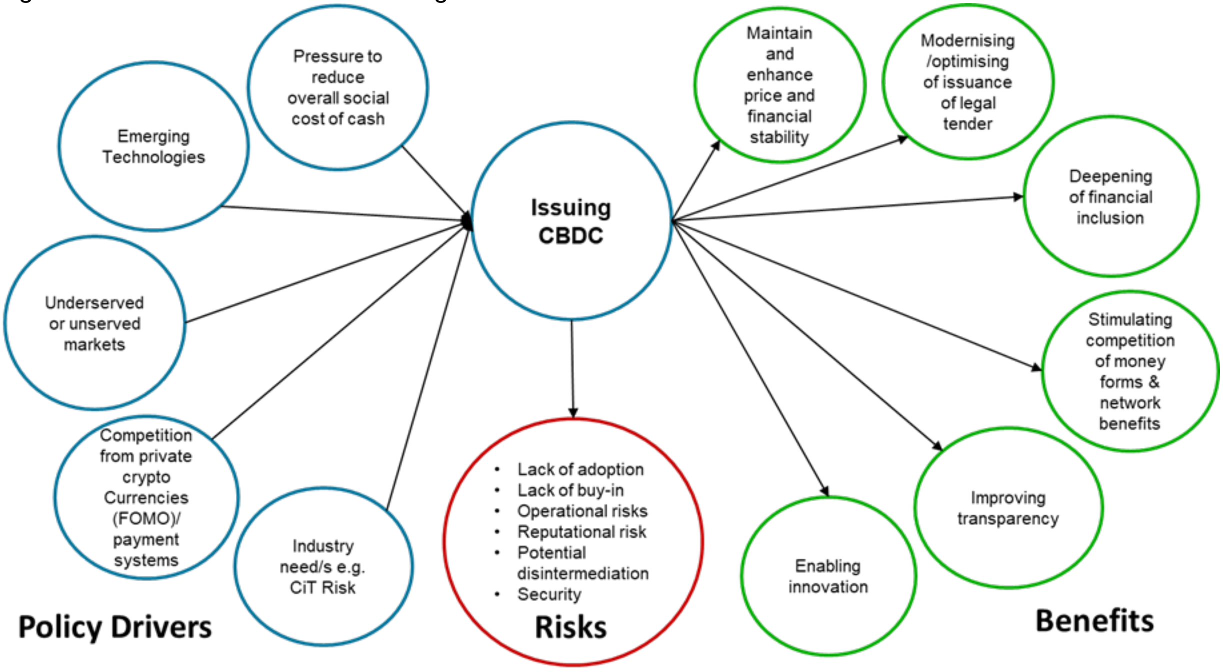
[38] Project Khokha Report, South African Reserve Bank,

CBDC.

Considerations: weighing up the costs and benefits in South Africa

When considering whether to issue digital currency, the central bank needs to understand the primary goal of CBDC and weigh up the benefits and costs accordingly. During the workshop, delegates debated the benefits and risks associated with CBDC, and whether this is a feasible and appropriate solution for South Africa. Figure 7 below summarises some of the key considerations when investigating a CBDC.

Figure 7: Considerations when issuing a CBDC


Pressure to reduce overall social cost of cash
Emerging Technologies
Underserved or unserved markets
Competition from private crypto Currencies (FOMO)/ payment systems
Industry need/s e.g. CiT Risk
Policy Drivers
Issuing CBDC
Lack of adoption
Lack of buy-in
Operational risks
Reputational risk
Potential disintermediation
Security
Risks
Maintain and enhance price and financial stability
Modernising /optimising of issuance of legal tender
Deepening of financial inclusion
Stimulating competition of money forms & network benefits
Improving transparency
Enabling innovation
Benefits

Source: Johann Bence, SARB, Workshop presentation, Sep 2019

As depicted in Figure 7 above, some delegates argued that CBDC could present a competitive alternative to the private sector by creating a theoretically better payment innovation. Linked to this, many emphasised that CBDC guarantees universal access, thus potentially enhancing financial inclusion. This is because it is not necessary to have a bank account to transact with CBDC as transactions can be made using an e-wallet. However, it is important to note that infrastructure gaps may undermine this outcome, as universal access is only possible where connectivity is not an issue. High data costs can also limit this possibility.

