International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, June 13, 2022

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

These days, the crypto industry reminds me the Latin proverb "*perfer et obdura; dolor hic tibi proderit olim"* (be patient and tough; some day this pain will be useful to you).

"Crypto-assets, including stablecoins and decentralized finance (DeFi), as an emerging industry and asset class, offer new opportunities, but also significant challenges. Technology is blurring one of the last functional boundaries, the distinction between an individual and a financial intermediary." This is part of the paper with title *Fintech and the Future of Finance, Overview Paper,* from the World Bank Group. I liked the first words of this paper:

"The monumental challenges we face today, from COVID-19 to the war in Ukraine, have reminded us that throughout history, turbulent times are often accompanied by innovation. The technology-enabled innovation in

financial services —known as fintech—is one such example, accelerating rapidly as pandemic shutdowns amplified its importance for maintaining business activity and financial services during a time of social distancing."

We also read that Distributed Ledger Technologies (DLT) underpin new decentralized financial infrastructures that reduce or remove the role of intermediaries, enabling users to interact directly on a peer-to-peer basis and providing open-source platforms that anybody can use and build upon, spurring innovation and network effects and giving rise to new, interoperable financial services and vibrant ecosystems.

Crypto-assets, including stablecoins, and DeFi are DLT-based decentralized forms of digital value and financial services that aim to serve a range of economic functions. They hold promise for financial innovation, inclusion, efficiency, capital formation, and transparency.

For example, they could improve the speed and cost of cross-border payments and remittances. However, these new technologies carry significant risks related to, among others, financial integrity, consumer and investor protection, financial stability, fair competition, and monetary sovereignty.

Some types of crypto-assets notably global stablecoins have the potential to attract broad public usage as a means of payments including in the De-Fi ecosystems. In this context, public authorities are exploring issuing Central Bank Digital Currencies (CBDCs).

Widespread adoption of crypto-assets could challenge the primacy of public money with implications for, among others, monetary policy and financial stability.

Some authorities have also noted the concentration, data protection, and privacy risks that large-scale payment service providers can pose, particularly the ones employing a data monetization-led business strategy.

It is perceived that a CBDC, being a digital version of fiat currency, could imbue public money with the necessary digital features and enable it to provide a safer and efficient alternative to society, while promoting competition and innovation.

The perceived potential of CBDCs to advance financial inclusion is also of interest to some public authorities, notably the EMDEs. CBDCs however are not a panacea for financial inclusion since key behavioral, technological, and infrastructural barriers faced by other digital payment solutions may remain in place.

Several jurisdictions and international standard-setting bodies are studying design options and developing roadmaps to introduce CBDCs. The scale and pace of adoption and implications are not fully clear at this point, but the general thrust appears to position CBDCs as co-existing with other forms of money and payment mechanisms.

CBDCs could be limited for use by regulated financial-sector players — wholesale or open-to-all retail CBDCs. Wholesale CBDCs, given their limited use, do not pose any significant policy challenges.

A *retail CBDC* may however adversely impact bank funding and credit intermediation, impact monetary stability, distort the level playing field, and raise financial integrity and data privacy challenges. As such, careful attention needs to be given to various implementation options related to, for example, distribution, wallet limits, privacy features, onboarding, and verification mechanisms.

Read more at number 1 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 6)

Fintech and the Future of Finance

THE WORLD BANK
IBRD • IDA

Number 2 (Page 13)

Cyber security for farmers

Guidance to help farmers improve the security and resilience of their business against cyber threats.

National Cyber Security Centre

Number 3 (Page 16)

Risks of using AI to grow our food are substantial and must not be ignored, warn researchers

UNIVERSITY OF CAMBRIDGE

Number 4 (Page 18)

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

United States Senate Committee on
Homeland Security & Governmental Affairs
U.S. Senator Gary Peters | Chairman

Number 5 (Page 25)

Revisiting a paper that answers many questions asked in Davos

Climate-related risk drivers and their transmission channels

BANK FOR INTERNATIONAL SETTLEMENTS

Number 6 (Page 28)

Regulation and Supervision of Fintech: Considerations for EMDE Policymakers

THE WORLD BANK
IBRD • IDA

Number 7 (Page 31)

What Does Digital Money Mean for Emerging Market and Developing Economies?

THE WORLD BANK
IBRD • IDA

Number 8 (Page 34)

Global Cybersecurity Outlook

Karen Tso, Chander Prakash Gurnani, Jürgen Stock, Josephine Teo, Robert M. Lee

WORLD ECONOMIC FORUM

Number 9 (Page 35)

Central Bank Digital Currencies

Julia Chatterley, Kristalina Georgieva, Sethaput Suthiwartnarueput, François Villeroy de Galhau, Axel Lehmann

WORLD ECONOMIC FORUM

Number 10 (Page 36)

Where Will the Jobs of Tomorrow Come From?

Rebecca Blumenstein, François-Philippe Champagne, Jos De Blok, Dipu Moni, Mikael Damberg

WORLD ECONOMIC FORUM

Number 1

Fintech and the Future of Finance

THE WORLD BANK
IBRD • IDA

The ongoing digitization of financial services and money creates opportunities to build more inclusive and efficient financial services and promote economic development. This digital transformation presents a paradigm shift that has various policy implications, including:

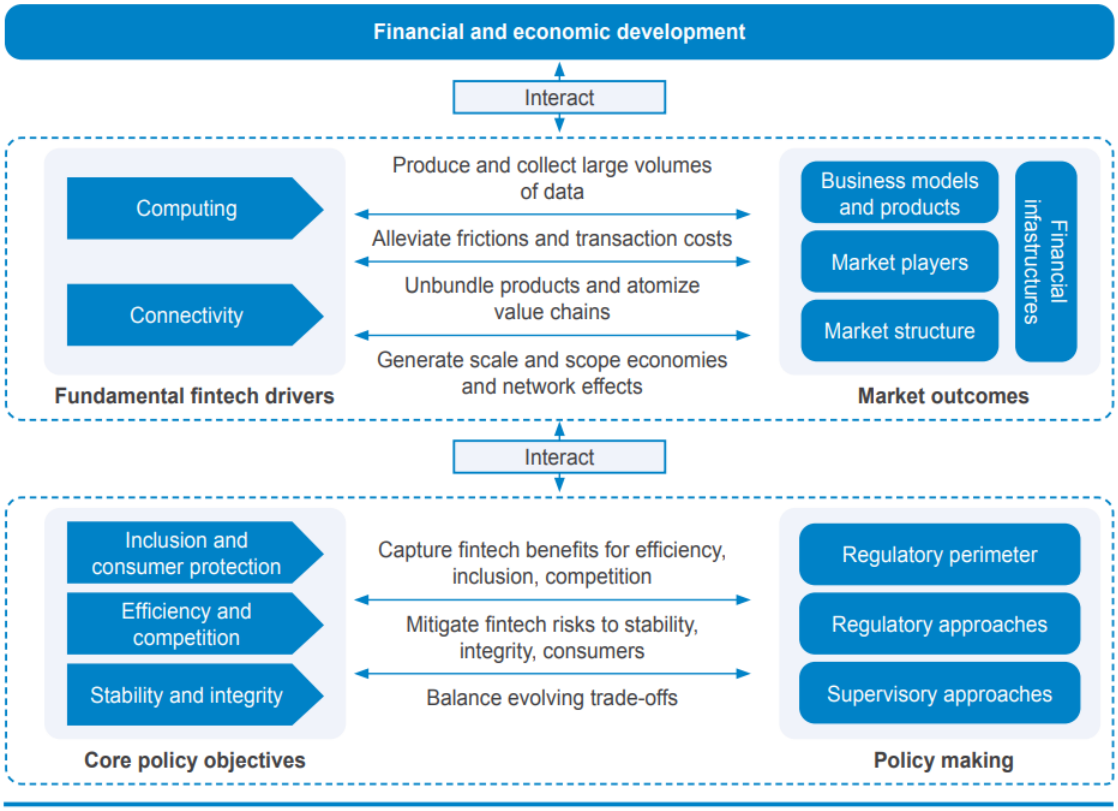
- Foster beneficial innovation and competition, while managing the risks.
- Broaden monitoring horizons and re-assess regulatory perimeters as embedding of financial services blurs the boundaries of the financial sector.
- Be mindful of evolving policy tradeoffs as fintech adoption deepens.
- Review regulatory, supervisory, and oversight frameworks to ensure they remain fit for purpose and enable the authorities to foster a safe, efficient, and inclusive financial system.
- Anticipate market structure tendencies and proactively shape them to foster competition and contestability in the financial sector.
- Modernize and open up financial infrastructures to enable competition and contestability.
- Ensure public money remains fit for the digital world amid rapid advances in private money solutions.
- Pursue strong cross-border coordination and sharing of information and best practices, given the supra-national nature of fintech.

