

International Association of Hedge Funds Professionals (IAHFP)

1200 G Street NW Suite 800 Washington DC 20005-6705 USA

Tel: 202-449-9750 Web: www.hedge-funds-association.com*Hedge Funds News, April 2022*

Dear members and friends,

We will start with an interesting paper from BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht, the German Federal Financial Supervisory Authority).



Surfing on behalf of consumers

Do banks and insurers provide information about alternative dispute resolution mechanisms on their websites and in their small print? BaFin investigated the situation.

When most people hear the words “surf days” they think of sun, sand and metre-high waves. But for BaFin staff the term is an important supervisory tool in an era of increasing digitalisation.

Supervisors visit selected companies’ websites to gain an overview of how specific supervisory issues are handled.

BaFin's Consumer Protection Directorate (VBS) looked at banks' and insurers' websites on two surf days in 2021.

The goal was to check whether the companies were complying with their duty to provide information on alternative dispute resolution mechanisms under section 36 of the German Act on Alternative Dispute Resolution in Consumer Matters (Verbraucherstreitbeilegungsgesetz – VSBG) to the extent necessary.

The Directorate found that most companies were already compliant: only in a few cases did the supervisors have to require changes.

The background to the surf days was a ruling by Germany's Federal Court of Justice (Bundesgerichtshof – BGH) on the VSBG dated 22 September 2020 (case ref.: XI ZR 162/19).

This specified that companies have to inform consumers about alternative dispute resolutions mechanisms both on their website and in their general terms and conditions of business.

“Alternative dispute resolution mechanisms” are defined as conflict resolution methods that can be pursued instead of court cases.

Alternative dispute resolution

The term “alternative dispute resolution” is used to describe conflict resolution methods that can be pursued instead of court cases. Many banks and insurers have signed up to the dedicated consumer dispute resolution entities that have been recognised by the Federal Office of Justice (Bundesamt für Justiz).

These give consumers an independent, cost-effective, and efficient way of clarifying and resolving any disputes that arise.

Further information on this topic and an overview of the most important dispute resolution entities, ombudsperson schemes and complaints offices for customers in the German finance industry can be found on BaFin's website.

You may visit:

https://www.bafin.de/EN/Verbraucher/BeschwerdenStreitschlichtung/StreitSchlichtungsstellen/StreitSchlichtungsstellen_node_en.html;jsessionid=2DC57AEED7B2B810A4ABB7449BB0A3CC.1_cid500

A broad-based sample

BaFin selected 50 credit institutions and 30 insurance undertakings for its investigations. The institutions included savings banks, cooperative banks and private banks of different sizes and from different regions.

The insurers comprised 10 life insurers, 10 health insurers and 10 property/casualty insurers. The goal was to have as representative a sample as possible.

Banks: most results were satisfactory

The banking surf day revealed that 40 out of the 50 institutions complied with their duties to provide information in full. The references to alternative dispute resolution mechanisms provided both on their websites and in the terms and conditions that are accessible there complied with the statutory requirements. However, BaFin discovered that four institutions had what were in part material defects.

Either the websites provided no information at all on out-of-court dispute resolution mechanisms or the information given was imprecise. For example, foreign dispute resolution entities that do not actually have jurisdiction were mentioned or institutions that have not been approved for alternative dispute resolution, such as the European Central Bank, were listed.

Insurers: most undertakings provide information

The surf day for the insurance sector revealed that all undertakings with an Internet presence that were investigated had published the necessary reference to out-of-court dispute resolution mechanisms on their websites.

In addition, BaFin checked whether the insurers, like the banks, had added an appropriate reference in the general policy conditions that are accessible via their websites.

A total of 15 undertakings published their current general policy conditions directly on their websites – something they are not actually obliged to do.

However, only six of these general policy conditions contained all necessary information on alternative dispute resolution, whereas nine insurance undertakings did not provide the information for some tariffs at least.

Defects are being remedied

The banks and insurers for which BaFin discovered defects during its surf days have all reacted and have rectified, or promised to rectify, the errors in their general terms and conditions or their general policy conditions.

Authors

Julia Halm, Market Supervision concerning the Conduct of Insurance
Undertakings towards Consumers
Christian Pampel, Policy Issues, Consumer Protection Forum and
Consumer Advisory Council

Warning to consumers on the risks of crypto-assets



The European Supervisory Authorities (EBA, ESMA and EIOPA – the ESAs) warn consumers that many crypto-assets are highly risky and speculative. The ESAs set out key steps consumers can take to ensure they make informed decisions.

This warning comes in the context of growing consumer activity and interest in crypto-assets and the aggressive promotion of those assets and related products to the public, including through social media.

You should be aware of the specific risks of crypto-assets and related products and services and carefully weigh up whether the risks are acceptable given your own preferences and financial situation.

These include the risk that:

- you may lose all the money you invest;
- prices can fall and rise quickly over short periods;
- you may fall victim to scams, fraud, operational errors or cyber attacks;
- you are unlikely to have any rights to protection or compensation if things go wrong.

If you are thinking about buying crypto-assets or related products and services, you should ask yourself the following:

- can you afford to lose all the money you invest?
- are you ready to take on high risks to earn the advertised returns?
- do you understand the features of the crypto-asset or related products and services?
- are the firms/parties you are dealing with reputable?
- are the firms/parties you are dealing with blacklisted by the relevant national authorities?
- are you able to protect effectively the devices you use for buying, storing or transferring crypto-assets, including your private keys?

What are the key risks?

- *Extreme price movements:* many crypto-assets are subject to sudden and extreme price movements and are speculative, because their price often relies solely on consumer demand (i.e., there may be no backing assets or other tangible value).

You may lose a large amount or even all of the money invested. The extreme price movements also mean that many crypto-assets are unsuitable as a store of value, and as a means of exchange or payment;

- *Misleading information:* some crypto-assets and related products are aggressively advertised to the public, using marketing material and other information that may be unclear, incomplete, inaccurate or even purposefully misleading.

For instance, advertisements via social media may be very short, with a focus on the potential gains but not the high risks involved. You should also beware of social media ‘influencers’ who typically have a financial incentive to market certain crypto-assets and related products and services and therefore may be biased in the communications they issue;

- *Absence of protection:* the majority of crypto-assets and the selling of products or services in relation to crypto-assets are unregulated in the EU.

In these cases you will not benefit from the rights and protections available to consumers for regulated financial services, such as complaints or recourse mechanisms;

- *Product complexity:* some products providing exposure to crypto-assets are very complex, sometimes with features that can increase the magnitude of losses in case of adverse price movements. These products, given their complexity, are not suitable for many consumers;

- *Fraud and malicious activities:* numerous fake crypto-assets and scams exist and you should be aware that their sole purpose is to deprive you of your money using different techniques, for example phishing;

- *Market manipulation, lack of price transparency and low liquidity:* how cryptoassets prices are determined and the execution of transactions at exchanges is often not transparent.

The holding of certain crypto-assets is also highly concentrated, which may impact prices or liquidity. You may therefore not get a fair price or treatment when buying or selling crypto-assets, or not be able to sell your crypto-assets as quickly as you would want in the absence of a potential

buyer. Cases of market manipulation have been reported on multiple occasions; and

- *Hacks, operational risks and security issues:* the distributed ledger technology underpinning crypto-assets can bear specific risks. Several issuers and service providers for crypto-assets, including crypto exchanges and wallet providers, have experienced cyber-attacks and severe operational problems.

Many consumers have lost their crypto-assets or suffered losses due to such hacks and disruptions or because they have lost the private keys providing access to their assets.

You may visit: https://www.eiopa.europa.eu/document-library/consumer-warnings/warning-consumers-risks-of-crypto-assets_en

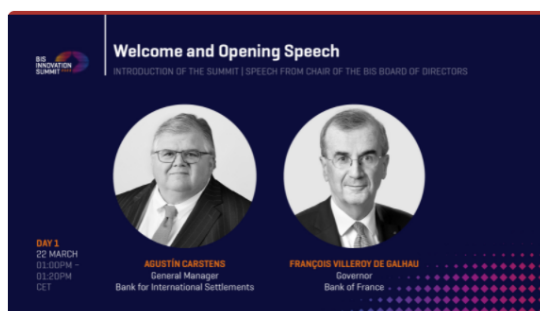
BIS Innovation Summit 2022



The BIS Innovation Summit brings together global policymakers, senior executives from the financial and technology industries, and academics to discuss technology and innovation.

Global leaders from the public and private sector discussed key issues around the future of money and payments, CBDC, DeFi, new technology in the financial system, green initiatives, and technology as an enabler for financial inclusion.

Day 1 videos - Money and Payments



Welcome and opening speech at the BIS Innovation Summit 2022 (00:23:05)
by Agustín Carstens and François Villeroy de Galhau

22 Mar 2022 | BIS Innovation Summit 2022

Agustín Carstens (General Manager, Bank for International Settlements) and François Villeroy de Galhau (Chair, BIS Board of Directors and Governor, Bank of France) open the BIS Innovation Summit 2022.

You may visit: https://www.youtube.com/watch?v=tXvV5G_qtaw




Central bank digital currencies, digital payments, and the future of money (00:46:32)

by Stefan Ingves, Patrick Njoroge, Gary Gorton and Jose Antonio Alvarez

22 Mar 2022 | BIS Innovation Summit 2022

Speakers discuss plans and challenges for the digital payments era and explore what the future might bring for money and payments from the perspectives of the private and public sectors.

You may visit: <https://www.youtube.com/watch?v=xVD1ZFPzcbg>



The graphic is a promotional poster for the BIS Innovation Summit 2022. It features a dark blue background with a grid of small, colorful dots in the bottom right corner. On the left, there is a circular portrait of Josh Lipsky, with text identifying him as the President of The Atlantic Council's MacArthur Foundation Center. Above this, the text 'In conversation with Christine Lagarde' is displayed in white, with 'Christine Lagarde' in orange. Below this, the text 'THE FUTURE OF MONEY IN THE EUROSISTEM' is written in small white capital letters. To the right of the portrait, a circular portrait of Christine Lagarde is shown, with text identifying her as the President of the European Central Bank. At the bottom left, the text 'DAY 1 22 MARCH 02:15PM - 02:40PM CET' is displayed in white. The BIS Innovation Summit 2022 logo is in the top left corner.

In conversation with Christine Lagarde about the future of money in the Eurosystem (00:25:49)
by Christine Lagarde

22 Mar 2022 | BIS Innovation Summit 2022

Josh Lipsky has a one on one conversation with the President of the European Central Bank, Christine Lagarde, about the future of money in the Eurosystem and the potential role for a digital Euro.

You may visit: <https://youtu.be/vdqfIYj6oDc>

To read more:

https://www.bis.org/events/bis_innovation_summit_2022/overview.htm

FinTech and Market Structure in the COVID-19 Pandemic Implications for financial stability



The COVID-19 pandemic has accelerated the trend toward digitalisation of retail financial services.

Comprehensive data on market shares of FinTechs, BigTechs and incumbent financial institutions in retail digital services are lacking, but proxies in the form of revenue and app downloads, and insights from market outreach suggest that BigTechs and larger FinTechs have further expanded their footprint in financial services.

In some markets, concentration measures are high, but there is no evidence yet of a generalised increase.

The observations in this report broadly support the conclusions of previous FIN reports. BigTech and FinTech firms' expansion into financial services can bring benefits such as improved cost efficiencies and wider financial inclusion for previously underserved groups.

