

# Pushing Through Undercurrents

Sectoral and Regional Forces Influencing Technology-driven Systemic Risk, and Resulting Mitigation Opportunities

Part of the Future of Financial Services series

Prepared in collaboration with Deloitte

## Foreword

For feedback or questions,  
please contact:

Drew Propson, Lead Author  
[drew.propson@weforum.org](mailto:drew.propson@weforum.org)  
+1 (917) 224-6239

The World Economic Forum applies a multistakeholder approach to address issues of global importance. Consistent with this mission, the creation of this report involved extensive outreach to, and dialogue with, numerous organizations and individuals. These included the Forum's financial services, innovation and technology communities, and leaders from academia and the public sector.

The outreach comprised over one hundred interviews and seven global workshops, conducted virtually and in person, over the past twelve months. The aim of these dialogues was to capture insights around sectoral and regional forces that influence the spread of technology-driven systemic risk across the financial system and to identify targeted mitigation opportunities available for financial services players.

The holistic and global content of this report would not be as complete without contributions from the subject matter experts who helped to shape our thoughts on the emergence of technology-driven systemic risks and possible risk mitigation approaches. We particularly thank this project's Steering Committee and Working Group. Their expertise and generosity with their time have been invaluable. Also critical has been the ongoing institutional support for this initiative from the World Economic Forum and the leadership of our Chairman, whose vision for a more inclusive, resilient and sustainable world, particularly in these times of increasing complexity and fragmentation, has been integral to this work. Finally, we are grateful to Deloitte for their commitment to, and support of, this project.

## Editor's note

The deepening adoption of technology within global financial services continues to come with considerable benefits while also introducing new risks that threaten the stability of the financial system if not properly managed. In an effort to better understand these risks and identify approaches to addressing them, the World Economic Forum launched the Technology, Innovation and Systemic Risk (TISR) initiative in 2021 to explore the role of technology in both increasing and mitigating systemic risk in the financial system and, by extension, the economy.

The publication of [Beneath the Surface](#) in 2021 raised new questions about the sectoral and regional conditions under which technology-driven risk can originate and spread across an ecosystem and which targeted mitigation opportunities will warrant further exploration. While mitigation approaches for systemic risk in financial services have been examined in other research studies, few have looked at how technology and sources of innovation can be used to identify and mitigate specific technology-driven systemic risks, with consideration for jurisdictional circumstances and geographical nuances.

This comprehensive study brings together a global community of stakeholders across industries and disciplines to better understand these research topics and provide strategic insights to the public and private sectors.

The outcomes of this research have reinforced the urgency for financial ecosystem players to sharpen their understanding of the origination points and spread of technology-driven risk from sectors and regions to implement effective mitigation solutions.

It is hoped that this document will help you push through the undercurrents influencing technology-driven systemic risk and inspire you to initiate new conversations around mitigation opportunities.

Drew Propson

Head, Technology and Innovation in Financial Services,  
World Economic Forum

Rob Galaski

Vice-Chairman and Managing Partner, Financial Services,  
Deloitte

*Other recent reports from the Future of Financial Services series*



2019



2019



2020



2021

## Members of the Steering Committee



**Sami Ahmed**

Senior Vice-President, Data and Advanced Analytics, OMERS



**Shivaji Dasgupta**

Global Head, Data Products and Artificial Intelligence, Deutsche Bank



**Kate Platonova**

Group Chief Data Officer, HSBC



**Stefan Altner**

Managing Director, Head, Risk Governance and Assessment, Julius Baer



**Kfir Godrich**

Managing Director, Global Head, Technology and Enterprise Services, BlackRock



**Dirk Stephanek**

Head, GCOO Risk Management, UBS



**Peter Cai**

Managing Director, Global Head, Risk Data, Analytics, Reporting and Tech (DART), Citigroup



**Gero Gunkel**

Chief Operating Officer, ZCAM, Zurich Insurance



**Aman Thind**

Global Chief Architect, State Street



**Fergal Coburn**

Chief Technology Officer, Allied Irish Banks



**Basak Koralturk**

Head, Corporate Strategy, JP Morgan Chase



**Susanna Wooders**

Chief Risk Officer, Fidelity International



**Robert Contri**

Global Financial Services Industry Leader, Emeritus, Deloitte



**Lena Mass-Cresnik**

Chief Data Officer, Moelis & Company



**Thomas Zschach**

Chief Innovation Officer, SWIFT

## Members of the Working Group



**Tobias Amiet**  
Managing Director, Global Head, Products and Services Compliance, Julius Baer



**Philip Garner**  
Head, Innovation, Lloyds Banking Group (through April 2022)



**Vincent Loy**  
Assistant Managing Director, Technology, Monetary Authority of Singapore



**Steven Asprey**  
Managing Director, Global Diversified Program, OMERS



**Eva Gustavsson**  
Director, Government Relations EMEA, PayPal



**Christian Mittelberg**  
Global Risk Officer, S&P Global



**Shane De Zilwa**  
Vice-President, Analytics, Verisk



**James Harborne**  
Head, Group Digital Public Policy, HSBC



**Harqs Singh**  
Managing Director and Chief Operating Officer, Technology Platforms, Data & AI, Information Security and Enterprise Services, BlackRock



**Nicola Feakin**  
Head, Technology Risk and Management, Oversight, Fidelity International



**Valérie Hoess**  
Head, Digital and AML Policy, Political Affairs, Deutsche Bank AG



**Tobias Wild**  
Head, Architecture and Technical Delivery, ZCAM, Zurich Insurance



**Doria Ferrante**  
Senior Vice-President, Product and Payment Services Risk, Visa



**Michael Leibrock**  
Chief Systemic Risk Officer and Head, Counterparty Credit Risk, DTCC

## Members of the Project Team

### Project leadership

The Technology, Innovation and Systemic Risk project leadership team includes the following individuals:

#### World Economic Forum

Drew Propson, Lead Author, Head of Technology and Innovation in Financial Services  
 Matthew Blake, Head of Shaping the Future of Financial and Monetary Systems

#### Professional services leadership from Deloitte Canada

Rob Galaski, Co-Author, Project Adviser, Vice-Chairman and Managing Partner, Financial Services  
 Hwan Kim, Project Adviser, Partner  
 Gayatri Suresh Kumar, Project Adviser, Partner  
 Luca De Blasis, Project Adviser, Chief of Staff

### Project authors

The World Economic Forum expresses its gratitude to the following individuals on the project team:

#### Deloitte Canada

Ayesha Madan, Senior Consultant (Seconded to the Forum)  
 John Okoronkwo, Manager (Seconded to the Forum)

---

### Additional thanks

The project team expresses gratitude to the following individuals for their contributions and support:

Emina Ajvazoska	Laurent Collet	Vincent Gouverneur	Markus Salchegger	Dimitri Tsopanacos	Tony Wood
Laurent Berliner	Jay Deverett	Suchitra Nair	Ian Sandler	Denizhan Uykur	Saemoon Yoon
Julie Bernard	Valeria Gallo	Michael Nassar	Marius von Spreti	John Wang	Jenny Zhang
Jonathan Burdett	Richard Godfrey	Mike Ritchie	Usha Sthankiya	Michelle Watt	

# Contents

Context and approach 8

Executive summary and key findings 12

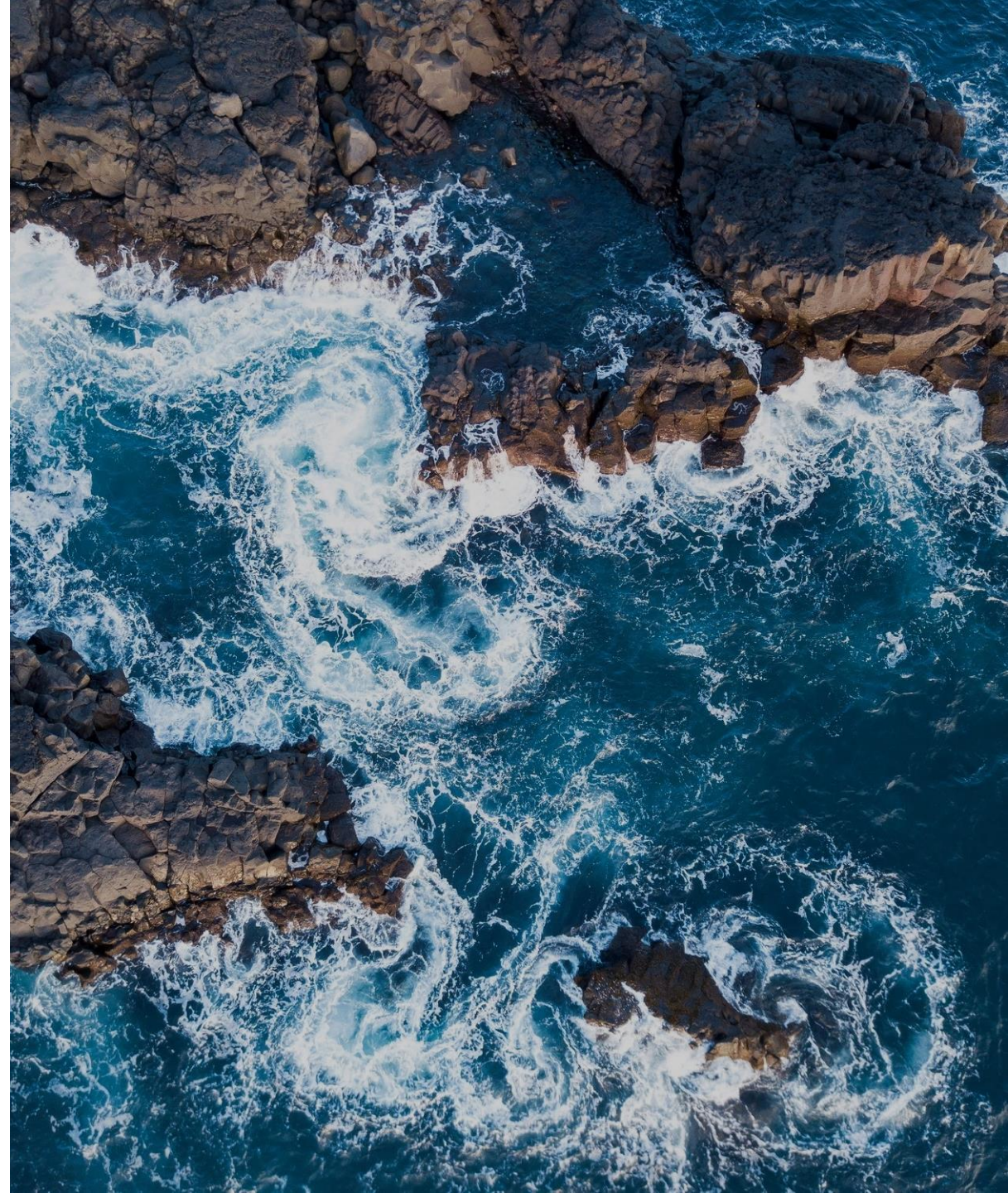
Sector-specific risks and mitigation 21

Regional risks and mitigation 82

Conclusion 93

Acknowledgements 95

Endnotes 98



# Context and approach

---



## Recent explorations of technology-driven systemic risk in financial services have raised new questions about which hidden forces influence risk and what targeted mitigation opportunities are available

- The Forum’s most recent report of the Technology, Innovation and Systemic Risk (TISR) Initiative, [Beneath the Surface](#), was launched in 2021 to explore the relationship between adopting technologies in financial services and systemic risk.
- This current report, Phase II of the TISR initiative, explores the underlying sectoral and regional forces that influence technology-driven systemic risk and targeted mitigation opportunities.