Delegates also discussed monetary policy arguments for issuing a CBDC. For example, some delegates noted that a CBDC could increase the speed of the monetary transmission mechanism, allowing monetary policy decisions to affect the economy more quickly. Delegates also referenced the potential to apply negative interest rates, whereas cash has a zero-lower bound. This would allow the central bank to set its inflation targets at theoretically optimal levels and manage the possibility of banks financial intermediation. Introducing a CBDC would also present an alternative to quantitative easing, as the central bank could use the CBDC to pay non-banks directly, thereby enabling the bank to bypass the banking sector.

Introducing a CBDC can also protect the seigniorage revenue of a central bank as the bank does not have to print as much currency and coin. Finally, CBDC can improve the data available on the financial sector; this can improve monetary and economic policy and enable improved money laundering management when cash is removed.

On the other hand, one of the core arguments against CBDC is that South Africa already has a highly sophisticated, well-functioning financial system. This is similar to the argument posed in Case study 8 above. Many delegates expressed the concern that a CBDC could become a competing force with retail banks and could crowd out existing banks as holding deposits for retail clients is one of their main functions. However, the SARB emphasised that a CBDC would be in addition *to* other forms of currency, and not replace them.

Furthermore, in contrast to countries like Canada, South Africa is a cash-heavy market, especially in the informal sectors. Therefore, the declining use of cash is not currently a concern in the context of South Africa. At the same time, however, some delegates noted that the high share of cash transactions in South Africa is a burden on the payment system and having a retail CBDC to supplement cash may reduce this burden. Additional arguments against a retail CBDC in South Africa included:

1. Lack of expertise in retail CBDC, and the need to have well-trained experts;
2. South Africa does not yet have a policy position and legal framework to oversee CBDC activity; and
3. Data privacy and cybersecurity can lead to reputational risk for the central bank.

Conclusion: The road ahead for CBDC

In view of all the considerations, workshop delegates were split on whether CBDC is the next step for South Africa's financial system. However, most agreed that the SARB should explore CBDC. Therefore, the work of the bank is now to engage policymakers to deliberate on policy positions and facilitate the discussion on whether CBDC has more merit than risks for the South African market. Delegates also agreed that a helpful next step in investigating this opportunity is to establish a task force that would lead any potential policy changes and a regulatory framework.

Despite the lack of consensus on whether CBDC is necessary for South Africa, many agreed on the practical design considerations that the SARB would need to ensure are in place to make the currency feasible. These included:

- Its value must be guaranteed and undisputable;
- It must be a generally accepted medium of exchange or transacting, accepted and trusted as legal tender, complementary to cash;
- It must be available and usable at all levels of the South African financial system and demographic or social fabric;
- Its value must be pegged at one-to-one parity with the Rand;
- It will be a liability on the balance sheet of the SARB and will remain so through the distribution chain (similar to cash);
- It must be divisible, durable, fungible, portable and limited in supply; and
- It must be an Irrevocable, Simultaneous, Final Transfer of Value (ISFTOV).[39]

It is evident that CBDC will be occupying the work of many central banks in the near future. Whilst there are sound policy reasons for implementing CBDC, efficacy of design is paramount to achieve the right outcomes. Whether these activities will lead to a new wave of electronic currency in developed and developing markets remains to be seen.

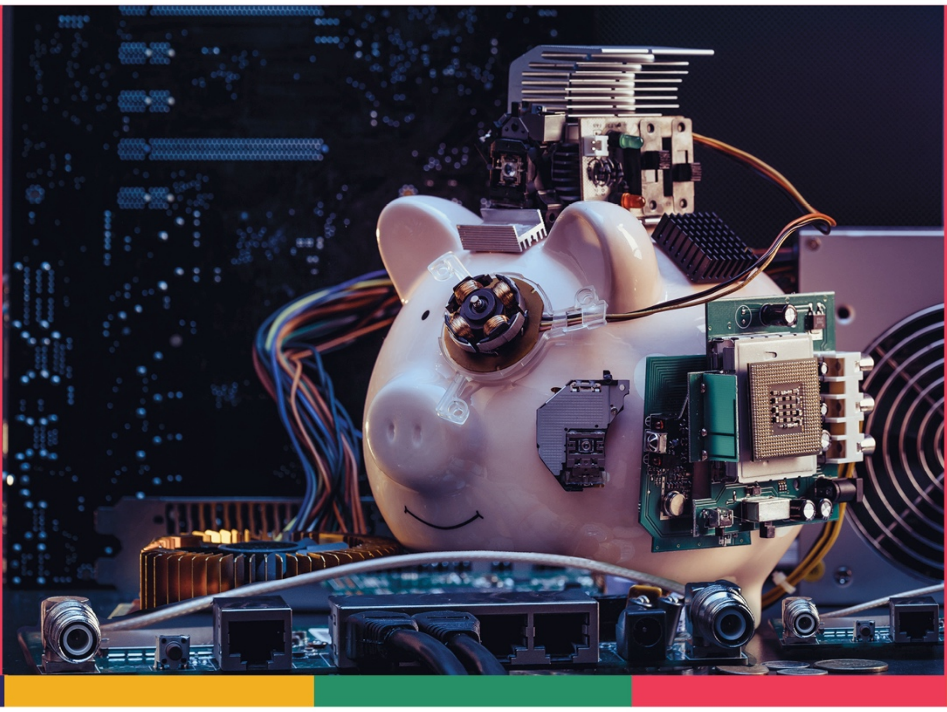
[39] Johann Bence, South African Reserve Bank