This flagship report explores the implications of fintech and the digital transformation of financial services for market outcomes on one side, and regulation and supervision, on the other, and how these interact.

This Overview Paper provides a high-level perspective for senior policy makers and is accompanied by a set of notes that focus in detail on selected salient issues for a more technical audience.

Figure 1 below lays down a conceptual framework for fintech, and the interactions between markets, policy, and development.

Figure 1. Conceptual Framework for Fintech: Interactions between Markets, Policy, and Development



Source: Authors' elaboration.

The Fundamental Drivers of Fintech

Technology-enabled innovation in financial services, fintech, is re-shaping financial products, payments, business models, market players, market structure and even money itself.

The adoption of fintech was accelerated by the COVID-19 pandemic. Fintech adoption can further financial development by promoting core policy objectives such as financial stability, integrity, inclusion, efficiency, innovation, and competition, and provide firm foundations for the digital economy to flourish.

Fintech-enabled business models and products can support economies to become more resilient and promote an equitable recovery from the COVID-19 pandemic (World Development Report 2022).

At the same time, a balanced policy approach is required to also mitigate various risks related to, among others, financial stability and integrity, consumer and investor protection, and data privacy. The two fundamental drivers of this wave of fintech are ubiquitous connectivity through mobile,

internetconnected devices and communication networks, and low-cost computing and data storage.

Together these enable new business models for the delivery of technology, such as cloud computing. Applications leveraging these advances, such as e-commerce and mobile apps, create reams of Big Data about users and transactions.

Low-cost computing and storage allow that data to be mined for insights. Data and connectivity can alleviate key frictions in the provision of financial services, such as information asymmetries and transactions costs, and have enabled a wide range of data-driven process automation and product applications, from credit and insurance underwriting to investment robo-advisors.

Datadriven business models are able to scale rapidly, leveraging positive feedback loops from customer activity that generates data that is used to provide additional services, which in turn generate more user engagement and data.

Lenders that previously relied on a borrower's credit history or collateral to fill information gaps about cash flows and ability to repay can use data-driven credit scores and real time payments data on cash flows to extend credit to previously underserved individuals and small and medium enterprises (SMEs), reaching them at lower cost through mobile channels.

These drivers enable the reconfiguration of the value chains that produce financial services.

Transaction costs and barriers to information flows have long defined the scope of what was produced within a single firm; reduced transaction costs and friction-free information flows allow a reconfiguration of financial services value chains and product bundles.

Connectivity and data exchange allow a product or service to be broken up into distinct components (atomization), which can be offered by different providers and recombined in new ways.

Account opening, for example, has moved from a single-provider service delivered at the bank branch using its own front and back office, to a range of potential configurations: an account at a bank might be opened through the physical locations or the mobile app of a partner such as a retailer or an e-commerce platform, with ID verification provided by a specialized fintech, the ledger sitting on an outsourced cloud-based IT infrastructure, and customer service provided by an off-shore call center.

That account might be branded as a product of the bank or might be delivered by the partner as a service 'powered by' with the consumer barely aware of the underlying financial institution.

The ability of customers and providers to access information and move funds more easily has enabled the unbundling of financial services: specialized providers offer single products and customers are able to choose a set of service providers that collectively meets their needs.

Rather than using the deposit, payment, and loan products of a single institution, the customer can choose to keep deposits in one (or more), shop around for the best loan offer, and use different payments providers for different uses–paying bills, splitting a restaurant bill, or sending money overseas.

Customers can now assemble their own set of services and bundle them at the level of app icons on a smartphone screen. Critically, the same advances in computing power, data, and connectivity allow services providers, who do not own the whole customer financial relationship (as banks once did), to provide single solutions and new packages of financial services, or rebundle financial services with other business or commercial activities.

Atomization, unbundling, and rebundling are re-shaping business models and product economics as well as the provider landscape.

An account holder might choose a 3rd party application for remote access to an account, effectively separating the account-holding institution from the end product and user interface–and much of the consumer value creation.

Economy-wide trends such as wider use of application programming interfaces (APIs) in technology architecture and the rise of multi-party platforms in e-commerce, logistics, and other sectors further enable information exchanges and the rebundling of financial services, which are being embedded into non-financial products and workflows.

The introduction of variable and on-demand (cloud-based) infrastructure, automation, remote channels, and capital-light and embedded business models is reducing costs to customers.

The new array of customer-facing providers will, however, take some of the margin that was previously earned by banks, even where regulation may still require that a bank sit behind the product.

Fintech: What it is and Why it Matters

There are a number of ways to define fintech.

The Bali Fintech Agenda, FSB, and others broadly define fintech as "advances in technology that have the potential to transform the provision of financial services, spurring the development of new business models, applications, and processes, and products." (IMF/World Bank 2018)

In the accompanying technical notes, specific technologies are addressed where relevant. The overall focus, however, is on the market trends and regulatory implications of the digital transformation of finance in the context of rapidly digitizing economies rather than on specific technologies that may have currency today and get superseded tomorrow.

For that reason, this report starts its analysis with key drivers of change on the technology side and links these to the underlying economics of financial intermediation: the economic frictions that gave rise to intermediaries, and the economic forces that shaped their scope and scale.

Technology can lower costs and increase the speed, transparency, security, and availability of more tailored financial services.

Digitization can reduce frictions in each step along the financial service lifecycle, from opening an account to conducting customer due diligence, authenticating transactions, and automating other, product-specific processes, such as assessing creditworthiness.

Fintech is therefore characterized by low marginal costs per account or transaction and scale efficiencies. Fintech can also enhance transparency and reduce information asymmetries since digital processes generate a data trail, which can be used to better understand consumers, improve products, manage risks, and promote regulatory compliance.

The use of technology in finance has a long history.

In fact, since finance involves high-value activities, there has always been an incentive to use the latest technology, whether that was the finest scales to weigh gold pieces or the fastest communication methods of the day, from Rothschild's carrier pigeons to Reuter's telegraph.