TISR Phase I identified six systemic risk themes that have emerged from the growing adoption of technology...

...while raising new questions for Phase II about the *sectoral and regional forces* that influence technology-driven systemic risk and mitigation

### Phase I systemic risk themes:



Digital interdependencies



Emerging sources of influence



New drivers of financial exclusion



Gaps in entity-based regulation



Shared model vulnerabilities



Conflicting national priorities

### Core research objectives:



How do technology-driven systemic risks originate and spread within **sectors** in the financial services ecosystem?



What types of **entities** in financial services have the most influence in exacerbating or mitigating technology-driven systemic risks?



What **sectoral and regional opportunities** exist to mitigate technology-driven systemic risks?

Over the past year, over 100 financial services and technology experts have been engaged in global workshops and expert interviews.\*

### Global workshops

Seven workshops were conducted during 2022, both virtually and in person. These sessions brought together leaders across the financial ecosystem: financial institutions (e.g. banks, asset managers, exchanges, infrastructure providers), financial and non-financial technology firms, regulators and policy-makers. Non-governmental organizations and academic institutions were also engaged in a series of interactive discussions with these entities. Three workshops explored the sectoral and regional forces influencing the trajectory of technology-driven systemic risk. Four workshops tested and refined insights on targeted and technology-led mitigation opportunities available for sectors, entities and regions.

### Expert interviews

Interviews were conducted with over 100 public and private sector leaders from prominent entities and experts adjacent to the industry.



The inclusion of company case studies or references within this report does not reflect an explicit endorsement of the company or its products and services by the World Economic Forum.

\*Note: Please see Acknowledgements for a list of individuals who participated in the workshops and interviews

This report introduces leaders, regulators and policy-makers to the sectoral and regional forces that influence technology-driven systemic risks in financial services and how these risks can be mitigated



- This report **WILL**:
- Explore how sectoral forces influence the way technology-driven systemic risk spreads
  - Explore how regional forces influence the spread of cross-sector risks
  - Determine which entities are best positioned to lead mitigation opportunities to address technology-driven systemic risk
  - Present targeted opportunities to strengthen efforts to address technology-driven systemic risk.



- This report **WILL NOT**:
- Identify idiosyncratic risks that an individual financial ecosystem player faces from the adoption of emerging technology
  - Investigate sectoral forces influencing systemic risks that are not driven or amplified by technology
  - Provide detailed implementation approaches to execute mitigation opportunities.

### This report **seeks to help**:

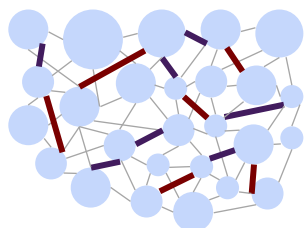
- **Leaders focused on strategy, innovation and/or risk at financial and non-financial organizations** to gain clarity into:
  - The sectoral and regional forces that drive their unique exposure to technology-driven systemic risk
  - Targeted mitigation opportunities for public and private sector players.
- **Policy-makers and regulators** better understand how to design targeted policies and mitigation strategies to support private entities across different sectors and regions.

# Executive summary and key findings

---

## The sectoral and regional forces that underlie technology-driven risk present both challenges and mitigation opportunities for financial services ecosystem players

### Technology-driven risks can proliferate across sectors and regions to grow systemic when...



- 1 ... there is fragmentation across product development and distribution areas in financial services
- 2 ... speed, accessibility and cost are unintentionally emphasized over long-term resilience and transparency
- 3 ... highly dynamic geopolitical and regional forces outpace a financial institution's resilience measures for cybersecurity, workforce shortages and environmental threats.

### Sectoral and regional forces reveal targeted opportunities for public and private players to enhance mitigation efforts by...



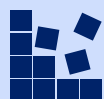
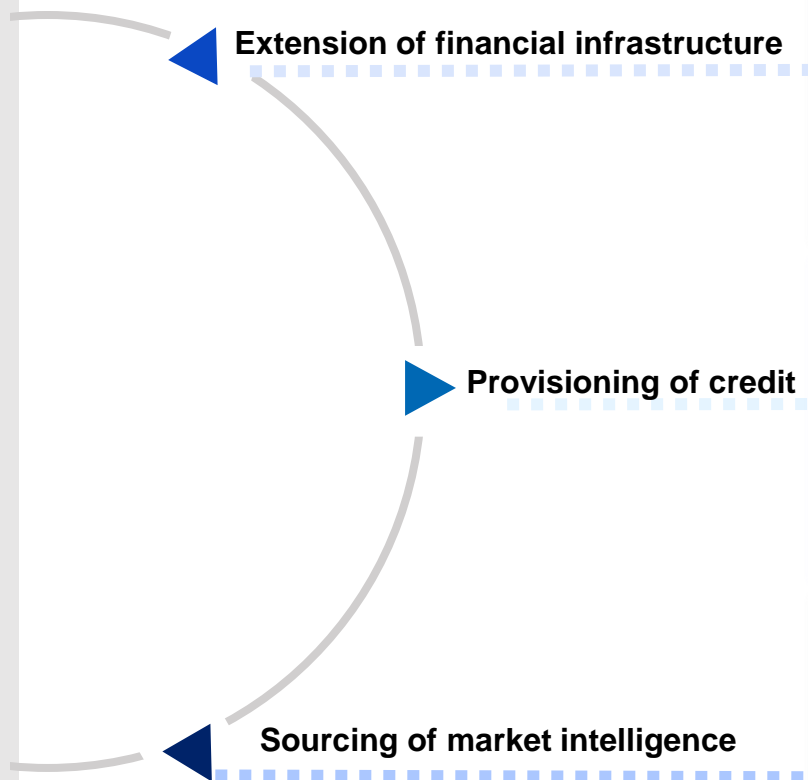
- 4 ...promoting trust-enhancing products that help consumers make informed decisions and minimize the trade-off between bringing transparency and offering convenience
- 5 ...dismantling information siloes to identify clusters of technology-driven risk at the ecosystem level
- 6 ... extending predictive analytics capabilities to better determine the effects of future geopolitical and regional uncertainty on a financial institution's resilience.