IFWG FINTECH WORKSHOPS

INTERGOVERNMENTAL FINTECH WORKING GROUP

04 September 2019

Open banking



Financial Intelligence Centre

FSCA Financial Sector Conduct Authority

national treasury Department: National Treasury REPUBLIC OF SOUTH AFRICA

NCR National Credit Regulator

SARS South African Revenue Service

South African Reserve Bank

Open banking

Many people view open banking as the new frontier of banking, giving customers more control of their finances and data. Open banking is shaking up the financial landscape globally, with over 22 jurisdictions across the world developing and implementing an open banking framework. Workshop delegates acknowledged that open banking presents significant opportunities for the South African market, while risks related to privacy and data sharing need to be understood and managed. However, to fully leverage opportunities, a number of regulatory changes need to take place to enable open banking in South Africa.

At a glance

As open banking becomes increasingly adopted, workshop delegates met to debate whether this is the next frontier of banking.
- The financial sector has traditionally been dominated by large incumbent banks, and open banking could solve for competition in this sector.
- Delegates highlighted that fintech innovations linked to open banking have benefited both incumbents and start-ups. Additionally, as in the other workshops, delegates also noted the benefits related to enhanced financial inclusion.
- However, the question of data ownership and data privacy was noted as potential risks associated with the trend toward open banking.
- Most delegates agreed that the regulator has a role to play in supporting an open banking environment, including guidelines for licencing and consumer protection.

What is open banking?

The UK government describes open banking as a secure way to give providers access to [customers'] financial information that paves the way to new products and services.[40] Open banking can also give consumers more comprehensive view of all their accounts. This all takes place on online or mobile banking platforms.[41]

The conversation around open banking is being driven by global trends. Regulatory initiatives such as the EU's Second Payment Services Directive (PSD2), issued in 2015, requires banks to provide customer data to third party providers and aims to promote the development and usage of digital payments innovation. In 2016, the UK Government introduced new requirements, specifying that the largest UK banks must allow licenced startups direct access to a customer's data down to the transaction account level. By 2019, open banking has risen to the top of many bank regulators' agendas.

The discussion at the workshop began by framing the context of open banking. Delegates probed the enabling factors that gave rise to open banking, including technological advancements that made integration possible and even necessary. Many questioned whether open banking is a regulatory construct necessary to keep pace with global markets, while others debated whether it is a material market opportunity or merely a risk to the sector. While the answer to these questions varied across stakeholders, all agreed that a common framework is necessary as South Africa and its regulators contemplate a roadmap for open banking.

Global advancements: "Banking is necessary. Banks are not"[42]

The traditional banking model is based on four capabilities: transactional services, safekeeping of money, credit provision and investment opportunities. Integration between these capabilities provides synergy and drives the economies of scale that have led to the growth of large banks.

However, the industry is evolving, and it requires banks to shift their thinking. Modern banks are focusing on three pillars:

1. **Platforms:** A technical architecture that can be used as a base from which to build applications, functionality and services.
2. **Curation functionality:** A deep understanding of customers is needed to meet their financial needs.
3. **Content:** Banks need to decide what products or services to offer; what they will produce internally and where they will partner.

[40] Open Banking Limited. Open Banking. 2019. Available: https://www.openbanking.org.uk.
[41] Open Banking Limited. Open Banking. 2019. Available: https://www.openbanking.org.uk/customers/what-is-open-banking/.
[42] Bill Gates, 1990.

This shift away from traditional banking capabilities and infrastructure is allowing new and innovative players to offer relevant banking services in a more cost-effective manner. Technology is transforming the cost to serve and unlocking the potential to reach and serve more people.