BigTechs' financial activities in emerging market and developing economies (EMDEs) bring particular benefits in this regard. At the same time, there is potential for (rapid) market dominance.

There could be negative financial stability implications from dependence on a limited number of BigTech and FinTech providers in some markets, the complexity and opacity of their partnership activities, and potential incentives for risk taking by incumbent financial institutions to preserve profitability.

Consumer protection risks could arise from greater dependency on technology and potential data protection issues, e.g. the unauthorised use or the misuse of users' personal data.

Cloud computing by third-party service providers not subject, in many cases, to financial regulation can introduce cost efficiencies and access to innovations in artificial intelligence (AI).

But the limited number of providers of cloud services could magnify the impact of any operational vulnerability.

The growth of BigTechs in particular may give greater urgency to financial stability issues previously discussed, such as the potential for greater

systemic importance of new players that may not be subject to financial regulation.

This underscores the need to address data gaps that currently hamper the assessment of the financial risks and systemic importance of BigTechs. Such data gaps make it difficult for authorities to decide whether and how to include BigTechs in the regulatory perimeter.

Authorities have taken a range of policy actions during the pandemic that may impact market structure and the role of FinTechs, BigTechs and incumbent financial institutions.

These actions relate to financial stability, competition, data privacy and governance issues.

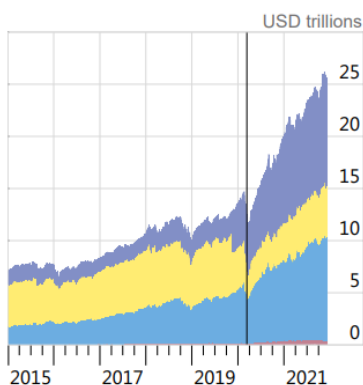
In parallel, there is international work on third-party dependencies of the financial sector, for instance in cloud computing.

This highlights the importance of cooperation between regulatory and supervisory authorities, including those charged with overseeing the bank and non-bank sectors, and where relevant, with competition and data protection authorities.

Performance of BigTechs, FinTech and incumbents during Covid-19

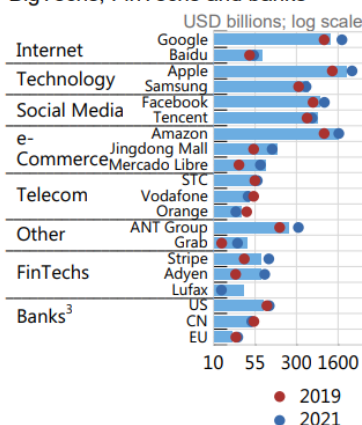
Graph 1

Shares in US equity markets¹

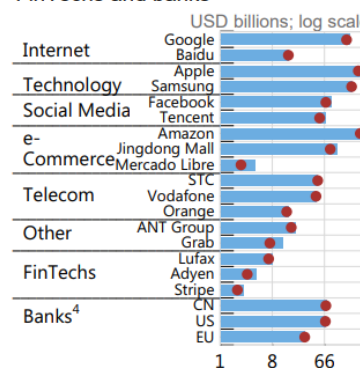


Market capitalisation of US:
 FinTechs Financials
 BigTechs Other²

Market capitalisation of selected BigTechs, FinTechs and banks



Revenues of selected BigTechs, FinTechs and banks



¹ The vertical line denotes 11 March 2020, when the WHO characterised Covid-19 as a pandemic. ² Calculated as the market capitalisation of S&P 500 and Nasdaq minus the market capitalisation of FinTechs, BigTechs and financials. ³ Many FinTechs are not publicly listed. In these cases, data on market capitalisation and revenues are drawn from news sources. ⁴ Average market capitalisation of banks in the S&P 500 index, EuroStoxx Banks index and Shanghai Composite index. ⁵ Average revenue, weighted by market capitalisation, of banks in the S&P 500, EuroStoxx Banks index and Shanghai Composite index.

Sources: Bloomberg, Eikon, S&P Capital IQ; FSB calculations.

Executive summary	1
1. Introduction	2
2. Trends in market structure during the pandemic	2
3. Drivers of digitalisation in finance during the pandemic.....	8
3.1. Supply-side drivers	8
3.2. Demand-side drivers.....	10
4. Benefits and risks of changes in market structure	11
4.1. Potential benefits	11
4.2. Potential risks	12
4.3. Assessment of changes since the pandemic.....	15
5. Regulatory changes during the pandemic	16
6. Conclusion	18
Annex 1: Glossary	19
Annex 2: Selected policy measures affecting market structure	20
Annex 3: List of contributors to the report.....	24

To read more:

<https://www.fsb.org/wp-content/uploads/P210322.pdf>

Project Ellipse

An integrated regulatory data and analytics platform



Executive summary

A transformational shift in the volume, speed and variety of data is driving the innovative use of financial technology, leading to rapid changes in the financial landscape.

At the same time, regulatory authorities still rely on the collection of template-based supervisory data, which has remained largely unchanged.

Supervisors are faced with the challenge of needing to assess rapidly evolving risks to business models and technology-driven changes that may affect financial stability, with regulatory data that are infrequent and collected according to legacy frameworks.

In January 2021, the BIS Innovation Hub Singapore Centre and the Monetary Authority of Singapore (MAS) launched Project Ellipse.

With the support of the Bank of England (BoE), the International Swaps and Derivatives Association (ISDA), Financial Network Analytics (FNA) and Accenture, Project Ellipse explores how technology solutions could enable supervision to be more forward-looking, insights-based and data-driven, using an integrated regulatory data and analytics platform.

Importantly, the Ellipse prototype combines both structured and unstructured sources of data that are relevant to current events in real time.

Advanced analytics are then applied to those integrated data sources to provide supervisors with early warning indicators, analytics and prudential metrics.

Project Ellipse was undertaken in two phases. In Phase 1, the project investigated how data-driven supervision could be enabled by machine-executable digital reporting, using a cross-border common data model.

Our exploration found that regulatory reporting requirements can be expressed in unambiguous machinereadable logical reporting instructions underpinned by a consistent data model.

Programmatic specifications of the steps for generating regulatory reports can also be published alongside regulations to ensure a clear understanding of the expected data at the most granular level.

With additional logical instructions based on the same data model, supervisors could also automatically query the underlying transaction data and generate regulatory metrics referencing that standardised data.

Phase 1 illustrated the possibilities and the efficiencies that could be gained if machine-executable reporting using common data models were to be adopted.

This could also increase the volume of granular data available to supervisors, as needed to enable the use of advanced analytics.

In Phase 2, the project took existing large exposures regulatory data and integrated these with unstructured data.

Advanced analytics such as machine learning and natural language processing were applied to these data sources to make risk correlations and to analyse sentiment, alerting supervisors in real time of issues that might need further investigation.

Network analytics were also used to demonstrate how exposures could be mapped, indicating possible systemic risks to the banking system.

The Ellipse platform prototype was developed, which can extract insights from the mined data and display these via dashboards as early warnings for supervisory attention.

The second phase of Project Ellipse demonstrates how a single platform could be built so that authorities could benefit from “on demand” access to timely and integrated sources of data to help support and inform their supervisory assessments.

The BIS Innovation Hub’s Project Ellipse is a prototype that authorities can test in their own environments and which may help them to explore new solutions.

It also presents an opportunity for the global regulatory community to further consider, explore and collaborate on common solutions to future-proof the data and analytical capabilities of supervisors.

To read more: <https://www.bis.org/publ/othp48.pdf>

Table 1 — Challenges of regulatory reporting

1 Template based, aggregated

Regulatory requirements are often template-based and call for aggregated data, meaning that data sets are fixed to a use case and hence the data received cannot be easily reused for other purposes. New reporting requirements are needed whenever additional or ad hoc information is needed.

2 Data are inconsistently described

Reporting data are often sourced from reporting firms' legacy data systems, which may not be integrated. This often results in heterogeneity of data for any given product or transaction – both within a bank and across different banks – as different systems will describe these data differently.

CHALLENGES FACED**3 Infrequent, backward looking**

Regulatory reports are submitted to supervisors from reporting entities on an infrequent basis (eg every month or quarter). At times of heightened risk, the need for up-to-date data increases but, given the static nature of regulatory reports, supervisors may not have the timeliest data to make informed judgments.

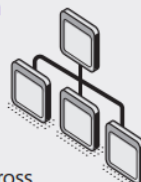
4 Different sources of data are not integrated

Information contained in regulatory reports is often linked to other types of information that may point to emerging risks, but these sources of information are not connected. For instance, information sourced from market data and news often gives the first indication of emerging risks but it is difficult for supervisors to scan through the vast volumes of market and news data to assess which point to a need to take early action.

Table 2 — Possible solutions explored in Project Ellipse

1 Granular data

The collection of granular data from reporting entities could replace the need for authorities to request information using templates. It could also enable authorities to reuse those data for different use cases. Supervisory metrics could also be derived using granular data, as opposed to requiring reporting entities to aggregate the required data prior to submission.

2 Common data models

Differences in the description of data for similar products and transactions across banks can be addressed using data standards and common data models. Granular reporting requires a common understanding by authorities and financial institutions of what these data are, so that financial institutions can map their operational data to a common "input" before the required data can be reported. Supervisory metrics could then be derived using programmable rules that reference machine-readable and machine-executable common data models.

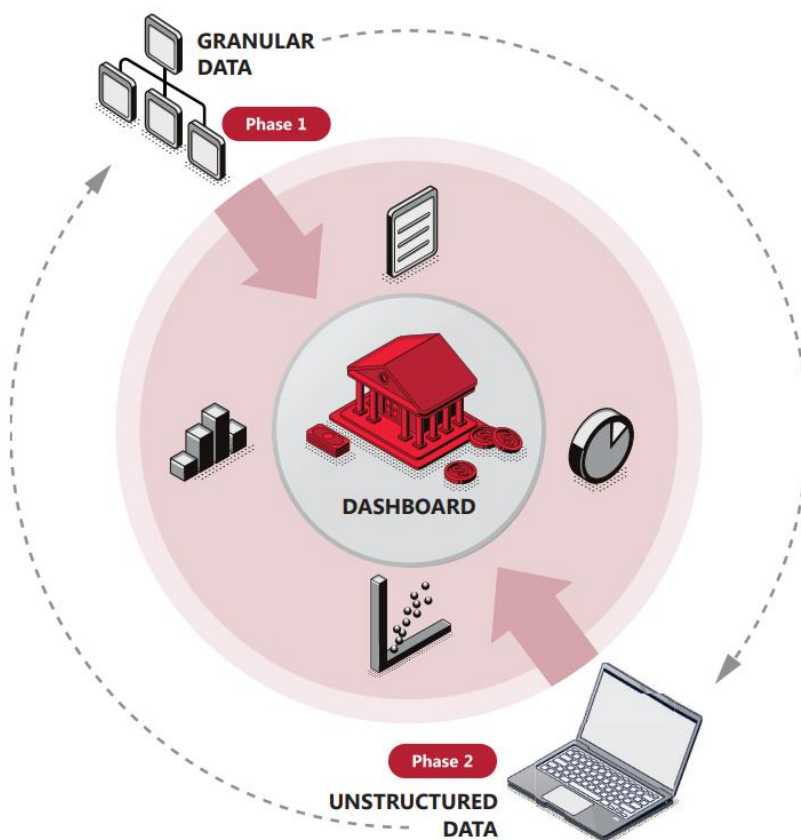
SOLUTIONS EXPLORED

SOLUTIONS
EXPLORED**3 Real-time information**

Real-time insights using advanced analytics could be derived from large volumes of unstructured data that would supplement the granular reporting available. This would provide supervisors with additional indicators and early warnings of any at-risk exposures of reporting entities.