# Technology-driven risks can proliferate across sectors and regions to grow systemic when there is fragmentation across product development and distribution areas in financial services

Three areas where fragmentation is most prominently occurring are the extension of financial infrastructure, provisioning of credit and sourcing of market intelligence

## Where is fragmentation coming from?

## How is this accelerating the spread of technology-driven risk?



The fragmentation of financial infrastructure is advancing through “as-a-service” models that are being offered by regulated financial services entities. The risk of incomplete oversight will grow as the entities responsible for risk oversight (e.g. regulated financial institutions) decouple from those that manufacture and distribute financial products (e.g. non-financial players).

*Example: Regulated traditional financial institutions are extending their existing infrastructure to non-financial players through banking-as-a-service (BaaS) products and depending on partnerships with platform and application programming interface (API) providers to participate in embedded financial offerings.*



Large multinational technology platform providers are strengthening their alliances with non-financial players to displace traditional financial credit offerings and harvest more first-party data. This pattern has increased blind spots to credit default risk and fragmented the development and distribution of credit products into multiple non-financial entities.

*Example: Point-of-sale credit offerings from technology platforms (e.g. buy now pay later) are helping retail players grow faster, giving these technology platforms access to first-party consumer spending data, and forming credit ecosystems that operate without traditional financial players.*



The mainstream distribution of market intelligence has fragmented into partially regulated entities like data brokers and social news providers. This intelligence is feeding directly into artificial intelligence (AI) models that make real-time financial decisions and has the potential to amplify the impact of data deception tools (e.g. deepfakes) on financial markets and consumer trust.

*Example: Investment firms are relying on unregulated data brokers for access to non-financial data generated and sold by adjacent players (e.g. retailers) to expedite their access to rich sources of market intelligence.*

## Some new entrants across sectors are unintentionally emphasizing near-term competitive advantages over long-term resilience and transparency



### The separation of risk management and product distribution functions




- Value propositions from groups of new entrants are focused on enabling instant and affordable access to financial products for all consumers and less on the ability to manage and anticipate the associated long-term risks. This is leaving the ownership and management of risk downstream to traditional financial services players.
- Separating risk management and product distribution capabilities is beginning to reduce end-to-end visibility for consumer protection (e.g. protection against chronic overborrowing) and fuel future product liability challenges and potential consumer distrust in the industry (e.g. distrust from a lack of transparency in how personal data is managed).



### The rising cost of conducting due diligence and reinforcing trust with consumers

- The cost and complexity of conducting due diligence will continue to rise for financial institutions as the externalization of infrastructure and data services will increase the number of third-party relationships to manage.
- Inefficiencies in centralized due diligence and transparency solutions (e.g. third-party audits and certifications that verify financial solvency and data protection measures for consumers) will continue to challenge financial services players in bringing transparency to consumers while competing on speed, cost and convenience.

# Highly dynamic geopolitical and regional forces are outpacing a financial institution’s resilience measures against cybersecurity, workforce shortages and environmental threats

Highly dynamic geopolitical and regional forces	Where regional vulnerabilities are growing	Example
<p><b>Sophisticated and geopolitically-motivated cyberattacks</b></p> 	<p><b>1. Risk assessments for vulnerable critical service providers and institutional clients</b></p> <p>Cyberattacks are becoming increasingly geopolitically motivated, sophisticated and frequent against financial institutions and critical service providers. Given limitations in the speed and granularity of risk assessments currently conducted for a financial institution’s client base and supplier network, the evolving nature of cyberattacks on these types of institutions may be putting financial institutions at risk.</p>	<p><i>Cyberattacks on businesses providing critical services to a nation can be used as a gateway for damaging a nation’s economy (e.g. Hydro-Quebec’s critical role in supplying energy to the US<sup>2</sup>), making these institutions more likely targets for cyberattacks. This can increase credit default risks for financial institutions that fund these institutions.</i></p>
<p><b>Heightened competition for technology talent pools</b></p> 	<p><b>2. Maintenance of critical operations</b></p> <p>Regional competition for technology talent and growing competition from adjacent industries are leaving some regions vulnerable to shortages in the skills required to maintain critical operations (e.g. disaster recovery solutions). Localized dependencies to fulfil critical services (e.g. customer support) are also creating potential clusters of concentration risk should talent availability in these regions be disrupted.</p>	<p><i>A 2022 global report on talent trends revealed that 49% of C-suite and human capital leaders in the banking and financial services industry (BFSI) report talent scarcity for IT skills.<sup>3</sup></i></p>
<p><b>Chronic changes in climate patterns</b></p> 	<p><b>3. Pricing of climate-related risk within financial services products</b></p> <p>Limitations in the availability of, and accessibility to, climate-related data, including data on the chronic effects of climate change (e.g. a long-term gradual change in agricultural productivity<sup>1</sup>), are affecting financial institutions’ ability to price in the financial risks of climate patterns, loan adjudication, insurance policies and investment policies.</p>	<p><i>Government-sponsored enterprises, such as Fannie Mae and Freddie Mac, hold over \$6 trillion in mortgage debt that does not price flood risk.<sup>4</sup></i></p>



## Sectoral and regional nuances reveal targeted opportunities for traditional financial institutions and fintechs to promote trust-enhancing products and services that help reinforce financial system stability

### There is an emerging opportunity for incumbents and fintechs to offer trust-enhancing value propositions in a fragmented product landscape



- The fragmentation of financial services capabilities has led to gaps in holistic consumer protection practices, as fewer private entities offer end-to-end visibility on consumers' financial health or are obligated to make a customer whole.
- There is a growing market gap for offering consumers personal financial management across their financial dealings while maintaining a highly convenient and affordable shopping experience.