Digital technology made its way into finance as the second major application of electronic computers after the military. The first wave of financial technology in the 1950s to 1970s saw bespoke mainframe computer systems become part of the fabric of the back office and then

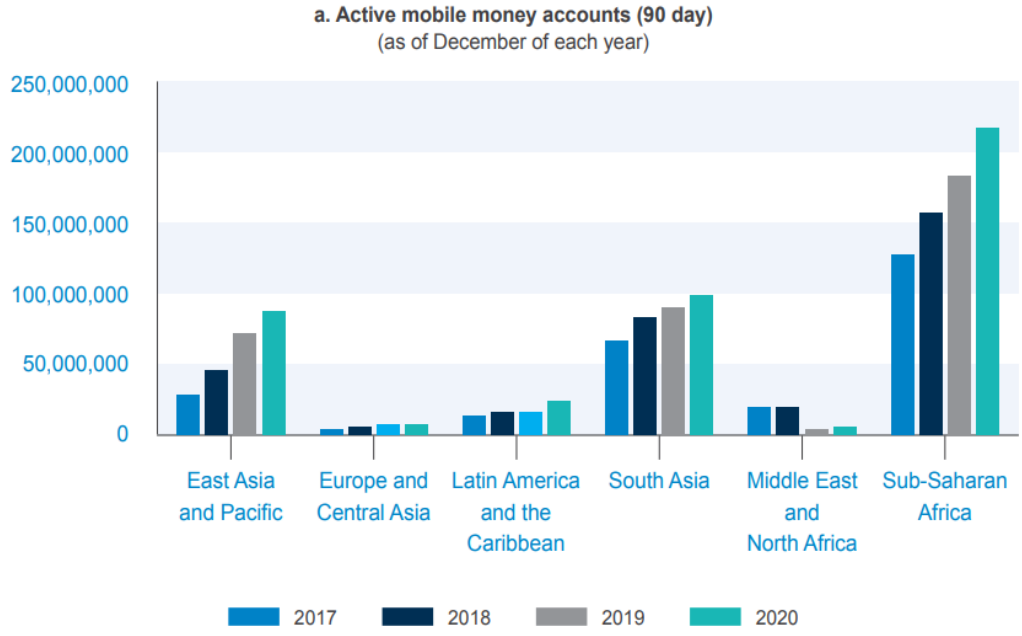
gradually the middle and front offices of most large financial institutions. The late 1960s through the 1980s saw the emergence of digital technology companies dedicated to serving financial institutions, including core banking system providers like FIS and Fiserv, and payments networks like Mastercard and SWIFT.

The current wave of fintech innovation is marked by the technology companies increasingly interacting directly with customers and becoming the providers of financial services themselves.

This wave leverages the increasingly sophisticated technology that is in the hands of increasingly sophisticated customers, along with innovations in business models, to disaggregate services and offer new reconfigurations of products directly to individuals and business users.

That has resulted in disruptive changes to the market in terms of the pace of technological advances, who is providing financial services, and how consumers use those services and interact with providers.

Figure 2. Growth in Mobile Money Accounts and Transactions (By Volume and Value) Between 2017-2020

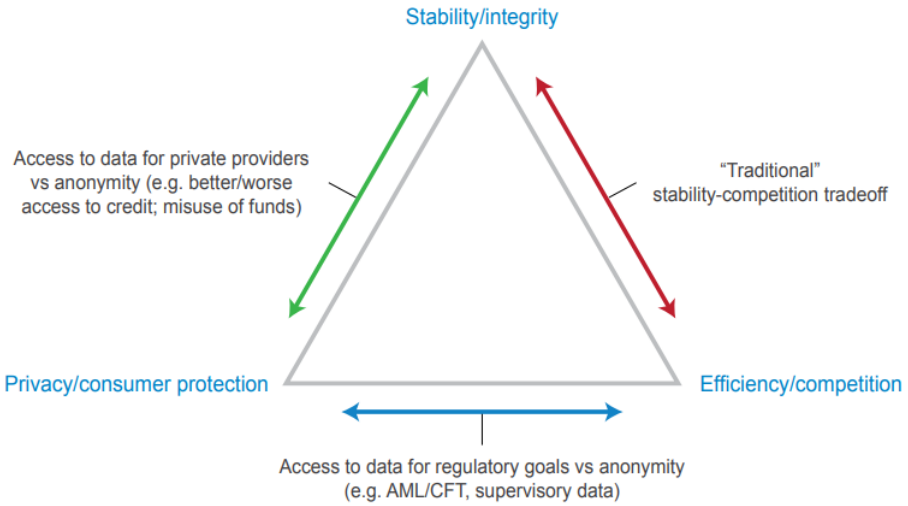


This is evident, for example, in the statistics on global uptake of mobile-money accounts and increases in mobile-money transactions.

The Global Findex surveys show that mobile-money operators added more than twice as many accounts as banks in sub-Saharan Africa from 2014 to 2017, becoming the key drivers of increased financial access.

A significant majority (92 percent) of respondents to the Fintech Market Participants Survey2 indicated that fintech and digital transformation is a strategic priority at the board level for their organizations.

Figure 15. Policy Trade-Offs Due to Fintech Developments



Source: Market Structure note, World Bank Group and Bank for International Settlements.

To read more:
https://www.worldbank.org/en/publication/fintech-and-the-future-of-finance

Number 2

Cyber security for farmers

Guidance to help farmers improve the security and resilience of their business against cyber threats.

National Cyber Security Centre

The NCSC has worked with the National Farmers Union to support the Agriculture and Farming Sector with this guide especially created for the industry.

The increased use of email, online accounting tools, online payment systems as well as automated farming equipment means that its increasingly important for farmers and rural communities to look at their growing exposure to cyber risks and how they can best protect themselves and their businesses.

The guide has been written to be clear and understandable for a range of technical abilities, to help you become more aware or enhance your knowledge of cyber security measures. It offers advice in the form of tips for you to easily implement to become a more resilient and secure business.

Whilst we can't guarantee that you'll be protected from all forms of cyber attack, following this advice will significantly increase the protections you have from the most common cyber crimes.

Why cyber security matters in Farming

We all keep information about ourselves and our businesses electronically. This is particularly true for the agricultural sector, which makes use of many 'smart', internet connected systems as well as the usual email and accounting packages.

These internet-connected technologies have become central to the way we live and do business today. As a direct result, they have become an attractive target for cyber criminals.

This is why it's so important to secure all the digital aspects of your business. So, what are the digital aspects of your business?

Firstly, your IT and other computerised equipment. This means everything from the computer where you do your emails and run your farm management software, to the automated machinery, security cameras and smart phones which help you run your farm.

The second aspect to keep in mind involves your online activity. You must consider all the online accounts that you use. This means banking, email and social media but also things like the Rural Payments service, HMRC online services, online shopping and cloud document storage (e.g. Office365, Google Docs, DropBox etc).

This guide has been produced by the NCSC and NFU to help you protect your devices and accounts from the unwanted attention of Cyber Criminals. By following the steps in this guide, you should be in a much more secure and resilient position.

Protect your farm from malware

The name 'malware' comes from the joining of two words: malicious software. This is the slightly more technical term for 'a computer virus.'