4 Integration of structured and unstructured data

Integrating granular data from reporting entities with other sources of unstructured information such as news and market data on the same platform would obviate the need for supervisors to spend time manually scanning for information. Advanced analytics such as AI and ML could be used to make risk correlations and analyse sentiment, alerting supervisors in real time of issues that may need further investigation.



The return of inflation

Agustín Carstens, General Manager of the BIS at the International Center for Monetary and Banking Studies, Geneva



Thank you very much for inviting me to give this lecture. It is a pleasure and an honour to be here today.

Being the BIS's General Manager, it will not come as a surprise to you that I have decided to devote my presentation to the issue that is top of mind for policymakers around the world, namely the return of inflation.

After more than a decade of struggling to bring inflation up to target, central banks now face the opposite problem.

The shift in the inflationary environment has been remarkable.

If you had asked me a year ago to lay out the key challenges for the global economy, I could have given you a long list, but high inflation would not have made the cut.

This evening, I will describe the rise in inflation over the past year and discuss why this came as a surprise to many.

I will argue that the pandemic and the extraordinary policy response laid the groundwork for a rapid and goods-intensive bounceback in demand which supply has been unable to fully meet.

The war in Ukraine has further disrupted supply, particularly for commodities.

I will also draw some broader lessons about the inflationary process – in particular, the need to look “under the hood” of aggregate data and models to understand how the behaviour of individual firms and workers drives inflation outcomes.

A key message is that we may be on the cusp of a new inflationary era. The forces behind high inflation could persist for some time.

New pressures are emerging, not least from labour markets, as workers look to make up for inflation-induced reductions in real income.

And the structural factors that have kept inflation low in recent decades may wane as globalisation retreats.

If my thesis is correct, central banks will need to adjust, as some are already doing.

For many years now, having conquered inflation, they have had unprecedented leeway to focus on growth and employment.

Indeed, with inflation stubbornly below target, stimulating activity hit two birds with one stone.

But this is now no longer possible, since low and stable inflation must remain the priority.

If circumstances have fundamentally changed, a change in paradigm may be called for.

That change requires a broader recognition in policymaking that boosting resilient long-term growth cannot rely on repeated macroeconomic stimulus, be it monetary or fiscal.

It can only be achieved through structural policies that strengthen the productive capacity of the economy.

To read more: <https://www.bis.org/speeches/sp220405.pdf>

FSB Work Programme for 2022



The Financial Stability Board's (FSB) work programme for 2022 aims to maximise the value of the FSB's global and cross-sectoral approach to financial stability policy.

The FSB's work priorities reflect that financial challenges are global in nature and affect the financial system as a whole.

These challenges include digitalisation, climate change and potentially also shifts in the macroeconomic and interest rate environment.

This note summarises the ongoing and planned FSB initiatives in 2022 organised by:

- (1) priority areas of work and new initiatives;
- (2) work programme items that are continuing or reaching completion; and
- (3) regular monitoring and reporting.

The Annex provides an indicative timeline of the FSB's publications planned for 2022.

1. Priority areas of work and new initiatives

Supporting international cooperation and coordination on current financial stability issues.

The FSB, with its broad and diverse membership of national authorities, international standard setters and international bodies, continues to promote financial stability in a rapidly evolving financial market environment.

Against the backdrop of the Russia-Ukraine conflict and its economic impacts, the FSB is reinforcing its forward-looking monitoring to identify, assess and address new and emerging risks to global financial stability.

This enhanced monitoring is informed by the FSB's new surveillance framework.

Work will also continue on policy responses to COVID-19, including: sharing information on policy responses and the timely unwinding of the

temporary measures adopted in response to COVID-19, and assessing the effectiveness of those measures; and monitoring, with the standard-setting bodies (SSBs), the use of flexibility within international standards and consistency of policy responses with existing international financial standards.

- Work on the financial stability implications of current developments will continue in a flexible mode – including on specific vulnerabilities, policy issues and monitoring – and be adjusted as needed.
- FSB will work with SSBs to follow up on specific issues identified in the report on lessons learnt from COVID-19 for financial stability, including macroprudential aspects of buffer functioning.
- At the request of the Indonesian G20 Presidency, the FSB will report to the G20 on exit strategies to support equitable recovery for financial stability, and on effective practices and policy recommendations for addressing the effects of COVID-19 scarring in the financial sector.

Enhancing the resilience of the non-bank financial intermediation (NBFI) sector, while preserving its benefits.

The FSB will advance its work programme for strengthening the resilience of NBFI.

This work, set out in the FSB's holistic review of the March 2020 market turmoil, will be carried out within the FSB as well as by SSBs and international organisations.

- In 2022, remaining work on specific issues identified in the holistic review will be completed, including on open-ended funds (OEFs); margining practices; the liquidity, structure and resilience of core bond markets; and USD funding and emerging market economy (EME) vulnerabilities.
- In addition, work will focus on developing a systemic approach to NBFI. This includes enhancing the understanding of systemic risks in NBFI and strengthening their ongoing monitoring; and developing policies to address such risks.

Enhancing cross-border payments.

The FSB roadmap for enhancing cross-border payments contains a large number of actions, guided by a set of quantitative targets.

To help achieve these targets, specific proposals for material improvements to existing payments systems and arrangements are being discussed, as well as the development of new systems.

The FSB will continue to coordinate with CPMI and other SSBs and international organisations in implementing the FSB roadmap to enhance cross-border payments.

- In 2022, the FSB has committed to complete a number of actions under the roadmap, including the development of an approach to monitor progress against the quantitative targets; identification of gaps or areas for enhanced implementation in standards; and work on enhancing data sharing.
- The FSB will deliver to the G20 a progress report on the overall roadmap and the development of key performance indicators to monitor progress towards the quantitative targets.

To read more: <https://www.fsb.org/wp-content/uploads/P310322.pdf>

Fake WhatsApp 'voice message' emails are spreading malware



A phishing campaign which impersonates WhatsApp's voice message feature has been spreading information-stealing malware.

The attack starts with an email claiming to be a notification from WhatsApp of a new private voice message. The email contains a creation date and clip duration for the supposed message, and a 'Play' button.

The identity 'Whatsapp Notifier' masks a real email address belonging to a Russian road safety organisation. As the address and organisation are real, the messages aren't flagged as spam or blocked by email security tools. Armorblox, who discovered the scam, believe the Russian organisation is playing a role without realising.

The 'Play' button will take the email recipient to a website which then asks them to click 'Allow' in an allow/block prompt to 'confirm you are not a robot'. Once 'allow' is clicked, the browser will prompt to install software that turns out to be information-stealing malware.

While there are numerous 'tells' that this is a scam, these attacks rely on people missing the signs – perhaps because they are waiting for urgent or exciting news that could well be delivered by a voice message.

The NCSC has published guidance on how to spot and report scams, including those delivered by email and messaging. You may visit: <https://www.ncsc.gov.uk/collection/phishing-scams>

GUIDANCE

Phishing: Spot and report scam emails, texts, websites and calls


How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

Our top tips for staying secure online will help you keep your devices and information secure even if you do click on a scam, and you can also learn how to recover a hacked account.

As of March 2022 the NCSC has received over:

 **11m** reported scams

Which has resulted to:

 **78k** scams being removed across 144,000 urls

Capability Assessment for StratCom:

Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations



There are no established models for assessing an organisation's capability to respond to *information influence operations (IIOs)*.

While great efforts have been made to improve our knowledge and understanding of IIOs and how to counter them, and measures have been taken to strengthen democratic processes and to decrease societal vulnerabilities, few efforts have been made to measure the impact of IIOs or to assess the efficacy of the countermeasures currently in place—the response capability—to mitigate those consequences.

When facing a potential threat, we don't want to just sit and wait for something bad to happen, experience the impact, and only then consider how best to respond.

It is much better to be proactive and seek to develop a response capability that can prevent losses or effectively mitigate the negative impact of an adverse event when it occurs.

To assess whether our response capability is sufficient we must be able to:

- 1) clearly identify the critical assets we wish to protect, and
- 2) accurately describe the response we have in place for when those assets are threatened.

Traditionally, 'risk' has been defined as 'a measure of the probability and severity of adverse effects', but recent advancements in risk research have prompted a shift in thinking.

The new perspective on risk management takes into account 'the effect of uncertainty on objectives'.

While these two orientations are largely compatible, incorporating what we know about uncertainties into estimates of response effectiveness rather

than relying on probability calculations results in more robust and flexible capability assessments.

Capability assessments have been a key activity within crisis and emergency management in the last decades.

The purpose of these assessments is to support proactive decision-making concerning resource allocation for response preparedness.

Traditional assessment models—the so-called indicator and index models — equate resources with capability; such assessments provide decision – makers with either a checklist of resources or a numerical representation that evaluates the resources available for a crisis response within a target range for acceptability.

While such models have proven utility in the business world, where production can be (more or less) planned, they are not well suited to crisis and emergency management where uncertainty plays a much larger role.

The new risk perspective addresses this dilemma, suggesting a way forward for an assessment model that takes uncertainties into account, identifies the most effective response tasks and, in the absence of actual feedback and the wisdom of hindsight, provides the best possible information for making decisions regarding investments in capability.

The first part of this report describes response capability assessment—what it is for, what goes into preparing one, and why incorporating the new risk perspective leads to more useful information.

The theoretical explanation will be illustrated with typical examples from the field of risk management concerning residential fires and the response capability of a local fire service.

The second part of the report offers suggestions on how these concepts and ideas might be adapted for responding to IIOs.

The report ends with concluding remarks and a glossary of terms.