### How can financial services entities address this opportunity?



- Traditional financial institutions are uniquely positioned to “connect the dots” and extend their role as trusted partners for consumers who have multiple financial dealings with niche and adjacent players.
- In partnership with fintechs, traditional financial institutions can also use insights into their customer's financial activity across niche offerings to further deepen customer relationships and reinforce value propositions that are centred on trust and transparency.

### Where can traditional financial institutions and fintechs offer trust-enhancing products and services?



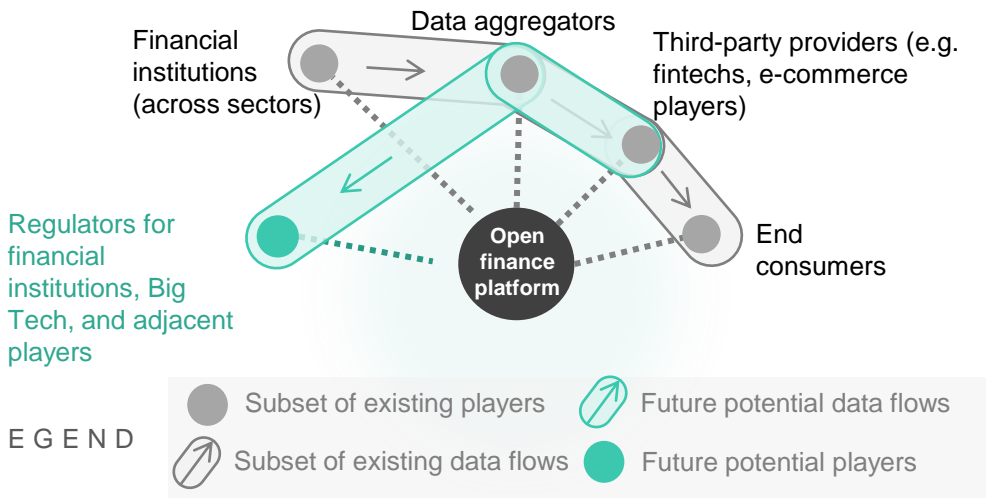
- As consumer data becomes democratized through open banking platforms, connecting consumer financial activity across different products can enable **automated money management intelligence services that financial services players can offer to guide long-term customer choice and balance decisions** that protect long-term financial health.
  - *Example: Finicity and Plaid are aggregating consumer and small business account data and applying advanced analytics to offer personalized financial advice<sup>5</sup>*
- Liability insurance products can **protect consumers from data breaches or unauthorized activities that cannot be attributed to a single third-party provider** or financial institution (e.g. a consumer's bank account data is compromised in a merchant's website, which is built on a platform by a third-party provider).
- Alongside existing financial and media literacy efforts, financial institutions and fintechs can embed **authentication and digital credential services** for financial services-related content to help protect consumers from the effects of disinformation and data deception tools.

# Public and private sector players can collectively dismantle information siloes to help better identify technology-driven risk at the ecosystem level

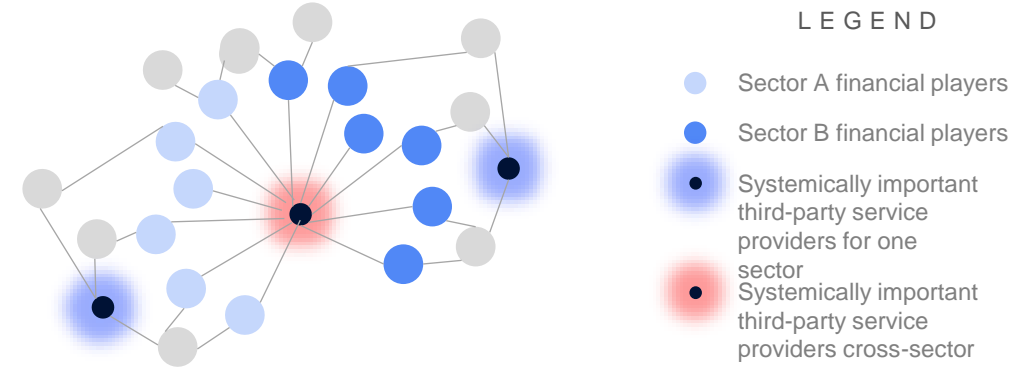
As an entity’s network size grows more relevant in determining systemic importance (as identified in the Phase I report), regulators and institutions can use existing open data platforms to access and aggregate real-time and verifiable insights on technology-driven risk

## How can information siloes be dismantled and distributed?

- Regulators can aggregate existing open banking platforms and transactional data to monitor the trajectory of regional credit risk trends.
- Standardized data aggregation from open finance ecosystems can help regulators across jurisdictions compare regional risk trends and design data-driven approaches to regulation (e.g. by analysing the implications of active regulation on a customer’s financial activity).



## How can technology-driven risk be identified at the ecosystem level?



- Mapping the degree of common service provider relationships across cloud infrastructure, alternative data providers and API stack providers will help regulators identify common dependencies across financial institutions (regionally or by sector).
- Generating and aggregating these datasets can make way for intelligent monitoring solutions that predict disruptions to a third-party vendor’s financial health and security posture and enable proactive action by financial institutions and regulators.

## Financial services players' predictive analytics capabilities should reflect future geopolitical and regional uncertainty and be applied towards resilience efforts

In what ways can private and public financial ecosystem players use predictive analytics capabilities to better meet the evolving speed of geopolitical and regional forces?