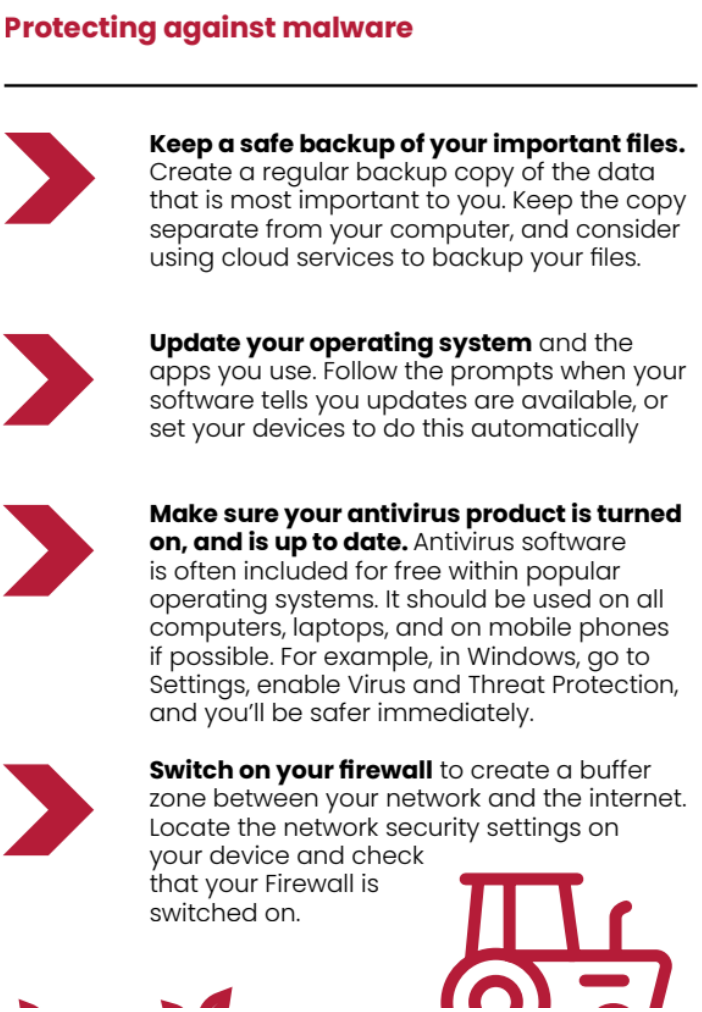
Malware is usually designed to steal or extort money from you, often by holding your data to ransom.

Malware can attack your laptop and your phone, but it can also target less obvious 'devices.' Anything which connects to the internet is at risk from malware.

For example, malware could:

• Lock your device or make it unusable

- Immobilise your farm vehicles
- Steal, delete or encrypt your data
- Interfere with any automated systems which you use
- Use services that cost you money, such as premium rate phone calls
- Divert your confidential farm data into the public domain



To read more:
https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf

Number 3

Risks of using AI to grow our food are substantial and must not be ignored, warn researchers

UNIVERSITY OF CAMBRIDGE

Artificial intelligence (AI) is on the cusp of driving an agricultural revolution, and helping confront the challenge of feeding our growing global population in a sustainable way. But researchers warn that using new AI technologies at scale holds huge risks that are not being considered.

Imagine a field of wheat that extends to the horizon, being grown for flour that will be made into bread to feed cities' worth of people. Imagine that all authority for tilling, planting, fertilising, monitoring and harvesting this field has been delegated to artificial intelligence: algorithms that control drip-irrigation systems, self-driving tractors and combine harvesters, clever enough to respond to the weather and the exact needs of the crop. Then imagine a hacker messes things up.

A new risk analysis, published today in the journal Nature Machine Intelligence, warns that the future use of artificial intelligence in agriculture comes with substantial potential risks for farms, farmers and food security that are poorly understood and under-appreciated.

"The idea of intelligent machines running farms is not science fiction. Large companies are already pioneering the next generation of autonomous ag-bots and decision support systems that will replace humans in the field," said Dr Asaf Tzachor in the University of Cambridge's Centre for the Study of Existential Risk (CSER), first author of the paper.

"But so far no-one seems to have asked the question 'are there any risks associated with a rapid deployment of agricultural AI?'" he added.

Despite the huge promise of AI for improving crop management and agricultural productivity, potential risks must be addressed responsibly and new technologies properly tested in experimental settings to ensure they are safe, and secure against accidental failures, unintended consequences, and cyber-attacks, the authors say.

In their research, the authors have come up with a catalogue of risks that must be considered in the responsible development of AI for agriculture – and ways to address them. In it, they raise the alarm about cyber-attackers potentially causing disruption to commercial farms using AI, by poisoning datasets or by shutting down sprayers, autonomous drones, and robotic harvesters.

To guard against this they suggest that 'white hat hackers' help companies uncover any security failings during the development phase, so that systems can be safeguarded against real hackers.

In a scenario associated with accidental failure, the authors suggest that an AI system programmed only to deliver the best crop yield in the short term might ignore the environmental consequences of achieving this, leading to overuse of fertilisers and soil erosion in the long term.

Over-application of pesticides in pursuit of high yields could poison ecosystems; over-application of nitrogen fertiliser would pollute the soil and surrounding waterways. The authors suggest involving applied ecologists in the technology design process to ensure these scenarios are avoided.

Autonomous machines could improve the working conditions of farmers, relieving them of manual labour. But without inclusive technology design, socioeconomic inequalities that are currently entrenched in global agriculture - including gender, class, and ethnic discriminations - will remain.

"Expert AI farming systems that don't consider the complexities of labour inputs will ignore, and potentially sustain, the exploitation of disadvantaged communities," warned Tzachor.

To read more:
https://www.cam.ac.uk/research/news/risks-of-using-ai-to-grow-our-food-are-substantial-and-must-not-be-ignored-warn-researchers

Number 4

Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns

United States Senate Committee on Homeland Security & Governmental Affairs
U.S. Senator Gary Peters | Chairman

Ransomware is a dangerous form of cyber-attack where threat actors prevent access to computer systems or threaten to release data unless a ransom is paid.

It has the power to bankrupt businesses and cripple critical infrastructure – posing a grave threat to our national and economic security.

The use of cryptocurrencies has further enabled ransomware attacks, particularly because cryptocurrency is decentralized and distributed and illicit actors can take steps to obscure transactions and make them more difficult to track.

In recent years, ransomware attack victims have included hospitals, school systems, local, state, and federal government agencies, as well as other critical infrastructure, including the water and energy sectors.

In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the United States.

According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and "are outpacing societies' ability to effectively prevent or respond to them."

Many of these attacks generated significant losses and damages for victims. A threeyear comparison of the number of complaints of ransomware submitted to the Federal Bureau of Investigation (FBI) between 2018 and 2020, demonstrates a 65.7 percent increase in victim count and a staggering 705 percent increase in adjusted losses.

In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million. However, even these figures likely drastically underestimate the actual number of attacks and ransom payments made by victims and related losses.

In fact, the FBI acknowledges that its data is "artificially low." Further evidence of this under-reporting is that the government data is significantly lower than several private sector estimates.

For instance, Chainalysis, a blockchain data and analysis company that works with financial institutions, insurance and cybersecurity companies, and as a contractor for the U.S. government, reports that in 2020, malign actors received at least $692 million in cryptocurrency extorted as part of ransomware attacks, up from $152 million in 2019, close to a 300 percent increase over a two-year period.

A separate study by the anti-malware company Emsisoft found that there were at least 24,770 ransomware incidents in the U.S. in 2019 and estimated their costs (including costs of downtime) at just under $10 billion.

To better understand this growing threat, U.S. Senator Gary Peters, Chairman of the Senate Homeland Security and Governmental Affairs Committee, announced in July 2020 an investigation into the role of cryptocurrency in incentivizing and enabling ransomware attacks, and the resulting harm of such attacks to victims.

As a part of this ten-month investigation, Committee staff conducted interviews with federal law enforcement and regulatory agencies as well as private companies that assist ransomware victims with ransom demands.

While not exhaustive, this report addresses key pieces of the larger landscape of the increasing national security threat from ransomware attacks and the use of cryptocurrency for ransom payments.

The report details recommendations to address current gaps in information on ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

The report finds that there is a lack of comprehensive data on the amount of ransomware attacks and use of cryptocurrency as ransom payments in these attacks.