To read more: <https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240>

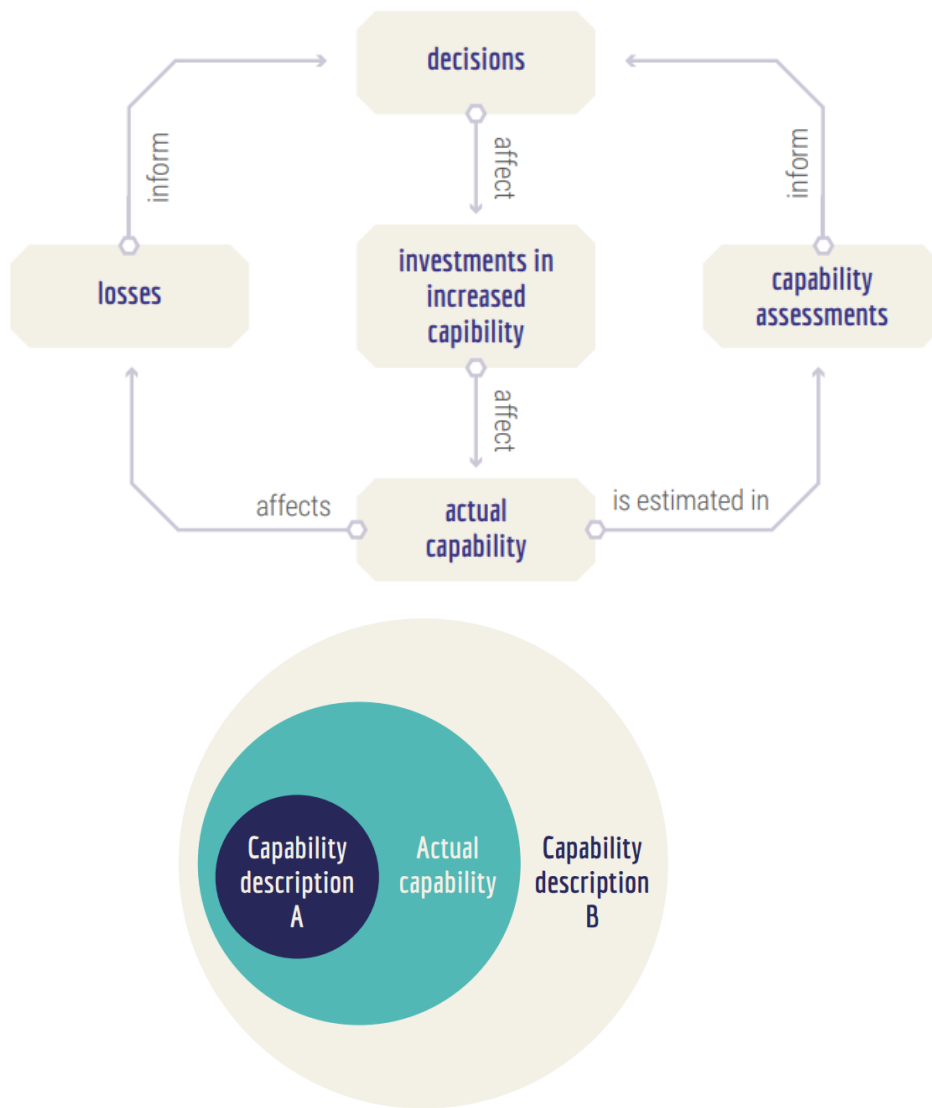


Figure 4. The difference between actual capability and possible descriptions of that capability

Full disclosure - coming to grips with an inconvenient truth

Frank Elderson, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the ECB, at the 14th European Bank Institute Policy Webinar on the ECB's supervisory approach on climate-related and environmental risks, Frankfurt am Main



Some years ago, Andrea Enria, the Chair of the Supervisory Board, gave a speech, precisely at an EBI conference, calling for greater transparency in prudential supervision.

When describing the role of transparency and information disclosure, he echoed the words of Supreme Court Justice Louis Brandeis:

"Sunlight is said to be the best of disinfectants; electric light the most efficient policeman".

This couldn't be truer for climate-related disclosures, too. As I have said before when discussing the supervision and prominence of climate-related and environmental, or C&E, risks, we can only tackle a problem once we get a good grip on its shape and size. Some information may be uncomfortable to face up to – but bringing it to light is the first step in making progress.

When it comes to climate change, the information on what Al Gore famously dubbed an inconvenient truth is indeed getting bleaker by the day.

The most recent IPCC report confirms the dramatic consequences of not taking immediate action: additional global warming of up to 1.5 degrees Celsius in the near term would increase climate hazards, and present numerous risks to ecosystems and human society.

Europe is particularly badly affected, as temperatures here continue to rise above the mean and, despite our efforts to reduce CO₂ emissions, we lag far behind in terms of what we need to do to adapt to some of the inevitable consequences.

It is time we face the facts. As citizens, as institutions, and as all actors in the economy – including of course banks.

It is essential that banks share with their stakeholders detailed information on their exposures to C&E – risks. Only then can we all effectively work together to address the consequences of climate change.

This is why today I would like to draw your attention to another important landmark in the ECB's supervision of C&E risks: the publication of our second stocktake on the transparency of banks' disclosures of their C&E risk profiles.

The European and international agenda on climate

Publishing this update is part of our supervisory agenda on climate. As you know, C&E risks have been one of our supervisory priorities for some years now and we have started treating them just like any other prudential risk.

In this context, we have been rolling out a series of corresponding supervisory activities.

In 2020 we published our guide on climate-related and environmental risks, which outlined our supervisory expectations relating to the management and disclosure of C&E risks.

In 2021 we published a self-assessment benchmarking report. And in 2022 we launched the climate risk stress test and a thematic review of how banks incorporate C&E risks into their processes, a fully-fledged supervisory exercise, involving teams responsible for the day-to-day supervision of banks.

At the same time, we are gradually integrating C&E risks into our regular supervisory methodology, and how banks manage these risks will ultimately impact their Pillar 2 capital requirements.

The ECB's supervisory actions on climate are part of broader international efforts to advance the supervision and regulation of C&E risks.

At global level, the Basel Committee on Banking Supervision recently concluded a public consultation on draft supervisory principles for the prudential treatment of climate-related risks, and the input they received is now being reviewed with the aim of finalising those supervisory principles.

This is part of a broader workplan of the Committee to evaluate how to consider climate-related financial risks in all pillars of the Basel framework. Supervision, regulation and – the topic of the ECB report that is published this morning – disclosures.

The importance of transparent disclosures

There is growing international awareness of the great value of transparent disclosures. Disclosures that are clear and easy to understand tend to benefit any company, banks included.

Generally, companies have strong incentives to publish frank and meaningful disclosures because transparency is usually rewarded by investors; it helps reduce uncertainty and allows all interested parties to feel they are making safe investments based on trustworthy data.

This is particularly true for climate-related and environmental risks. As the materiality of physical and transition risks increases by the day, investors are on the lookout for those companies that proactively take these risks into account in their daily operations and across all their activities. One of the essential functions of financial markets is to price risk and thus support informed and efficient capital allocation decisions.

The accurate and timely disclosure of current and past operating and financial results is central to this function. To make it concrete: the more transparent banks are about their C&E risk profiles and their concrete efforts to align their portfolios with the Paris Agreement, the easier it is for market participants to compare banks, reward those which are taking the necessary steps to adopt risk management practices aligned with a carbon-neutral economy, and re-evaluate those with misaligned trajectories.

Transparent disclosures also create a certain level of peer and stakeholder pressure, which is essential to making companies properly manage their risks. Investors and asset managers are seeking to develop and market portfolios that are aligned with the sustainability objectives of their own clients. As such, they are becoming increasingly demanding about corporate C&E disclosures.

Banks' own shareholders are becoming increasingly demanding, too, especially concerning banks that have publicly committed to achieving net zero targets. In fact, failure to disclose meaningful follow-up information on their climate commitments has already led to significant litigation and given rise to heightened reputational and legal risks for some banks.

Recent regulatory and legislative initiatives reflect growing international awareness of the great value of transparent disclosures on C&E risks. In Europe, large banks will have to disclose climate-related information under the European Banking Authority's comprehensive implementing technical standards.

They will have to already do so by early 2023, referencing data from the end of 2022. The information requested from banks includes qualitative and quantitative information on environmental, social and governance

risks, as well as indicators such as alignment metrics and the green asset ratio – thus significantly raising the bar in terms of C&E risk reporting.

In the same vein, sustainability reporting obligations under the European Commission's Corporate Sustainability Reporting Directive will shortly apply to large corporations, including banks under our direct supervision.

Main findings of the ECB report on banks' progress towards transparently disclosing their C&E risk profile

The ECB is also well aware of the importance of transparent disclosures. We published our first stocktake of banks' C&E disclosures back in November 2020.

We did so precisely to give banks the time and the incentive to improve the quality of their own disclosures in this field. Back then, virtually none of the institutions in the scope of the assessment met our expectations as set out in the ECB Guide on climate-related and environmental risks, which we published at the same time.

The second stocktake, published today, shows that the quality of banks' disclosures has improved since then, especially in the areas of risk management, governance and business models.

However, this improvement has been only marginal: as of 2021, seven in ten banks disclosed information about C&E risk management and governance – compared to five in ten in 2020 -, while only four in ten shared relevant information about the incorporation of C&E risks into their strategic considerations – up from three in ten in 2020. And, all in all, none of the 115 banks directly supervised by the ECB fully meets our supervisory expectations for disclosures.

There is very little justification for this lack of substantial progress, particularly considering the vast amount and quality of climate-related data, tools and information shared by different international and European organisations and institutions in recent years.

The sheer speed at which regulation and metrics are developing in this field should leave no room for any doubt: addressing climate-related and environmental risks, and publishing good-quality disclosures, is not optional. Banks can and must do much better to improve the quality of their disclosures, and they need to do it quickly.

However, we see a considerable disconnect between banks' perception of the importance of C&E risks as communicated to us, the supervisor, and what banks choose to publicly disclose.

Banks are trying to compensate for the poor quality of their disclosures by issuing a great volume of information around green topics.

We end up with a lot of white noise and no real substance on what both markets and supervisors really want to know: how exposed is a bank to C&E risks and what is it doing to manage that exposure? It is of course relevant for banks to publicise their efforts to, for example, reduce the electricity consumption of their branches.

However, it would be much more significant if they were to announce how they are steering their activities towards risk management practices that are aligned with a carbon-neutral economy. Looking at the world through "green-coloured glasses" is not quite the same as a sound management of all material C&E risks.

We also observe a lack of concrete detail in how banks substantiate their climate-related and environmental metrics and targets. For example, when reporting on their commitment to align with the Paris Agreement, only around one in five institutions disclose the methodologies, definitions and criteria for all of the figures, metrics and targets reported as material.

More than one-third of institutions do not disclose these aspects at all. In light of the increasing importance of such commitments, interested parties will increasingly seek information on these alignment metrics – and banks' disclosures must become meaningful in this regard.

Best practices

Like many other institutions and agencies, the ECB is committed to sharing the best practices we have found across the industry. Not only do they serve as inspiration for banks who need to catch up, they also show that the ECB's expectations can, in fact, be met.

For example, one of the banks under our direct supervision published its own climate strategy – which aims at achieving net zero emissions for its lending portfolio by 2050 or sooner – in tandem with a number of (interim) targets and related metrics, as well as the progress made in meeting them. For each of these targets and metrics, the bank discloses the sectors covered, the underlying methodology and the scenarios used to draw up benchmarks.

For the methodologies and scenarios, it reports on the options it chose, the data sources it used and the changes it made with respect to the previous disclosure.

Another bank endeavoured to align its portfolios with science-based transition pathways, including technology pathways originating from the International Energy Agency's "Net Zero by 2050" report.

The bank disclosed dashboards that displayed the performance of its loan books in various transition sectors, such as power generation, oil and gas, automotive, steel, cement and real estate, against a science-based transition pathway. It also disclosed the precise indicators used, the underlying methodologies and the reference scenarios for each indicator.

For each of the indicators, the bank then disclosed its current and projected performance against the pathway and set associated targets.

Importantly, many of the banks raising the bar in C&E disclosures are small and medium-sized – showing that remarkable progress is achievable by all.

Supervisory follow-up

Let me now outline the next steps that the ECB plans to take to follow up on the results of our assessment of banks' C&E disclosures.

We have sent individual feedback letters to all banks under our direct supervision, setting out the key gaps in their disclosures and conveying our explicit expectation that they will take decisive action to address these gaps. In doing so, banks will ultimately ensure that their risk profile is transparently and comprehensively reflected in the information they disclose to the public. Addressing such gaps will also mean banks are well prepared to meet impending technical requirements.

As I mentioned, the consequences of non-compliance with minimum transparency standards are only going to increase for banks, as legal and reputational risks are starting to materialise for banks which fail to step up the quality of their disclosures.