Consider new dimensions with which to predict and monitor a financial services players' operational resiliency



- Scenario implications and resilience strategies must include **geopolitically-motivated triggers and conditions that can compromise critical third-party service providers** or critical institutions to whom financial institutions have sold products and services.
- Exposure to **regional risk vectors** (across regulatory, cyberattack targeting and environmental factors) **should be embedded as an input variable** when updating risk profiles and pricing financial products for a financial institution's client base.



Embed real-time and forward-looking geopolitical data-gathering mechanisms



- Financial institutions can engage automated operational resilience platforms using **global market intelligence data to aggregate operational resilience risk scores** and evaluate a firm's risk exposure before engaging them as a third-party provider.<sup>6</sup>
- Financial services players should use synthetic datasets to enrich intelligence data from regions where diagnostic data is difficult to procure. These datasets will ensure better **representation of regional forces when simulating future geopolitically-triggered events** and response plans.



Test for sectoral resilience through cross-jurisdictional exercises that use simulation techniques



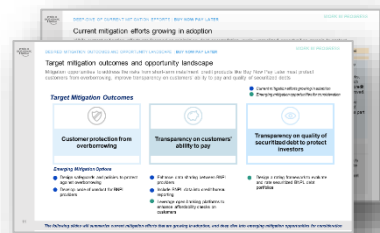
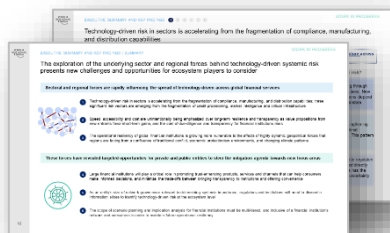
- International resilience exercises should focus on **simulations that disrupt a sector's shared global infrastructure (e.g. a global payments network) and test response patterns and regional exposures** for geopolitically-motivated cyberattacks.
- International resilience exercises and outcomes should also be analysed at a regional level to **determine what future public funding backstops and buffers are required** to contain the systemic effects of attacks.

This report is comprised of three core sections that explore the origination of technology-driven systemic risk across sectors and regions, and the targeted mitigation opportunities available

**1** Key findings

**2** Sectoral exposures to systemic risk and targeted mitigation opportunities

**3** Regional influences and mitigation opportunities



— Description —

Review key takeaways for public and private sector players within the financial services ecosystem

Explore the systemic nature and underlying forces behind technology-driven risks originating in financial services sectors (“sector-specific risks”)

Examine existing efforts and emerging opportunities available to identify and address sector-specific risks

Explore the regional forces that influence the proliferation of technology-driven systemic risks across financial services sectors, and the targeted mitigation opportunities available for consideration

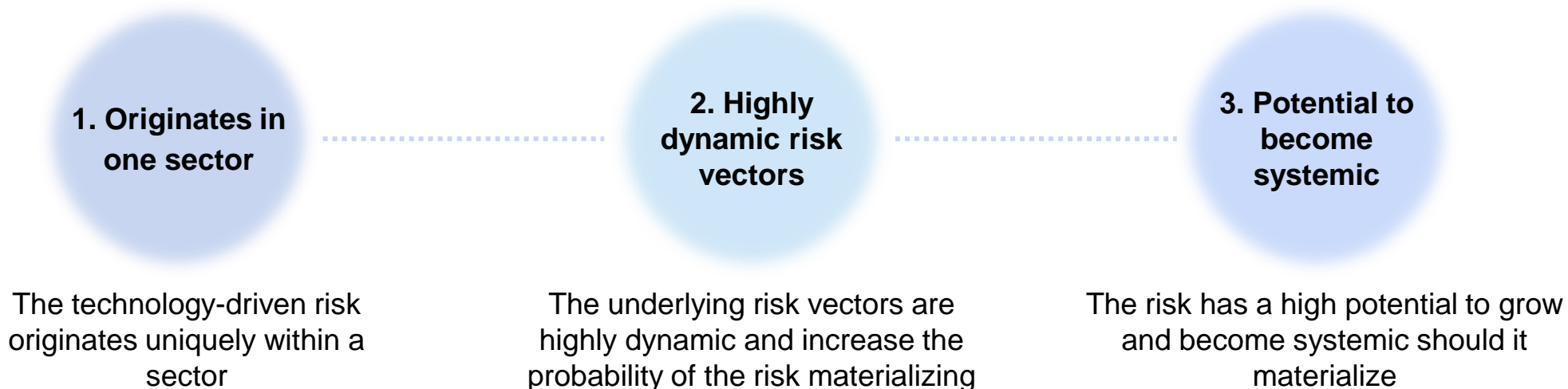
# Sector-specific risks and mitigation

---

## SECTOR-SPECIFIC RISKS

A collection of sector-specific risks have been identified as originating within a sector and having the potential to become systemic

**Sector-specific criteria:** In order to be classified as a sector-specific risk, the risk must meet all three criteria below.



**Prioritized sector-specific risks:** Two sector-specific risks have been identified for each sector (non-exhaustive) and will be explored in the following section of the report.