While multiple federal agencies are taking steps to address the increasing threat of ransomware attacks, more data is needed to better understand and combat these attacks.

In interviews with Committee staff, federal officials and private sector companies each acknowledged the need for more compliance and data (e.g., reporting of incidents and ransom payments).

When more data is collected, the federal government will be in a better position to assist existing and potential cybercrime victims with prevention, detection, mitigation, and recovery.

Such information also facilitates more efficient investigation and prosecution of illicit actors.

To address the current lack of information regarding the breadth and depth of the ransomware threat, Chairman Peters and Ranking Member Portman introduced the Cyber Incident Reporting Act of 2021, which passed the Senate as part of the Strengthening American Cybersecurity Act of 2022.

The incident reporting provisions later became law as the Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the Consolidated Appropriations Act of 2022 in March 2022. The new reporting mandates in the law will begin to address this problem.

Nevertheless, as indicated by the findings in the report, the Administration and Congress must remain vigilant against this growing threat. Almost 40 million Americans – including approximately three-in-ten Americans age 18 to 29 – have engaged in some form of investment, trade, or other legitimate use of cryptocurrencies according to a November 2021 estimate by the nonpartisan Pew Research Center.

The global market value of all cryptocurrencies reached $3 trillion in 2021, up from $14 billion in 2016. However, according to multiple agencies interviewed by Committee staff, cryptocurrency, typically Bitcoin, has become a near universal form of ransom payment in ransomware attacks, in part, because cryptocurrency enables criminals to extort huge sums of money from victims across diverse sectors with incredible speed.

The payment structure's decentralized nature, as well as irregular regulatory compliance by some entities within the space and new anonymizing techniques contribute to the challenges law enforcement faces when seeking to arrest criminal actors, particularly foreign-based actors.

High profile attacks, such as Colonial Pipeline, demonstrate ransomware attackers' threat to national security. The FBI's recovery of over half of the ransom paid by Colonial Pipeline, however, shows that with access to the right information, law enforcement can leverage cryptocurrency's unique features as well as other investigative techniques to track down cyber criminals and recover stolen funds.

Unfortunately, data reporting and collection on ransomware attacks and payments is fragmented and incomplete. Two federal agencies claim to host the government's one stop location for reporting ransomware attacks – the Cybersecurity and Infrastructure Agency (CISA) StopRansomware.gov website and the FBI's IC3.gov.

These two websites are separate and, while the agencies state that they share data with each other, in discussions with Committee staff, ransomware incident response firms questioned the effectiveness of such communication channels' impact on assisting victims of an attack.

Many federal regulators have taken steps to address the rising threat of ransomware attacks by issuing new, and expanding existing, regulations and guidance.

Generally, with respect to cryptocurrency, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has clarified that "money service businesses", e.g., persons that accept and transmit "value that substitutes for currency", are subject to key financial regulations.

Over the past few years, the Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and FinCEN have each issued new guidance and regulations subjecting cryptocurrency to additional oversight.

In 2021, the Department of Justice (DOJ), SEC, and the Treasury Department's Office of Foreign Assets Control (OFAC), among other agencies, also issued guidance recognizing the need for more ransomware incident reporting.

On March 9, 2022, the Biden Administration issued an Executive Order outlining a "whole-of-government" approach to examining the risks associated with the sharp increase in use of cryptocurrencies. Among other key policy priorities, the Administration recognizes that cryptocurrencies have "facilitated sophisticated cybercrime-related financial networks and activity, including through ransomware activity."

The data needed to support these initiatives, among other agency efforts to tackle ransomware and cryptocurrency ransom payments, however, is fragmented and incomplete.

This limited collective understanding of the ransomware landscape and the cryptocurrency payment system blunts the effectiveness of available tools to protect national security and limits private sector and federal government efforts to assist cybercrime victims.

As Russia's invasion of Ukraine continues and Russia seeks to find ways around the international finance system, the need to address these shortfalls grows. Approximately 74 percent of global ransomware revenue in 2021 went to entities either likely located in Russia or controlled by the Russian government.

Further, CISA and other federal agencies have warned that Russia's invasion of Ukraine could lead to additional malicious cyber activity, including ransomware attacks, in the United States.

Therefore, as the report finds, prioritizing the collection of data on ransomware attacks and cryptocurrency payments is critical to addressing increased national security threats.

FINDINGS OF FACT

1. The federal government lacks comprehensive data on ransomware attacks and use of cryptocurrency in ransom payments.

The government largely relies on voluntary reporting of ransomware attacks and cyber extortion demands, which only captures a fraction of the attacks that occur.

As of July 2021, the Cybersecurity and Infrastructure Security Agency (CISA), which was created in 2018 specifically to reduce risk to the nation's cyber and physical infrastructure, estimated that only about one quarter of ransomware incidents were reported.

2. Current reporting is fragmented across multiple federal agencies.

Data on ransomware attacks is reported to numerous federal agencies including CISA, the FBI, and the Treasury Department's FinCEN, among others. These agencies do not capture, categorize, or publicly share information uniformly.

3. Lack of reliable and comprehensive data on ransomware attacks and cryptocurrency payments limits available tools to guard against national security threats.

The lack of data on ransomware attacks and cryptocurrency ransom payments blunts the effectiveness of available tools for fighting ransomware attacks including U.S. sanctions, law enforcement efforts, and international partnerships, among other tools.

4. Currently available data on ransomware attacks and cryptocurrency payments limits both private sector and federal government efforts to assist cybercrime victims.

The private sector and the federal government are not able to fully and

effectively assist victims to prevent or recover from ransomware attacks without a comprehensive dataset on ransomware attacks, ransom demands, and payments. Such a dataset does not currently exist.

RECOMMENDATIONS

1. The Administration should swiftly implement the new ransomware attacks and ransom payments reporting mandate.

CISA should complete the required rulemaking as soon as possible to implement the requirements in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 signed into law as part of the Consolidated Appropriations Act of 2022, which mandates incident reporting of substantial cyber-attacks and ransomware payments against critical infrastructure.

Federal agencies should implement the requirement in the law to share all cyber incident reports with CISA to enable a consolidated view of incidents from across different sectors and reported under different regulatory regimes.

2. The federal government should standardize existing federal data on ransomware incidents and ransom payments to facilitate comprehensive analysis.

Agencies should standardize how data from existing reporting requirements for ransomware incidents and ransom payments is organized and formatted across federal government agencies to enable more comprehensive information sharing and analysis.

3. Congress should establish additional public-private initiatives to investigate the ransomware economy.

The federal government should promote public-private partnerships to research the ransomware economy, in particular, the interrelationships between cybercriminals who conduct or facilitate ransomware attacks and the financial structures facilitated by cryptocurrencies that sustain cybercriminals' illicit activities, including privacy coins.

These partnerships should also examine ransomware infrastructure to help design and promote effective countermeasures.

4. Congress should support information sharing regarding ransomware attacks and payments including crowdsourcing initiatives.

Congress and relevant agencies should consider ways to support partners within the private, nonprofit, and academic sectors seeking to expand the collection and organization of information on ransomware attacks including by examining federal funding options and sharing anonymized data regarding ransomware attacks and payments.

In addition, government agencies should collaborate with partners to identify viable crowdsourcing initiatives to pool information regarding ransomware attacks and extortion payments.

You may visit:
https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report.pdf

Number 5

Revisiting a paper that answers many questions asked in Davos

Climate-related risk drivers and their transmission channels

BANK FOR INTERNATIONAL SETTLEMENTS

This report explores how climate-related financial risks can arise and impact both banks and the banking system.