More and more, clients, investors and other market participants want meaningful, comprehensive information on the climate-related actions of their banks. That way, they can make conscious, informed decisions about where their money goes.

Moreover, failing to disclose exposure to risks, including C&E risks, constitutes a breach of the Capital Requirements Regulation. As such, we stand ready to use the full array of supervisory tools at our disposal to ensure banks' C&E disclosures are up to our standards, and ultimately that eligible banks are prepared for the new regulatory requirements.

The ECB in addition publishes a yearly report on banks' Pillar 3 disclosures, where we also have the option to publicly list those banks which repeatedly fail to disclose their C&E risks.

In view of the poor results shown by our stocktake, and to assess the extent to which the banks address individual feedback, C&E risk disclosures will continue to feature prominently in the ECB's supervision.

We will assess banks' C&E disclosures again at the end of 2022 and we expect to see major progress by then.

Conclusion

Let me conclude. Stricter disclosure regulation is on the way, and time is running out for banks to get ready. Five years have passed since the Task Force on Climate-related Financial Disclosures published its recommendations. There are also many initiatives, some of them open source, to support banks' efforts.

Many companies have improved their disclosures and now provide information that can feed into banks' own disclosure indicators. And for those banks that have systematically fallen behind the ECB's – and the market's – expectations there is only one way forward. It is time for banks to be transparent and comprehensive with their C&E disclosures, so we that by bringing them to light, we can progress from an inconvenient truth towards a desirable outcome – for us and for all future generations.

Let me end where I started: the first step in coming to grips with any inconvenient truth is full disclosure.

Deploying Pseudonymisation Techniques

The case of the Health Sector



As the healthcare domain is attempting to make the most of the evolving technical landscape and adapt the provision of services to fulfil the growing needs of patients in a timely manner, additional cybersecurity and data protection challenges come into play.

The integration of new technologies in already complex IT infrastructures opens up new challenges regarding data protection and cybersecurity.

This is due to the growing need to exchange and share the health related information of individuals among different stakeholders.

It is therefore essential for the entities processing personal data, on the one hand, to collect and further process only data that are necessary for their purposes and, on the other hand, to employ proper organisational and technical measures for the protection of such personal data.

Pseudonymisation is increasingly becoming a key security technique for providing a means that can facilitate personal data processing, while offering strong safeguards for the protection of personal data and thereby safeguarding the rights and freedoms of individuals.

Complementing previous work by ENISA that is relevant, this report demonstrates how pseudonymisation can be deployed in practice to further promote the protection of health data during processing.

Obviously, there is not a single solution on how and when to apply it; in fact different solutions might provide equally good results in specific scenarios, depending on the requirements in terms of protection, utility, scalability, etc.

Pseudonymisation can be a 'simple' option to adopt but it can also be comprised of a very complex process, both at technical as well as at organisational levels.

For this reason, defining the goals and objectives of pseudonymisation in each particular case and processing operation is really important.

This report highlights the added value of pseudonymisation in the healthcare sector and demonstrates its applicability through simple but specific use cases.

Complementing relevant ENISA publications in this area, it shows how such techniques can increase the level of protection for personal data being processed in the healthcare domain and will eventually promote and raise awareness on the usability and deployment of such technical measures.

Introduction

Recent decades have witnessed an accelerating pace in the development and adoption of new technologies.

This rapid technological change has also affected the healthcare sector which is going through the digitalisation process and has continuously been adopting new technologies to improve patient care, offer new services focusing on patient-at-home care and even preventive schemes.

The integration of new technologies into already complex IT infrastructures opens up new challenges regarding data protection and cybersecurity as there is an increasing need to exchange and share the health related information of individuals among different stakeholders, in some cases across countries, in order to provide better health services.

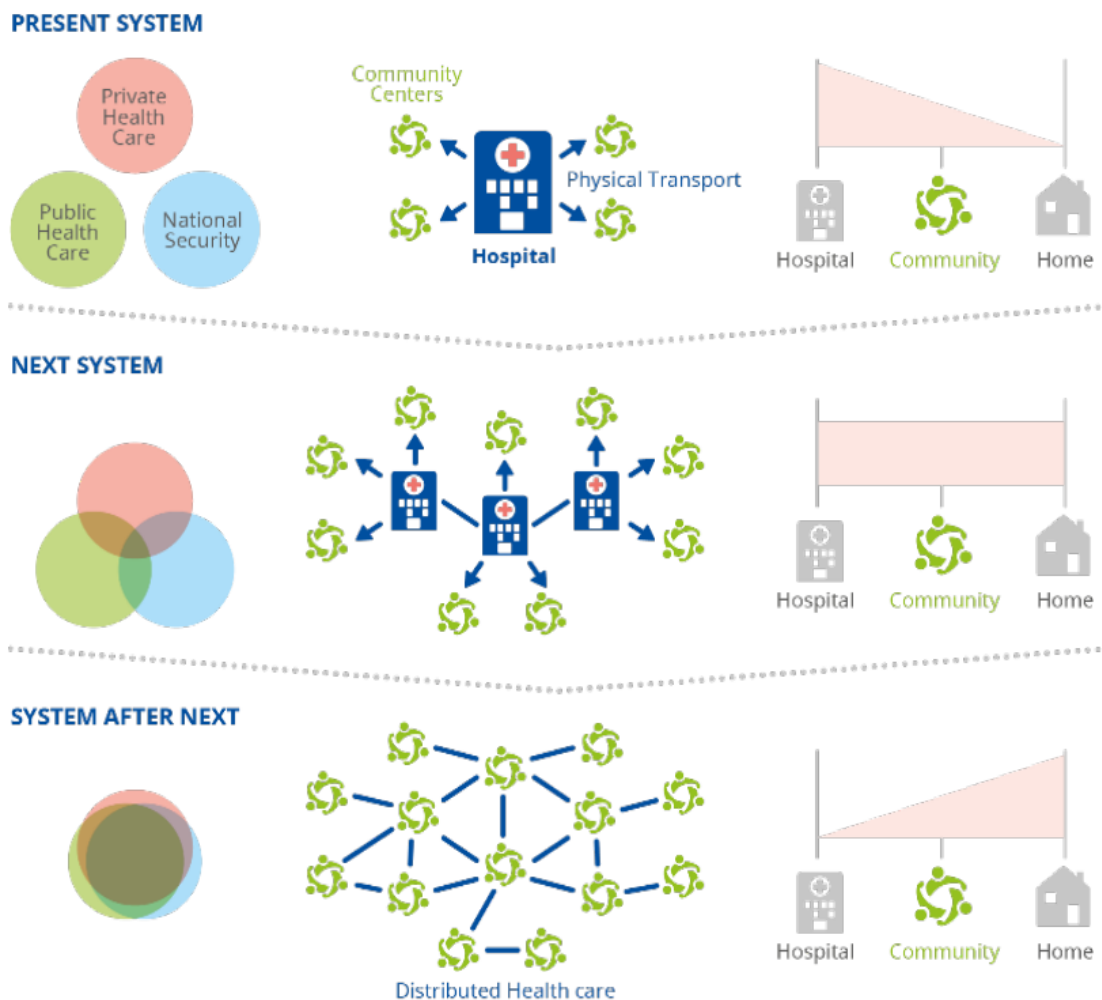
It is therefore essential for the entities processing personal data to collect and further process only data that are necessary for their purposes and, in addition, to employ proper organisational and technical measures for the protection of such data.

Pseudonymisation is one well-known measure that can significantly contribute to this end.

Broadly speaking, pseudonymisation aims at protecting personal data by hiding the identities of individuals in a dataset, e.g. by replacing one or more personal identifiers with the so-called pseudonyms (and appropriately protecting the link between the pseudonyms and the initial identifiers).

This process is not at all new in the design of information systems but gained special attention after the adoption of the General Data Protection Regulation (GDPR), where pseudonymisation is explicitly referred as a technique which can both promote data protection by design (Article 25 GDPR), as well as the security of personal data processing (Article 32 GDPR).

Figure 1: Digital transformation induced shift of value in healthcare [3]



1.1 DIGITAL TRANSFORMATION OF THE HEALTH SECTOR

Health data has always been a valuable source of knowledge in healthcare.

The healthcare domain has historically generated vast amounts of data, both for the treatment of patients and for research and further analysis.

Such processing was mostly performed in paper form but over the last few decades, the accessibility and amount of digitized data has increased massively.

More recently an abundance of new sources of health data occurred as a result of the widespread use of electronic health records, health applications and wearable devices.

Furthermore, advances in computational power have enabled the development of novel data analytics and machine learning techniques that improve diagnostics, treatment and administration in healthcare.

The result is a change in assumptions that is increasingly moving the patient away from hospitalization towards a distributed healthcare system provided by a blend of public and private operators while staying closer to home, as depicted in Figure 1.

To read more: <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques>

From open banking to open finance

Denis Beau, First Deputy Governor of the Bank of France, at the France Payments Forum "The Europe of banking and financial services" – Paris



Technological innovations, changes in demand, the arrival of new players: the changes underway in the financial sector are providing a strong impetus to relax the conditions of access to the market, in order to foster competition and thus encourage the development of new, more efficient and less costly services.

In Europe, in the field of payments, this relaxation has already occurred. The EMD, the PSD1 and finally the PSD2 directives have all resulted in the emergence of more agile players, particularly in terms of data exploitation.

The pressure to open up data now extends to insurance and savings: after open banking, we now speak of open finance. This pressure calls for further adapting the regulatory framework. But what should our guiding principles be?

In the payments sector, the main objective of the directives I mentioned was to reconcile openness and security. While this challenge remains relevant for the transition from open banking to open finance, with digitalisation and the development of the platform economy, we have seen two other challenges emerge: reconciling innovation and integration on the one hand and competition and sovereignty on the other.

How do we at the Banque de France and the ACPR, given our role and experience as a supervisor, plan to address these new challenges? This is what I would like to briefly discuss with you today, after a quick recap of the regulatory framework for open banking and the lessons that can be drawn from it to guide the development of open finance.

Part I: Openness and security

A- As regards the assessment of and lessons learned from the regulatory framework for open banking, I would like to start by recalling:

1- The key principles that governed the sharing of payment data: on the one hand, the creation of appropriate statuses and, on the other, the strengthening of security requirements for access.

The creation of the payment service or electronic money service provider status has fostered the emergence of an open banking ecosystem. The

introduction of an agent status has also contributed to this process, by creating a gradual – proportionate – regulatory framework: it thus allows emerging players to test the suitability of their services with the market under the aegis of a licensed institution, before applying for a license themselves, if necessary.

2 – These developments have led to the rapid growth of Fintechs, drawing on their competitive advantages: speed, agility and responsiveness to customer needs. The increase in the number of licences and authorisations issued by the ACPR illustrates this success: more than half of the 62 electronic money institutions and payment institutions currently in operation were licensed after 2018; the number of agents registered with the ACPR has risen by more than 40% in one year, with almost 3,300 decisions to register agents in 2021.

3- However, the framework established for open banking has its limitations.

First, in terms of the openness of the market: the new service providers remain dependent on traditional institutions, in particular for the opening of a segregated account, which raises questions given the difficulties that many Fintechs encounter in practice in accessing accounts.

In technical terms too. While the use of APIs makes account access more secure, these interfaces must also ensure that new entrants are able to provide their services at a level of quality that is consistent with their business model, as I will discuss later.