Capital markets*	Investment management	Payments	Banking	Insurance
Market manipulation from the distribution of synthetic media	Market volatility from speculation fuelled by social media	Accumulation and securitization of buy now pay later (BNPL) debt	Risk exposure from banking-as-a-service (BaaS) offerings	Vulnerabilities in parametric insurance smart contracts
Potential for contagion to spread into traditional markets if crypto-asset ecosystems collapse	Investor manipulation from compromised sensor-generated data	Security vulnerabilities of decentralized central bank digital currency (CBDC) architecture	Inadequate stability mechanisms for stablecoin arrangements	Growing protection gap for catastrophic cyberattacks

\*In this report, capital markets includes market infrastructure sector players

# The following section shares findings on the top sector-specific risks alongside targeted mitigation opportunities

Each sector-specific risk exploration will include the following:



## 1. Overview of sector-specific risk

- Background and context on the sector-specific risk
- Findings on the highly dynamic risk vectors that exacerbate the sector-specific risk



## 2. Plausible systemic scenario and amplifying forces

- A potential systemic scenario that illustrates the second-order impacts on other ecosystem players if the sector-specific risk materializes
- Exploration of the **entity** and **regional** forces that increase the probability and impact of the sector-specific risk materializing



## 1. Desired mitigation outcomes and opportunity landscape

- A summary of mitigation outcomes required to address the sector-specific risk
- A summary of current mitigation efforts and emerging opportunities for consideration to enable desired outcomes



## 2. Deep-dive into current mitigation efforts

- A summary of collaborative mitigation efforts largely government- or sector-initiated that are currently gaining traction across the ecosystem (including relevant examples)
- Analysis of the areas of opportunity available to strengthen existing efforts



## 3. Deep-dive into emerging mitigation opportunities

- An exploration of each emerging mitigation opportunity, how the solution can be executed to address the effects of the sector-specific risk, and the conditions necessary for success



# Capital markets



## Market manipulation from the distribution of synthetic media

Novel deception tools like deepfake voice phishing and synthetic social botnets that are underpinned by AI are becoming increasingly popular methods to spread disinformation that can maliciously influence financial markets.

### Background

The rapid growth of the synthetic media market and research advances in deep-learning algorithms have quickly lowered the financial and technological barriers for malicious actors to manipulate financial markets, specifically through the proliferation of deepfake videos and synthetic botnets. Generative AI modelling companies are seeing a rapid increase in deepfake applications, with content on the internet growing at the rate of 400% year on year.<sup>7</sup> While the adoption of synthetic media by legitimate actors grows in parallel (e.g. using synthetic datasets to enrich investment simulations), the implications of non-malicious inaccuracies within synthetic datasets may not yet be systemic.

Deepfake technologies are also beginning to take up a larger share of cyberthreats. Two out of three respondents in the 2022 Global Incident Response Threat report indicate that malicious deepfakes are increasingly being used for attacks. This trend reflects a 13% increase from 2021.<sup>8</sup>

### Emerging risks

- **Connected devices controlled by malware (“synthetic botnets”)** are increasingly being used to produce synthetic social media content positioned to induce withdrawals from fake “run on the bank” scenarios (impersonations of bank customers claiming to be unable to withdraw their deposits) and flash crash events (hacking and posting messages about fictional market-moving events on behalf of trusted accounts, like the Twitter account of a central bank chief).<sup>9</sup>
- **With the increased availability of large image and video databases accelerating the accuracy of AI models** used to generate deepfake videos and images and the growing maturity of deepfake algorithms, it is becoming increasingly difficult for fraud-detection software to identify deepfakes that target multiple attack surfaces (voice and video), meaning the risks from synthetic media are primed to grow with potentially systemic implications.

## Risk vectors



Ease of access to deepfake tools, open-source libraries and generative AI applications (e.g. ChatGPT) are lowering the cost of producing synthetic media



The growing volume of images and videos of systemically important individuals (e.g. central bank governors, bank CEOs) increases the precision and effectiveness of malicious synthetic media



Systemically important institutions that use social media channels to communicate with the public can increase the degree of trust placed in these platforms

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

If disinformation about interest rates proliferates across credible social media platforms and accounts through the use of synthetic media (e.g. the social media account of a trusted public official is compromised, and a face-swap video about a dramatic drop in interest rates is posted nationwide), shifts in public sentiment about financial markets can lead to the following second-order impact:





#### Impact on investor portfolios through bond price volatility

In response to dramatically lower interest rates, retail and institutional investors may begin selling their positions on bonds or money market accounts, resulting in sharp movements across financial markets.

#### Consumer mistrust and scepticism in government institutions

Individuals may not trust future communications made by public officials on social media platforms. As a result, long-term reputational damage to government institutions and lingering scepticism around current monetary policies may contribute to prolonged market volatility.

### Forces that can amplify and accelerate the risk

 Regional force  Entity force



#### Communities with high dependency on alternative media for information access

Communities with unaffordable or unstable internet connectivity are primed to consume most of their information from social media providers that have partnered with local network carriers (e.g. Meta's FreeBasics Program in Philippines).<sup>10</sup>



#### Technology companies lowering the financial barriers to generate synthetic media

The cost of generating synthetic media is dropping as companies are improving video-generation methods (e.g. Microsoft, GPT-3 language models) that enable users to use off-the-shelf or open-source machine learning software to quickly generate fake content.



#### High-frequency trading algorithms connected to real-time high-speed data feeds

High-frequency algorithmic trading programs that read real-time high-speed data feeds may not distinguish real news from disinformation and can amplify the systemic effects of synthetic media that are deployed on credible channels.




## Target mitigation outcomes and opportunity landscape


Mitigation opportunities to address the risks from distributing synthetic media about financial markets must centre on more robust media moderation, equipping users to recognize disinformation and strengthening authentication efforts for both content and users.

### Target mitigation outcomes


- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Stronger synthetic media moderation**



**Stronger content authentication and media literacy**



**Stronger user authentication on alternative media platforms**

### Mitigation opportunity landscape

- Limit the monetization opportunities available for synthetic media shared on social media.
- Crowdsourcing social media fact-checking capabilities by encouraging digital citizenship and collective trust.
- Embed digital content credentials within the social media upload process to maximize transparency.
- Decentralize transparency efforts through plug-in tools powered by artificial intelligence.
- Extend biometric authentication requirements for systemically influential individuals' social media accounts.

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*

## Current mitigation efforts growing in adoption

Current efforts to identify disinformation and boost media literacy among communities are gaining traction, while unrealized opportunities remain to better protect influential social media accounts from being compromised and sharing disinformation.