By synthesising existing literature, it illustrates how physical and transition climate risk drivers affect banks' financial risks via micro- and macroeconomic transmission channels. It also explores various factors that may determine the likelihood or size of the impact from climate-related risk drivers.

The report's main findings are as follows:

Banks and the banking system are exposed to climate change through macro- and microeconomic transmission channels that arise from two distinct types of climate risk drivers.

First, they may suffer from the economic costs and financial losses resulting from the increasing severity and frequency of physical climate risk drivers.

Second, as economies seek to reduce carbon dioxide emissions, which make up the vast majority of greenhouse gas (GHG) emissions, these efforts generate transition risk drivers. These arise through changes in government policies, technological developments, or investor and consumer sentiment. They may also generate significant costs and losses for banks and the banking system.

Credit risk

Climate risk drivers can impact household, corporate, or sovereign income and/or wealth. Physical and transition risk drivers increase a bank's credit risk as soon as they have a negative effect on a borrower's ability to repay and to service debt (the income effect) or on a bank's ability to fully recover the value of a loan in the event of default because the value of any pledged collateral or recoverable value has been reduced (the wealth effect). This credit risk impact takes many forms, which are explored in the examples drawn from the literature.

Physical risk drivers mainly impact banks' credit risk indirectly through their counterparties. The physical capital (housing, inventory, property, equipment or infrastructure 15) of households, corporates and sovereigns

can be damaged or destroyed by physical hazards. This damage reduces the value of assets and, consequently, a counterparty's wealth. Physical risk drivers can also negatively impact cash flows of the affected entities as damaged physical capital, such as impaired rental properties and factories, will generate less income.

The damage may be caused by acute physical risks, such as tropical storms, and also by chronic physical risks, such as rising sea levels. This section explores examples of how physical climate-related financial risks may crystallise in households, corporates and sovereigns.

Evidence shows that acute physical risks in the form of severe weather events reduce corporate profitability and potentially increase credit risk to lenders. Studies based on historical data find that natural disasters can result in short-term moderate decreases in corporate sales.

For example, US corporates have been shown to experience an average drop of 2 to 3 percentage points in sales growth following a major natural disaster that affects their suppliers, ultimately causing a 1% drop in corporates' equity value (Barrot and Sauvagnat (2016)).

An extensive body of literature and news articles have documented the impact of natural disasters on global supply chains, often referencing natural disasters in Japan and/or Thailand as case studies (Abe and Ye (2013); Park et al (2013); Bland and Kwong (2011)).

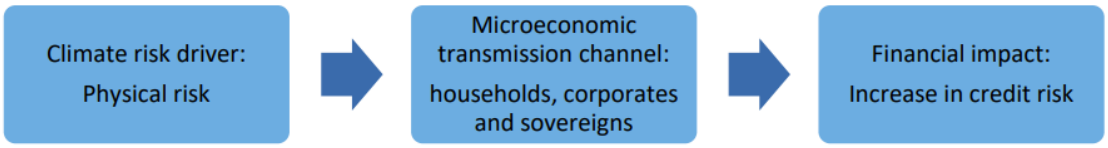
Global supply chains increase the potential for physical risks to impact banks' counterparties. This impact of climate change on corporates across countries is difficult to quantify, given the complexity of the global economic system, data gaps and methodological challenges (Andreoni and Miola (2014)).

However, the effects may be significant as developed countries are increasingly reliant on long supply chains and on supplies and services provided by countries vulnerable to climate risk. Companies in the S&P 500 index, for example, own physical assets across 68 countries globally, and 60% of these entities hold assets that are at high risk of at least one type of physical risk (Mattison (2020)).

Chronic physical risks, not necessarily reflected in historical data, are projected to negatively impact corporate credit portfolios primarily through income effects. A number of bank and industry scenario analyses project that incremental climate change, such as rising temperatures, drought and flood risk, may pose a greater risk to the financial health of borrowers than climate-related natural disasters (UNEP-FI (2018a,b)).

While severe droughts could increase bank corporate credit risk, the projected impact could vary by sector, geography, and reliance on hydropower (NCFA and GIZ (2017)).

The unprecedented nature of these changes increases the importance of climate-relevant data to better understand the ways in which chronic physical risks might impact economies and banks' financial risks.



To read more: https://www.bis.org/bcbs/publ/d517.pdf

Number 6

Regulation and Supervision of Fintech: Considerations for EMDE Policymakers

THE WORLD BANK
IBRD • IDA

Fintech is transforming the global financial landscape. It is creating new opportunities to advance financial inclusion and development in Emerging Markets and Developing Economies (EMDEs), but also presents risks that require updated supervision policy frameworks.

Fintech encompasses new financial digital products and services enabled by new technologies and policies.

Although technology has long played a key role in finance, recent fintech developments are generating disruptive innovation in data collection, processing, and analytics.

They are helping to introduce new relationship models and distribution channels that challenge traditional ways of finance, while creating additional risks.

While most of these risks are not new, their effects and the way they materialize and spread across the system are not yet fully understood, posing new challenges to regulators and supervisors.

For example, operational risk, especially cyber risk, is amplified as increasing numbers of customers access the financial network on a 24/7 basis. Likewise, increased reliance by financial firms on third parties for provision of digital services, such as cloud computing, may lead to new forms of systemic risks and concentration on new dominant unregulated players such as big tech firms.

This note aims to provide EMDE regulators and supervisors with high-level guidance on how to approach the regulating and supervising of fintech, and more specific advice on a few topics. Preserving the stability, safety, and integrity of the financial system requires increased attention to competition and ensuring a level playing field and to emerging data privacy risks.

As a general principle, policy response should be proportionate to risks posed by the fintech activity and its provider. While striking the right balance can be challenging in the absence of global standards, the IMF-World Bank Bali Fintech Agenda (BFA), along with guidance by Standard Setting Bodies, provides a good framework for reference.

A sound policy design must start with assessment of the fintech landscape, its risks and regulatory gaps. Simplicity and pragmatism—for example combining simple regulations with supervisory judgment—increases the odds of successful policy.

In practice, this will mean different things, depending on local context. In many cases, a clarification or review of existing frameworks will be sufficient and is easily done through enhanced supervisory guidance.

In others, a full regulatory overhaul might be required. In some systems, an activities-based, technology-neutral approach, based on the function of the financial service can help balance stability and innovation goals.

In others, a combined approach, taking into account the activity and the entity, might be necessary to ensure financial stability.

In any case, there needs to be clear definition of which activities are under the regulatory perimeter and which requirements apply, including the need for licenses.

Some fintech activities will require licences with integrity (AML/CFT) and conduct requirements. The introduction of data protection provisions in licensing frameworks is common. Activities that could potentially pose risks to stability should face prudential requirements.

Competition and inclusion objectives will become more relevant from a financial policy view, given the growing interdependencies and trade-offs with core priority mandates of preserving stability, integrity, and safety of the financial sector.

The multiplicity of new entrants and the potential for dominant players (for example, incumbents, big tech firms, platforms) and first movers (for example, M-Pesa) to create barriers and generate distortions has led to an increased recognition of the strong links between inclusion, competition, and financial stability.

Indeed, a targeted participation by financial service authorities in competition policy matters is increasingly being observed in EMDEs. The potential role of prudential and conduct regulation in mitigating barriers to market access and reining in abusive dominant practices should not be understated.