B- As part of our supervisory duties, I can draw two lessons from these observations for the development of open finance regulations: one concerns the statuses that are necessary for the opening of the market, and the other concerns the technical means to ensure proper security.

1- While the creation of new statuses would appear to promote the emergence of new business models, we must nevertheless seek to limit unnecessary sources of complexity and, more fundamentally, the risks of regulatory arbitrage. Here are two examples to illustrate my point.

The first concerns the electronic money and payment service activities and the associated risks, which are now very similar. And yet, there are still differences in their prudential and anti-money laundering frameworks.

There are also differences between the competent authorities when it comes to assign innovative payment solutions to regulatory categories.

My second example concerns the draft European MiCA regulation on crypto-asset markets. This draft regulation distinguishes between two kinds of stablecoins: those intended as investment instruments and backed by baskets of assets, Asset-Referenced Tokens (ART), and tokens for payments, Electronic Money Tokens (EMT), whose requirements are similar to those for electronic money.

This distinction requires vigilance in two respects: first, if they are not subject to the same rules, ARTs should not be able to be used for payment purposes; second, care should be taken to ensure that the regulatory requirements are clearly formulated in order to avoid multiple layers of redundant regulation.

2- The second lesson concerns the technical means to be implemented to reconcile openness and security, and in particular the use of APIs.

Should there be an extension of sharing to other financial data, the PSD2 directive calls for a more explicit definition of shareable data, a clearer allocation of responsibilities for authentication, and the promotion of the use of standardised APIs.

Part II: Innovation and integration

A- Let me now turn to the new challenges posed by the development of open banking and its extension towards open finance. I will start with that of promoting innovation without undermining the integration of the European market.

1- In the area of payments, we face a number of challenges, not least that of exchanges between financial intermediaries

The development of the tokenisation of financial assets could lead to a proliferation of new infrastructures that would no longer be interoperable with each other, leading to a risk of market and liquidity fragmentation.

2- This trade-off between innovation and fragmentation risk is also reflected in the settlement asset itself used in payment chains.

If we take the example of stablecoins, their use for the settlement of tokenised financial assets could undermine the stability and efficiency of settlement transactions for new assets by fragmenting the field of settlement assets.

B- To reduce this risk of fragmentation, we have two levers.

1- The first is cooperation between private players to support the efforts of the public authorities to establish a regulatory framework that is clear, proportionate and flexible enough to take account of rapid changes in the market and innovation.

In this respect, there are certainly lessons to be learned from the framework developed for open banking. For example, the deployment of the APIs I mentioned earlier proved to be more complex than expected due to heterogeneous applications, late developments and the lack of an underlying business model.

In this light, two key principles could guide us. On the one hand, institutional players can act as a catalyst for private initiatives on standardisation.

I am referring in particular to the mandate given to the European Payments Council (EPC) for the creation of a dedicated open finance scheme, the SEPA Payment Account Access Scheme (SPAA).

On the other hand, the debate on open finance should also be an opportunity to push for an improvement in the quality of APIs – i.e. premium APIs – by openly addressing the issue of financial compensation for data providers.

2- The second lever is in the hands of central banks, in the form of new services to financial intermediaries.

This is the aim of the Banque de France's experimentation programme with new technologies. These experiments show, in particular, that a wholesale Central Bank Digital Currency (CBDC) would make it possible not only to maintain but also to promote central bank money as the safest and most liquid settlement asset, while adapting it to changes in demand and thus avoiding the fragmentation of settlement assets.

With this improved security, wholesale settlement through distributed ledger could be optimised in terms of efficiency, cost and traceability, including for cross-border payments, by ensuring interoperability between several CBDCs in different jurisdictions.

Part III: Competition and sovereignty

To conclude, I would like to say a few words about the growing challenges related to competition and sovereignty.

A- In this regard, open finance is a development that must be addressed with caution: while it promises to open up the financial market to new

players, it could paradoxically increase its concentration, and compromise our strategic autonomy.

1- Indeed, with the platformisation of the digital economy, companies today aim to rapidly increase their market share in a specific segment and then extend the range of their services in order to build a captive customer base.

Open finance could accelerate this trend, which can already be seen in the payments market, by allowing the exchange and cross-referencing of an ever-increasing volume of data.

This may ultimately prove detrimental to competition. This challenge is particularly acute with the development of BigTechs in the financial services markets, which already have significant market power in the areas of cloud computing, mobile payments or digital identification.

2- Open finance also poses challenges in terms of sovereignty to which we must be attentive.

They primarily occur at the individual level. The increasing volume of data in circulation and its cross-referencing is a considerable challenge for the protection of personal data. Cross-border data flows also complicate the enforcement of regulations and make it more difficult for authorities to act.

Secondly, at the industrial level. Mastering artificial intelligence technologies is now contingent on the quantity and quality of accessible data. It is therefore essential that access to data should not be monopolised by non-European players alone.

Lastly, at the State level, because the concentration of data infrastructures raises concerns about their resilience in the event of an attack. Given the geopolitical risks, these aspects should not be underestimated.

The deployment of tokenised settlement assets across borders would also pose a risk to our monetary sovereignty, if it resulted in the use of stablecoins backed by foreign currencies or CBDCs.

B- To reconcile competition and sovereignty, a "retail" central bank digital currency is obviously a potentially important lever.

1- This was the main aim of the investigation phase launched by the Eurosystem in July last year.

Issuing a retail CBDC, nevertheless, raises a number of operational challenges. In particular because financial intermediaries, including banks,

play a key role in the security and financial stability of our monetary and financial system.

Introducing a CBDC must therefore neither result in the conversion of a significant proportion of bank deposits into assets held in CBDCs – in normal times as well as in times of stress – nor compete with banks in their day-to-day relations with their customers.

These issues need to be addressed by design in the architecture and functionality of a digital euro, for example by introducing holding limits or by promoting an intermediated model.

This is why it is essential that the financial intermediaries, along with the other stakeholders, be properly involved in the investigation phase that we are conducting: an expert advisory group has already been set up at European level, and this consultation will be extended to all stakeholders in the coming months, in particular via the European and French market bodies at our disposal.

2- But other levers will be needed to reconcile competition and sovereignty.

First and foremost, the regulatory lever. Against this backdrop, we welcome two European texts that are currently being finalised

(i) the Digital Operational Resilience Act (DORA), which aims, among other things, to bring critical service providers under the supervision of financial regulators;

(ii) and the Digital Market Act (DMA), which is intended to ensure that service providers have equal access to the hardware and software components of electronic devices.

These competition and sovereignty concerns should also be taken into account in the revision of PSD2.

Secondly, the industrial lever. While our market is and must remain open, it is nonetheless essential to encourage innovation by European players. This is why, in the area of payments, the Banque de France actively supports the EPI2 initiative for a modern European solution.

In conclusion, we can see that the changes taking place in the financial sector offer the prospect of even more accessible, efficient and innovative financial services, while at the same time raising new challenges for both market participants and public authorities.

I am convinced that the only way to meet these challenges is through a multi-faceted approach, with cooperation between public and private players.

That is why the Banque de France is fully committed to promoting innovation within a framework of trust: first, at the level of the regulatory framework and as a supervisor, then by facilitating private initiatives and mobilising the market, and lastly, as a driver and player in innovation.

Record-breaking, ultrafast devices step to protecting the grid from EMPs

New Sandia diode can shunt excess electricity in a few billionths of a second



Scientists from Sandia National Laboratories have announced a tiny, electronic device that can shunt excess electricity within a few billionths of a second while operating at a record-breaking 6,400 volts — a significant step towards protecting the nation’s electric grid from an *electromagnetic pulse*.

The team published the fabrication and testing results of their device on March 10 in the scientific journal IEEE Transactions on Electron Devices. You may visit: <https://ieeexplore.ieee.org/document/9732899>

The team’s ultimate goal is to provide protection from voltage surges, which could lead to months-long power interruptions, with a device that operates at up to 20,000 volts. For comparison, a household electric dryer uses 240 volts of electricity.

An electromagnetic pulse, or EMP, can be caused by natural phenomena, such as solar flares, or human activity, such as a nuclear detonation in the atmosphere. An EMP causes huge voltages in a few billionths of a second, potentially affecting and damaging electronic devices over large swaths of the country.

EMPs are unlikely, said Bob Kaplar, manager of a semiconductor device research group at Sandia, but if one were to occur and damage the huge transformers that form the backbone of our electric grid, it could take months to replace them and re-establish power to the affected portion of the nation.

“The reason why these devices are relevant to protecting the grid from an EMP is not just that they can get to high voltage — other devices can get to high voltage — but that they can respond in a couple billionths of a second,” Kaplar said.

“While the device is protecting the grid from an EMP, it’s at a very high voltage and thousands of amps are going through it, which is a huge amount of power. A material can only handle so much power for a certain amount of time, but we think the material in our diode has some advantages over other materials.”

A regulator valve for the grid

The new Sandia device is a diode that can shunt a record-breaking 6,400 volts of electricity within a few billionths of a second — a significant advancement toward being able to protect the nation's electric grid from an EMP. The team, including Sandia electrical engineer Luke Yates, the first author on the paper, is working towards fabricating a diode able to operate at around 20,000 volts, since most grid distribution electronics operate at around 13,000 volts.

Diodes are electronic components found in nearly every electronic device and serve as one-way regulator valves, said Mary Crawford a Sandia Senior Scientist leading diode design and fabrication for the project. Diodes allow electricity to flow in one direction through the device, but not the other. They can be used to convert AC power into DC power, and in this project, divert damaging high voltage away from sensitive grid transformers.

Kaplar agreed that the diode operates somewhat like a regulator valve in plumbing. He said, "In a regulator valve, even if you open that valve all the way, you can't flow an infinite amount of water through the valve. Similarly, there's a limit to how much current you can flow through our diode. If the valve on the pipe is closed, if the pressure reaches a certain point, it'll burst.

Analogously, the diode cannot block an infinite voltage. However, our EMP device uses the point at which the diode can no longer block the high voltage, holds the voltage to that 'pressure,' shunting the excess current through itself, to the ground and away from the grid equipment in a controlled, non-destructive fashion."

The voltage surges caused by EMPs are a hundred times faster than those caused by lightning, so experts don't know if the devices designed to protect the grid against lightning strikes would be effective against an EMP, said Jack Flicker, a Sandia electric grid resiliency expert on the team.

"The electric grid has a number of different protections," Flicker added. "They range in timeframe from very fast to very slow, and they're overlaid on the electric grid to ensure that an event cannot cause a catastrophic outage of the electric grid.

The fastest protection that we typically have on the grid reacts against pulses at one millionth of a second, to protect against lightning. For EMPs, we're talking ten billionths of a second, a hundred times faster."

The new Sandia device can react that quickly.

Growing perfect layers

Part of what makes the diode special is that it is made from gallium nitride, the same basic material used in LEDs, Kaplar said. Gallium nitride is a semiconductor, like silicon. But because of its chemical properties, it can hold off much higher voltage before it breaks down than silicon, Crawford said.

The material itself also responds very quickly and therefore is a good candidate to achieve the fast response needed to protect the grid from an EMP.

Crawford and materials scientists Brendan Gunning and Andrew Allerman made the devices by “growing” gallium nitride semiconductor layers using a process called chemical vapor deposition, she said.