However, there are many barriers to new and innovative players entering this market. In the UK, the Competition and Markets Authority carried out an investigation into the retail banking market and found that the four largest banking groups for personal current accounts had a combined market share of just over 70% in 2015. Open banking regulation could solve for competition in this market by giving customers more choice.

To date, there are over 22 jurisdictions across the world that have either implemented an open banking framework or are working towards it. Case study 8 below reviews the example of Mexico.

Case study 6: Mexico

Mexico has low financial inclusion and an economy heavily reliant on cash. The regulatory reform in Mexico is placing an emphasis on its potential for accelerating financial inclusion. In 2018 the government passed the *Fintech law,* regulating virtual assets, digital payments, crowdfunding, introducing a regulatory sandbox, and requiring the publication of a regulation for open APIs within two years.

Mexican regulators diverged from the scope of the UK standard, in that the regulation will apply to all products and services and will be adopted by all financial service providers. The scope includes open data (public information), aggregated data, transactional data and case studies. There will also be a charge for the sharing of data.

Regulators see open banking as means of encouraging innovation, fostering competition, developing the financial services ecosystem and/or improving access. However, many incumbents could see open banking as a risk to their existing business models.

Is this an opportunity or risk?

Delegates representing both incumbent FSPs and fintechs were keen to point out the opportunities for all stakeholders. Delegates noted that in the payments space, banks have been working with third party payment providers for more than a decade and have found ways to negotiate fair business models that serve both parties. Additionally, banks have used APIs, the technology that facilitates the sharing of data between entities and that is foundational to open banking, internally for many years. As banks modernise their technology infrastructure and increasingly adopt cloud-based solutions their ability to partner, connect and share data will improve.

Fintechs offer solutions that could greatly improve customer experience and solve for evolving customer needs. Delegates referenced the example of screen-scraping, which was developed by fintechs to facilitate ecommerce electronic funds transfer (EFT) payments. Screen-scraping allows customers to pay a merchant directly from their bank account; however, it requires customers to provide fintechs with sensitive login credentials. In an open banking context, with customer consent, a fintech could access the customers' account and facilitate the payment with less risk to the customer and the bank.

Other examples of innovation between banks and fintechs included the ability to provide customers with loans at the point of sale (POS), allowing access to bank statements and an initiative for fintechs to develop e-wallets in partnership with a bank.

Another example of banks benefitting from fintech innovation is the growth of mobile POS devices (mPOS). These have allowed micro and small merchants, who do not qualify for a POS device from a large bank, to accept card payments. This increases card transactions in the economy which directly benefits card-issuing banks who receive an interchange fee (a portion of the transaction fee). POS devices also allow acceptance of electronic stores of value which means safer and more efficient transacting for both merchants and consumers. As a result, consumers tend to spend more than they would if they were using cash in these informal economies. Additionally, POS devices allow traceability, meaning the merchant has a record of income which can be used to apply for other financial products like insurance and credit.

Incumbents however need to be cognisant of the risks when partnering with third parties. Banks need to consider issues such as data ownership and customer consent for the sharing of data; for example, is consent required for each use case or could consent be applicable over an agreed time period? Open banking also raises questions about shifts in liability and to what extent third party providers are responsible and accountable. The consensus among delegates was that while there may be some shift of liability, if the bank holds the customer relationship it will have to be ultimately responsible and accountable to its customers.

The topic of data ownership brought to the fore the participation and risk of allowing 'bigtech' firms (the likes of Google and Facebook) to access customer banking data. Bigtech firms have been allowed to amass vast amounts of customer data, unchecked and unregulated. Their business models are founded on their ability to mine this data, find patterns and predict behaviours. They are better placed than banks to understand spending habits and predict likelihoods of default – and their operations are far more efficient and cost effective.

Delegates expressed that Facebook’s announcement of Libra has the potential to create an entirely new global financial system. While regulators have spoken out against Libra and support from industry players has dwindled, crypto assets are changing the face of financial services. Regulators are right to be concerned about its impact on consumers, investors, monetary policies and global economies.