Cooperation, both interagency and cross-border, can help in the design and implementation of a sound supervisory response to fintech, which can be particularly challenging for EMDE countries suffering from

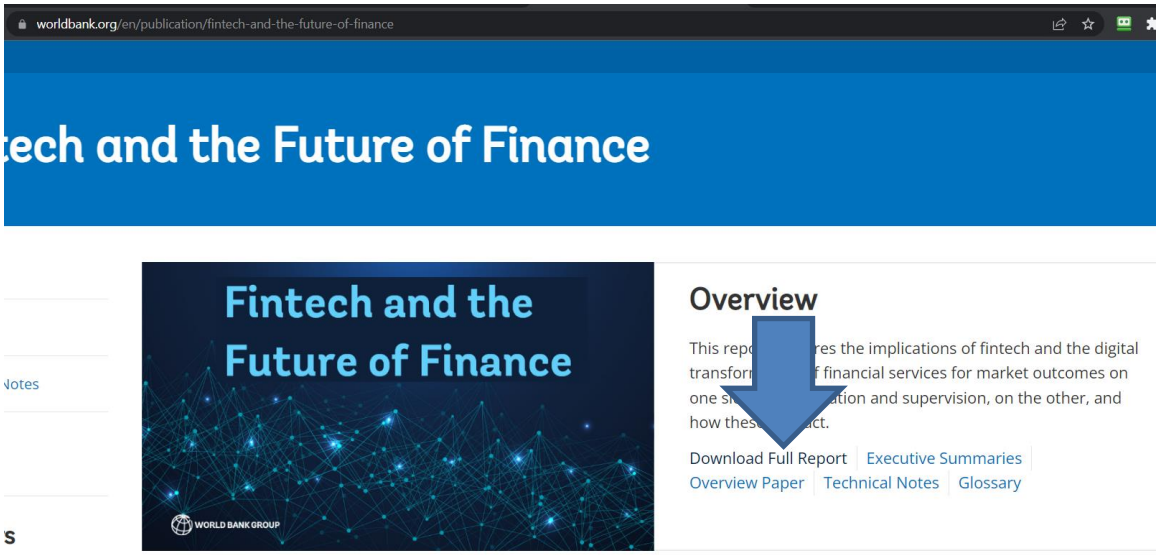
supervisory capacity constraints or juggling competing policy priorities.

An effective supervisory function for fintech activities is as essential as an appropriate regulatory regime. Supervisory processes and methods may need significant changes.

Supervisors' knowledge, skills, and tools should keep pace with the speed of innovation and related risks, including cyber threats.

Building proper expertise is crucial and suptech and regtech solutions could be excellent catalysts for this. Fintech is cross-sectoral and cross-country, making cooperation among agencies at the national and international levels essential for sound supervision.

To read more (please choose download full report) at:
https://www.worldbank.org/en/publication/fintech-and-the-future-of-finance



Number 7

What Does Digital Money Mean for Emerging Market and Developing Economies?

THE WORLD BANK
IBRD • IDA

Physical cash and commercial bank money are dominant vehicles for retail payments around the world, including in emerging market and developing economies (EMDEs).

Yet payments in EMDEs are marked by several key deficiencies—such as lack of universal access to transaction accounts, widespread informality, limited competition, and high costs, particularly for cross-border payments.

Digital money seeks to address these deficiencies.

This note categorizes new digital money proposals. These include crypto-assets, stablecoins, and central bank digital currencies (CBDCs). It assesses the supply and demand factors that may determine in which countries these innovations are more likely to be adopted.

It lays out particular policy challenges for authorities in EMDEs. Finally, it compares these with digital innovations such as mobile money, retail fast-payment systems, new products by incumbent financial institutions, and new entrants such as specialized cross-border money-transfer operators.

Proposals for global stablecoins have put a much-needed spotlight on deficiencies in financial inclusion, and in cross-border payments and remittances in EMDEs. Yet stablecoin initiatives are no panacea.

While they may achieve adoption in certain EMDEs, they may also pose particular development, macroeconomic, and cross-border challenges for these countries and have not been tested at scale.

Several EMDE authorities are weighing the potential costs and benefits of CBDCs. We argue that the distinction between token-based and account-based money matters less than the distinction between central bank and non-central bank money.

Fast-moving fintech innovations that are built on, or improve existing financial plumbing, may address many of the issues in EMDEs that both private stablecoins and CBDCs aim to tackle.

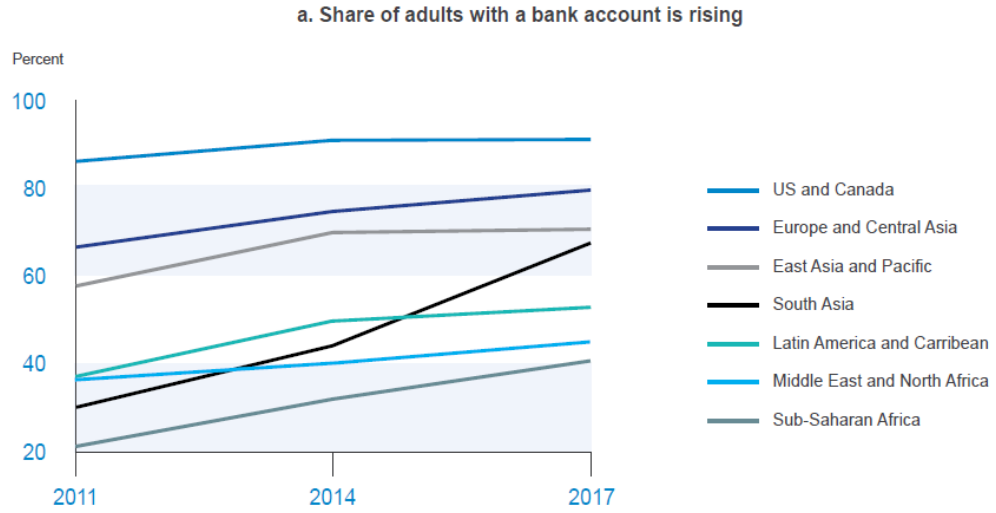
Introduction

From the ancient Indian rupya, to cacao beans in the Aztec empire, to the first paper money in China, money and payments have been evolving for centuries. The countries that are today called emerging market and developing economies (EMDEs), which collectively make up 84 percent of the world's population but only 37 percent of GDP at current prices, are no exception.

In recent decades, physical cash and claims on commercial banks (deposits) have become the main vehicles for retail payments around the world (Bech et al., 2018). Compared to physical cash, commercial bank money provides more safety, enables remote transactions, and allows banks to extend other useful financial services, This may ultimately benefit economic efficiency and enhance economic policy oversight (Listfield and Montes-Negret, 1994).

Yet for retail users, especially in EMDEs, commercial bank money poses at least three key challenges.

Figure 1. Access to Bank Accounts and Bank Services Is Heterogeneous, but Rising



First, it requires a bank account—access to which is rising (figure 1, left-hand panel) but is still far from universal. The poor often lack the proper documentation to comply with banks' customer due diligence (CDD) requirements.