First, they heat a commercially available gallium nitride wafer to around 1,800 degrees Fahrenheit and then add vapors that include gallium and nitrogen atoms. These chemicals form layers of crystalline gallium nitride on the surface of the wafer.

By tweaking the ingredients and the “baking” process, the team could produce layers with different electrical properties. By building up these layers in a specific order, combined with processing steps, such as etching and adding electrical contacts, the team produced devices with the needed behavior.

“A major challenge of achieving these very high voltage diodes is the need to have very thick gallium nitride layers,” Crawford said.

“The drift regions of these devices have thicknesses of about 50 microns, or 1/6th of a sheet of notebook paper. This may not sound like a lot, but the growth process we use can have growth rates of only one or two microns per hour. A second major challenge is maintaining very low densities of crystalline defects, specifically impurities or missing atoms in the semiconductor material, throughout the growth time in order to generate devices that work at these very high voltages.”

For the team to reach their ultimate goal of a device that operates at 20,000 volts, they will need to grow the thick layer even thicker with even fewer defects, Crawford said. There are several other technical challenges to constructing a device that can operate at such high voltages and currents, she added, including designs to manage the very high internal electric fields within the devices.

Testing ultrafast diodes

Once Crawford's team fabricated the devices, Flicker and his team tested how the devices responded to fast voltage spikes, similar to what would occur during an EMP. His challenge has been modifying a tool to measure the very fast response time of the devices.

"Developing the tools that can accurately measure the very fast responses is very difficult," Flicker said. "If we're talking one or two billionths of a second, they need to be able to measure even faster than that, which is a challenge."

Flicker and his team used very specialized equipment to apply a high voltage pulse, and measure the electric pulse that is reflected back from the diode to tell when the device turns on, very accurately and in less than a billionth of a second.

Useful for smart transformers, solar panel converters and more

Diode devices like the Sandia gallium nitride diode can be used for other purposes, beyond protecting the grid from EMPs, Kaplar said.

These include smart transformers for the grid, electronic devices to convert electricity from roof-top solar panels into power that can be used by household appliances, and even electric car charging infrastructure.

Commonly, solar panel converters and electric car charging infrastructure can handle 1,200 or 1,700 volts, he added. But operating at higher voltage allows for higher efficiencies and lower electricity losses.

Another portion of the project is to develop diodes for these types of devices that operate at high, but not record-breaking voltage but are easier to manufacture, Kaplar said. The Naval Research Laboratory is leading this part of the project.

Some smart transformers and electronic devices can now operate at up to 3,300 volts, Flicker said, but efficiencies would be even greater if they could operate at 10,000 or 15,000 volts with one semiconductor device.

"We have this primary goal of protection of the electrical grid, but these devices have other uses beyond that," Flicker said.

"It's interesting to have our application area, but know that these devices can be used in power electronics, power converters, everything that's at very high voltages."

This research is funded by ARPA-E and the larger project is conducted in partnership with the Naval Research Laboratory, Stanford University, National Institute of Standards and Technology, EDYNX and Sonrisa Research.

You may visit: https://newsreleases.sandia.gov/emp_devices/

Consumers warned about chatbot scam



Cyber criminals are sending phishing emails inviting people to trace deliveries, only for them to fall victim to a chatbot scam.

Which? have alerted customers to a chatbot scam which encourages interaction with a service impersonating the Royal Mail. This is the latest evolution to a number of scam communications seen over the past few years that pose as well-known delivery companies. You may visit:

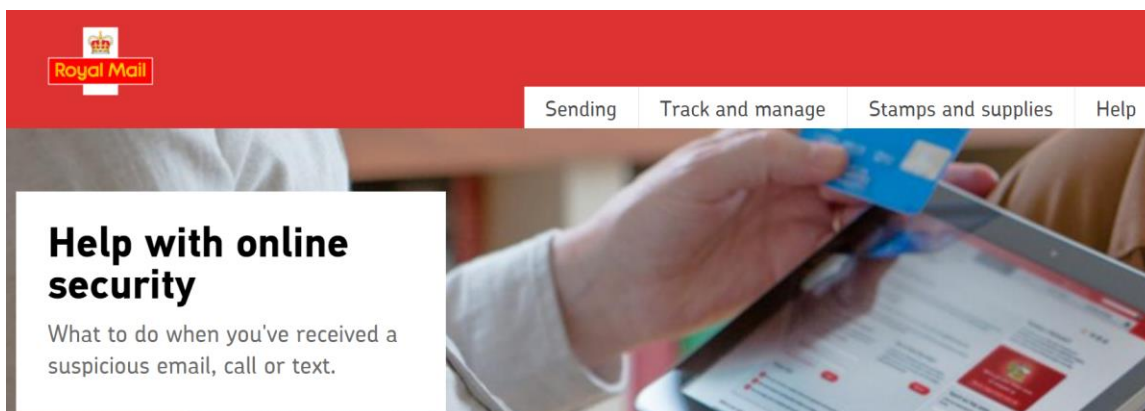
<https://www.which.co.uk/news/2022/03/watch-out-for-this-royal-mail-chatbot-scam/>

Watch out for this Royal Mail chatbot scam

Which? exposes the latest twist on the fake delivery scam



In the example shown on the Which? YouTube channel, consumers are sent a phishing email which encourages use of the chatbot. The victim will then be given plausible details such as a delivery number before being encouraged to click another link, which takes them to a different website where their name, address and payment details are requested.



The Royal Mail website provides plenty of information on how to check whether something you have seen from them is a scam, and what you can

expect from Royal Mail communications. You may visit:


<https://www.royalmail.com/help/scam-protection>

The NCSC has published guidance on how to protect yourself from phishing scams and how you can report suspicious texts, websites, emails and adverts. You may visit: <https://www.ncsc.gov.uk/collection/phishing-scams>

As of February 2022 the NCSC has received over:

 **10m** reported scams

Which has resulted to:

 **76k** scams being removed across 139,000 urls

If you are expecting a delivery and you receive a 'missed parcel' message then don't click the link and use the official website of the delivery company instead.

Blockchain: Financial and Non-Financial Uses and Challenges

U.S. Government Accountability Office (GAO)



Markets—for example the housing market or those for commercial goods—currently rely on institutions like banks or other intermediaries to facilitate transactions.

But blockchain technology could reduce the need for these steps, while providing a trusted, tamper-resistant record of transactions.

While this emerging technology could help level the playing field for businesses of all sizes or enable greater financial inclusion, it also faces some challenges and poses some risks to the consumers and businesses that hope to use it.

In today's WatchBlog post, we look at blockchain technology, including the benefits, challenges, and risks surrounding its use. You may visit:

<https://www.gao.gov/products/gao-22-104625>

What is blockchain?

Blockchain is not a new technology but instead an innovative way of using existing, mature technologies. Its core function is to create a tamper-resistant ledger for digital assets, such as cryptocurrency.

There are two types of blockchain implementations: public (sometimes known as “permissionless”) and private (“permissioned”). Public blockchains can be used by cryptocurrencies such as Bitcoin, and anyone can add to the chain.

Private blockchains are generally used by institutions (such as companies or government agencies) and have restrictions around who can participate in the network.

Financial blockchain applications

The most well-known applications of blockchain are in the financial sector. When people think of blockchain, they may also think of cryptocurrencies like Bitcoin.

Cryptocurrencies are a type of digital representation of value that uses blockchain technology to act as an investment or money. These uses may lead to cost savings, expanded access to financial products, and other transformational changes.

Unfortunately, several risks and challenges may prevent these benefits from being realized, or may even lead to negative consequences for users and the financial system.

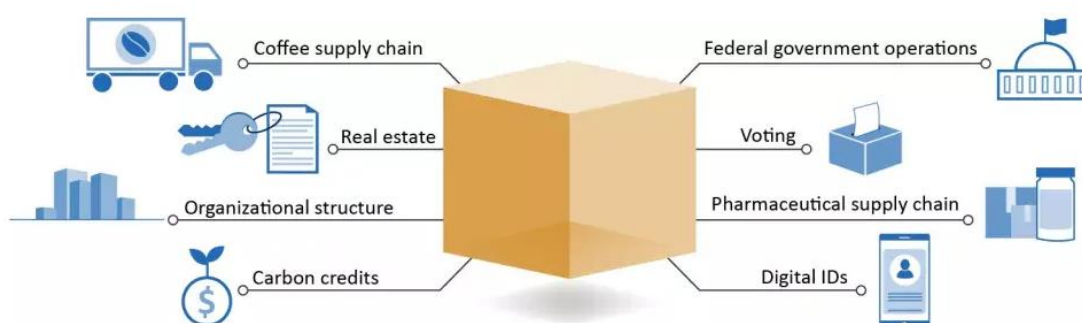
These include risks for users and to the broader financial system, due to a current lack of consumer protections, and the ability to use the technology to facilitate illegal activity.

Potential non-financial blockchain applications

Blockchain has potential non-financial applications. For example, blockchain could help combat counterfeit medicines and trace food-borne illnesses.

Governments could use it to maintain property records or to improve information sharing. Blockchain could also be used to create new kinds of non-hierarchical organizations (i.e., those without clear management titles such as Chief Executive Officer).

Blockchain has many potential non-financial applications



Source: GAO. | GAO-22-104625

However, in our review of some applications, we found that blockchain did not resolve a majority of the critical challenges associated with each application. We also found that blockchain can introduce new challenges. For example, it could end up excluding people who do not have internet or computer access.

Additionally, not many of the non-financial blockchain systems we looked at have made it out of the pilot stage. For example, the Department of the Treasury's blockchain pilot was designed to increase payment efficiency and reduce reporting requirements for federal grantees.

There were two reasons. The selected type of blockchain was inconsistent with National Institute of Standards and Technology cryptographic standards, and there is currently no legal authority allowing the system to operate.

Policy challenges and how to address them

We've developed four policy proposals to help enhance the potential benefits and mitigate the challenges of blockchain technology.

These proposals are for policymakers of all backgrounds—including Congress, state and local governments, and leaders in business, academia, and nonprofit institutions.

1. Policymakers could consolidate blockchain standards. This could help make it easier for organizations trying to use blockchain to integrate the technology with their existing systems.
2. Policymakers could either clarify existing rules and regulations or create new ones around blockchain. This could reduce the current uncertainty around how different implementations of the technology might be regulated, which could help companies and others feel more comfortable about adopting blockchain solutions.
3. Policymakers could support the development of blockchain educational materials. This could help users avoid common blockchain scams and companies be more able to find talent to help them implement the technology.
4. Policymakers could consider using blockchain to meet their own specific goals. This could help public and private-sector institutions determine whether the technology could help resolve specific problems.

Want to learn more about blockchain technology? Check out our new technology assessment on blockchain at:

<https://www.gao.gov/products/gao-22-104625>

Blockchain

Emerging Technology Offers Benefits for Some Applications but Faces Challenges, U.S. Government Accountability Office (GAO)



GAO developed four policy options that could help enhance benefits or mitigate challenges of blockchain technologies.

The policy options identify possible actions by policymakers, which may include Congress, federal agencies, state and local governments, academic and research institutions, and industry.

In addition, policymakers could choose to maintain the status quo, whereby they would not take additional action beyond any current efforts. See below for details of the policy options and relevant opportunities and considerations.