> *“Open banking is not just about big banks sharing with the little guy; open banking would mean data would have to be shared with everyone.”*

Open banking in South Africa and the rest of the continent: “In Africa, small business equals big business”

A number of speakers highlighted the opportunities for open banking in South Africa, and the African context more broadly. MSMEs are the real drivers of economic activity and growth. They provide employment and income opportunities and ensure that wealth is distributed more equitably. They are central to sustainable growth on the continent – but they often lack the access to capital, credit and other financial services products that could help them grow their businesses. Poor or patchy business data, low levels of business formality, and high financing costs are some of the reasons these enterprises struggle access formal and traditional financial markets. Fintechs are able to use innovative technology to bridge some of these gaps; for example, by using non-traditional data sources to verify customer behaviour (such as social media or utility payment history) to assess credit worthiness. Case study 9 below describes Yoco, a technology company targeting MSMEs in South Africa.

Delegates discussed some of the considerations around open banking in South Africa. Many felt that initiatives should be market-led and supported by regulators rather than mandated through regulation.

There was agreement that the financial services sector needs a clear understanding of what an open banking framework is trying to solve for in the South African context. Additionally, this framework should be shaped around the specific dynamic of the South African market as opposed to a 'copy and paste of international regulations or frameworks'. Delegates felt that open banking could address the following objectives: increasing competition; improving financial inclusion; increasing digitisation and reducing the dependency on cash; improving customer experiences and service; and reducing the cost of banking.

Some delegates also argued that the term should be broadened to 'open finance', to include data from other markets participants, such as mobile network operators. The concept of a 'reciprocity model' was also discussed, whereby data can be shared across industries and players, enabling banks to use external data sets to improve their products and services.

Case study 7: YOCO

Yoco is an African technology company that builds tools and services to help small businesses get paid, run their business better, and grow.

It was founded by four friends in 2013 who identified a gap for services, products and platforms that support African small business. They had a vision that by opening up more possibilities for entrepreneurs to be successful, they can help create more jobs, enable people to thrive and help to drive our economy forward.

Yoco's core customer is a self-directed entrepreneur running a small business in South Africa, previously ignored and underserved by traditional financial institutions. These are daily and weekly traders operating in industries such as retail, food and drink, health and beauty services with monthly turnover from ZAR 10,000 (USD 700) to ZAR 200,000 (USD 14,000). At present, the company's core products include: a mobile point of sale reader, a POS system, business capital, business tools and accessories. They have on-boarded 48,000 merchants nationwide since 2015.

Their model is based on reducing complexity for the merchant. They use digital channels to target small businesses at scale. Merchants are able to on-board digitally with no human intervention – the process takes 5 minutes. Real time transactions reduce fraud and give the merchant control; and there is support available over the phone, via email, chat and social media.

Yoco has been able to challenge stereotypes surrounding small businesses such as they prefer to transact in cash, they do not want to formalise, or they are not economically viable. In 2018 chargebacks of Yoco merchants were at 0%.

The business philosophy is that "the smallest investment in MSMEs has a multiplying effect compounding locally within the community."

Conclusion: Regulatory actions to support open banking

Open banking presents an innovative opportunity to increase access to finance, enhance market competition, and develop the financial services ecosystem. However, a number of barriers exist which undermine the prospect for open banking in South Africa. While delegates expressed that open banking should be market-led, many recognised that regulators have a responsibility to facilitate and enable elements of an open banking framework, such as:

- **Customer protection:** ensuring that customers are treated fairly, their money is protected and that there is transparency so that customers understand the risks of consenting to the sharing of their data. There needs to be more consideration around data, who owns it and how it is used. For example, aggregated data to demonstrate a trend has different ethical considerations to using a customer's individual data to cross-sell products or services.
- **Licencing:** evaluating the business models of fintechs and other third-party service providers to understand the risks they pose to the financial system. As part of this, delegates noted the need to ensure that there are "fair playing fields" and that incumbent institutions are not held to regulations that impact their costs and efficiencies that smaller competitors are exempt from.
- **Establishing the parameters:** stakeholders agreed that guidelines, agreed use cases and common standards would be necessary for the industry to work together. Some also suggested that experimentation with data sharing should start with the non-competitive areas of the value chain, such as fraud. Lessons from international markets show that the costs for open banking can be crippling to the banking industry. Therefore, regulators should consider prioritising areas and following a phased or targeted approach, focusing on the areas that can add value to customers.

As in the workshop on innovation, delegates recognised that the government cannot facilitate innovations in open banking independently, even those which rely on regulatory actions. Delegates agreed that a consultative approach between regulators, policymakers and market participants is necessary to ensure that innovation meets market needs and that regulators can manage the risks without stifling innovation.

The pace of technological advancement means that we can expect the pace of innovation to continue. If there are clear, well understood rules applied to all market participants, there is no reason why innovation should be seen as a threat.