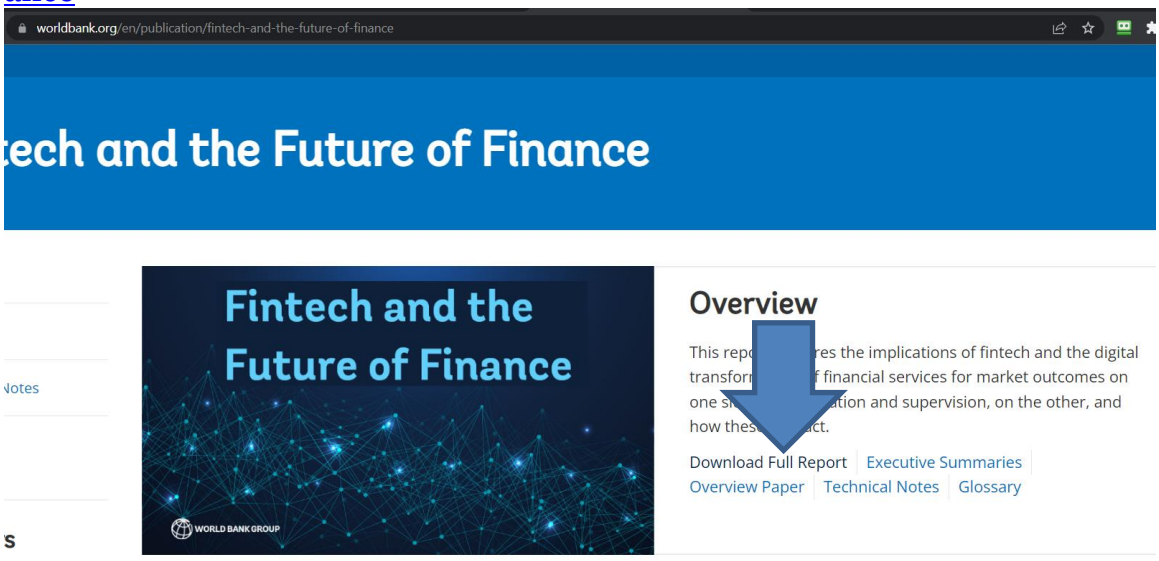
In some cases, they live too far from a bank branch, or find the maintenance costs or minimum balances too onerous. E-money, which can be seen as a variant of commercial bank money, seeks to address these challenges.

Together with simplified CDD and networks of agents, e-money has improved access to transaction services. Still, in countries where bank accounts and e-money have not reached universal levels, the poor rely heavily on cash.

This reliance on cash helps perpetuate informality, also known as the shadow economy—economic activities hidden from authorities for monetary, regulatory, and institutional reasons (Medina and Schneider, 2019).

Indeed, informality is higher in countries with lower use of digital payments like bank accounts and e-money (figure 1, right-hand panel).

To read more (please choose download full report) at:
https://www.worldbank.org/en/publication/fintech-and-the-future-of-finance



Number 8

Global Cybersecurity Outlook

Karen Tso, Chander Prakash Gurnani, Jürgen Stock, Josephine Teo, Robert M. Lee

The World Economic Forum's Global Cybersecurity Outlook report indicates that cyberattacks increased 125% globally in 2021, with evidence suggesting a continued uptick through 2022. In this fast-changing landscape it is vital for leaders to take a strategic approach to cyber risks.

How can leaders better prepare for future cyber shocks? What individual and collective actions will foster a more secure and resilient digital ecosystem?

This is a livestreamed session. You may visit: https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/global-cybersecurity-outlook-1a06c9fd7d

Number 9

Central Bank Digital Currencies

Julia Chatterley, Kristalina Georgieva, Sethaput Suthiwartnarueput, François Villeroy de Galhau, Axel Lehmann

Central bank digital currencies (CBDCs) have the potential to reshape financial systems, changing the landscape of payments and banking. More countries are experimenting with CBDCs and some are beginning to bring them to market, potentially offering lessons for the rest of the world.

What are the macroeconomic and geopolitical implications surrounding the roll-out of CBDCs? How can the public and private sectors work together to ensure that CBDC development ultimately benefits consumers and minimizes risks to financial stability?

This is a livestreamed session. You may visit:
https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/central-bank-digital-currencies

Number 10

Where Will the Jobs of Tomorrow Come From?

Rebecca Blumenstein, François-Philippe Champagne, Jos De Blok, Dipu Moni, Mikael Damberg

From care, education and health to green energy, infrastructure and digital, the jobs of tomorrow may emerge in several growing sectors of the global economy.

How can targeted investments and policies ensure such job creation and support workers in transitioning to them?

This is a livestreamed session. You may visit: https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/jobs-of-tomorrow-the-green-economy

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

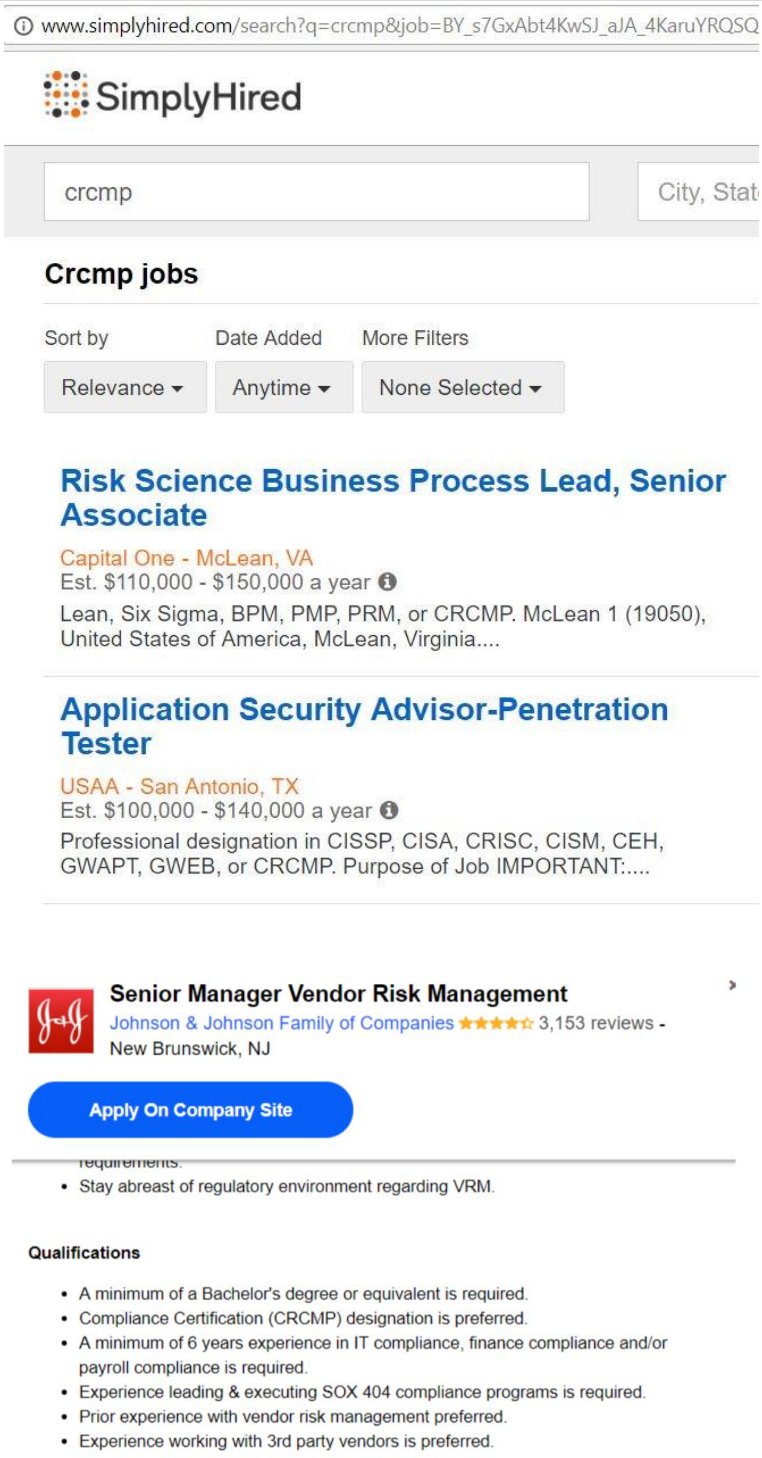
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.