Policy Options That Could Help Enhance Benefits or Mitigate Challenges of Blockchain Technologies

	Opportunities	Considerations
Standards (report p. 38) Policymakers could collaborate to unify standards that focus on the development, implementation, and use of blockchain technologies.	<ul style="list-style-type: none"> • Could simplify fragmented standards and help identify gaps and reduce overlap in standard-setting efforts. • Could identify the areas in which standards would be most beneficial across different sectors of the economy or applications of blockchain. • Could help address challenges around interoperability and data security. 	<ul style="list-style-type: none"> • Could require consensus from many public- and private-sector stakeholders, which can be time- and resource-intensive. • May not be clear which entities should take the lead in establishing internationally recognized standards for different technologies and application areas. • May require new funding or reallocation of existing resources to support new efforts.
Oversight (report p. 39) Policymakers could clarify existing oversight mechanisms, including regulations, or create new mechanisms to ensure appropriate oversight of blockchain applications.	<ul style="list-style-type: none"> • Clear, industry-specific U.S. oversight frameworks could offer the clarity needed for individuals and firms to more successfully engage in blockchain-related commerce in the U.S. • Policymakers, including regulatory entities and developers, could use tools to create oversight mechanisms in addition to testing innovative products and services. • Could provide coordinated and timely clarity to promote safety and soundness, consumer protection, and compliance with applicable laws and regulations to combat illicit activity in blockchain-related commerce. 	<ul style="list-style-type: none"> • Policymakers will need to determine the appropriate level of oversight. Aggressive oversight could hamper innovation and competition as the technology matures, whereas too little oversight could leave consumers and businesses unprotected. • Soliciting input across a range of stakeholders in various sectors may be time consuming and challenging. • May require new funding or reallocation of existing resources.
Educational materials (report p. 40) Policymakers could support the development of educational materials to help users and regulators better understand blockchain technologies beyond existing financial applications.	<ul style="list-style-type: none"> • Could enable instructors to train a workforce skilled in developing, implementing, and using blockchain-based products. • Could increase consumer literacy and help reduce negative public perceptions of blockchain. • Could stimulate critical thinking and innovation, as well as prompt innovative research and development. • Could help prepare policymakers to better use and regulate the latest technologies. 	<ul style="list-style-type: none"> • Educational materials will likely need to be tailored to meet a wide variety of learning needs across multiple target audiences. • May be difficult to identify who could most effectively create educational materials for any particular target audience. • May require new funding or reallocation of existing resources, especially to address the need for education regarding innovative uses of blockchain beyond existing financial applications.

Appropriate uses
(report p. 41)

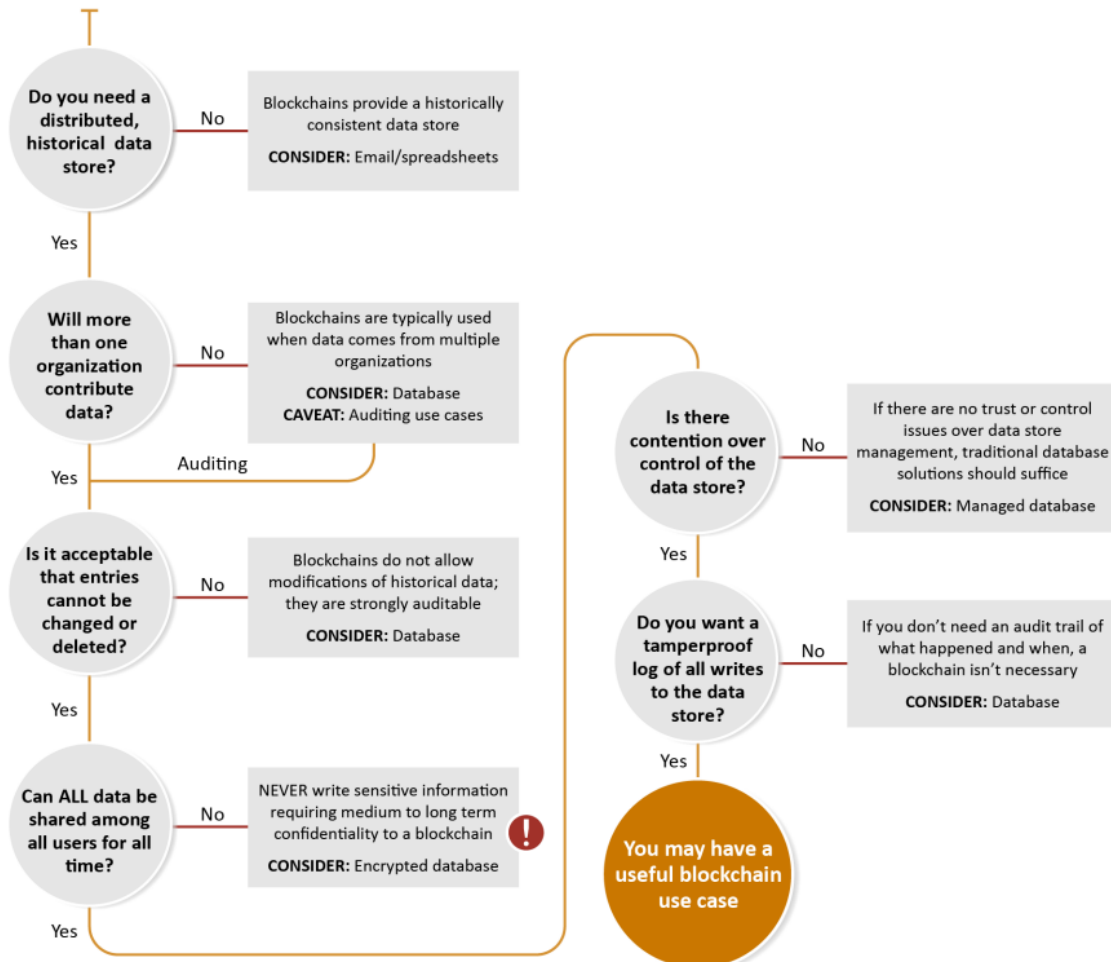
Policymakers could support activities designed to determine whether blockchain is appropriate for achieving specific missions and goals or to mitigate specific challenges.

- Actively investigating where and when blockchain would be the most useful could allow entities to capture the full benefits the technology might offer.
- Supporting blockchain use, where appropriate, could enhance transparency and accountability of existing systems and services.

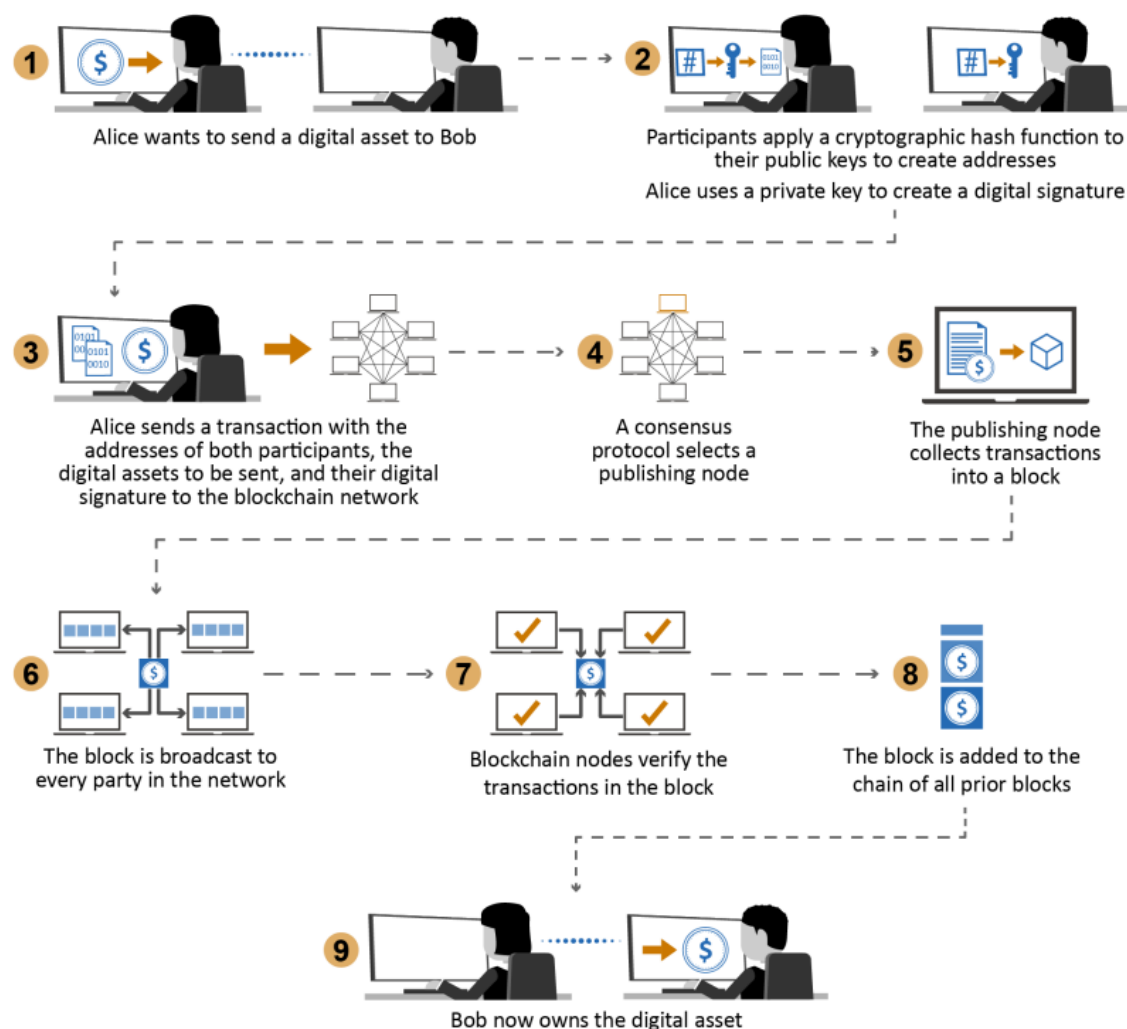
- Legal or regulatory uncertainty may hinder some potential users from benefitting from blockchain.
- Could be difficult to revert to a non-blockchain technology once an entity has invested a significant amount of time and resources.
- May require new funding or reallocation of existing resources.

Source: GAO. | GAO-22-104625

Figure 2: Flowchart for determining whether blockchain may be useful



Source: Department of Homeland Security Science & Technology Directorate. | GAO-22-104625

Figure 3: Simplified example of blockchain operation to send digital assets

Source: GAO and GAO analysis of report by the National Institute of Standards and Technology. | GAO-22-104625

To read more: <https://www.gao.gov/assets/gao-22-104625.pdf>



United States Government Accountability Office
Report to Congressional Requesters

March 2022

TECHNOLOGY ASSESSMENT

Blockchain

Emerging Technology Offers Benefits for Some Applications but Faces Challenges

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 particular individual or entity;
- should not be relied on in the particular 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 prejudice 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 prejudice 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 with regard to such problems incurred as a result of using this site or any linked external sites.

International Association of Hedge Funds Professionals (IAHFP)



At every stage of your career, our community provides training, certification programs, resources, updates, networking and services you can use.

You can explore what we offer to our members:

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

You may visit:

<https://www.hedge-funds-association.com/HowToBecomeMember.html>

2. Monthly Updates – Visit the Reading Room of the association at:

https://www.hedge-funds-association.com/Reading_Room.htm

3. Training and Certification – You may visit:

https://www.hedge-funds-association.com/Distance_Learning_and_Certification.htm