		Government-initiated	Sector-initiated
<p><b>Limit the monetization opportunities available for synthetic media shared on social media</b></p> <p>The European Commission’s Code of Practice on Disinformation was updated in 2022 to ensure that disinformation distributors do not benefit from advertising revenues and that signatories commit to stronger measures to avoid the placement of advertising next to disinformation shared on media platforms.<sup>11</sup></p>	<p><b>Crowdsource social media fact-checking capabilities by encouraging digital citizenship and collective trust</b></p> <p>Large social media platforms are beginning to employ users to police disinformation and publish recommendations within posts to scale their fact-checking capability, maximize transparency for users, maintain neutrality and help reinforce media literacy (e.g. Birdwatch/Community Notes, Twitter’s fact-checking tool).</p>	<p><b>Embed digital content credentials within the social media upload process to maximize transparency</b></p> <p>Content creator platforms are championing initiatives that increase users’ visibility into digital credentials (including edit history) for content shared online, thereby helping users distinguish reality from fabrication (e.g. Adobe’s Content Authenticity Initiative).<sup>12</sup></p>	<p><b>Decentralize transparency efforts through plug-in tools powered by artificial intelligence</b></p> <p>Fintechs like Factinsect offer plug-in fact-checking software for users to compare alternative media content against selected quality media by visually spotlighting contradictory or disproved text within seconds.<sup>13</sup></p>

### Considerations to strengthen existing mitigation efforts

As a part of the European Commission’s media literacy initiatives, platforms should be encouraged to publicly classify the content subject to limitations in advertising revenue due to the Code of Practice on Disinformation.

A crowd-sourced fact-checking tool on social media would need to reach mass consumption levels to gain credibility and would need to be continually monitored for diversity in the user base to gain credibility and minimize bias.

Partnerships with mainstream social media platforms, advertising agencies and regulators will be crucial for digital content credentials requirements to become an industry standard; partnerships should also be used to increase education for consumers and producers of content.

AI-powered fact-checking capabilities for users should include abilities to fact-check video content and identify fabricated user engagement coming from synthetic botnets.

# Extend biometric authentication requirements for systemically influential individuals' social media

## Opportunity overview

**Biometric authentication requirements** (e.g. face authentication with liveness assurance checks) should be extended for social media accounts that belong to systemically influential entities (e.g. bank CEOs, governors of central banks, high-profile investors) and influential individuals with high followership volumes to curb the negative second-order effects that can reach financial markets.

## How it could work



Governments set **shared standards** on **what constitutes a systemically important social media account** (e.g. followership volume, government officials, relevance to market movements).

**Capital market providers** share market datasets and correlation metrics to support the development of standards.



Social media platforms **pull facial recognition, fingerprint or voice data for systemically influential entities and their designated social media managers** as part of their onboarding process and security settings for verified accounts that meet government standards. They can also verify if the post is outside of the normal pattern and tone of past posts by the systemically influential individual.



Systemically influential entities or their associated social media managers **perform additional biometric checks before every content upload.**

## Conditions necessary for success

Data privacy mandates in place for biometric authentication data received by social media

Input from capital market makers, social media platforms and fourth-party software-as-service providers on government standards that define systemically influential entities

Social media content posts should be verified and confirmed as not being produced by generative AI applications

## Relevant case studies



Baaz, a social media platform in the Middle East, has partnered with IDMission to enable an end-to-end encrypted identity process that authenticates its users' identities through passive liveness, biometrics and industry-compliant security practices.<sup>14</sup>

## Potential for contagion to spread into traditional markets if crypto-asset ecosystems collapse

Should levels of retail and institutional investment in crypto rebound and outpace the effects of regulatory action, current lending and custody processes used in crypto-asset ecosystems may spread contagion into traditional markets should cryptocurrency exchanges fail.

### Background

Institutional cryptocurrency investments dropped by 95% in 2022 in response to the latest string of cryptocurrency exchange bankruptcies.<sup>15</sup> While the crypto market has remained largely isolated from traditional markets due to relatively low institutional exposure, the structural barriers that protect traditional markets from crypto contagion remain permeable.

Amid growing anticipation for regulatory action, institutional investor interest is beginning to resurface.<sup>16</sup> As established regulatory regimes formalize protection measures for crypto assets, retail and institutional investors may regain new levels of confidence and acceptance in cryptocurrencies as a long-term store of value.<sup>17</sup> In response to growing demand, investment firms can reaccelerate the channels available for investors to gain direct exposure to crypto-assets (e.g. through partnerships with cryptocurrency exchange platforms, bitcoin-backed loan offerings or cryptocurrency options for pension funds).

If the speed of renewed institutional and retail demand for crypto exposure outpaces the effects of enforcement and monitoring action from crypto regulators, traditional financial institutions may become vulnerable to the risk vectors from cryptocurrency exchanges' lenient lending models and complex investment products available to unsophisticated clients.

### Emerging risks

- **Unchecked use of consumer funds:** Unlike conventional stock exchanges that generate revenue exclusively from trading fees, many cryptocurrency exchanges also preserve client funds, provide counterparty services, and lend and borrow money outside regulatory oversight. Their multi-faceted role can create conflicts of interest when providing their investors with the best execution obligation (e.g. exchanges may face off one of its investors for a trade) and when borrowing funds (e.g. exchanges using their tokens as collateral for loans and incentivizing their customers to purchase their tokens to increase its value).<sup>18</sup>
- **Unrestricted access to leverage:** Many crypto-asset exchanges have allowed unsophisticated retail investors unrestricted access to significant amounts of leverage (up to 125 times) to purchase crypto-assets, often without sufficient disclosure and understanding of the associated financial risks.<sup>19</sup> Permitting overleveraged trades with limited restrictions heightens the insolvency risk for a cryptocurrency exchange.

## Risk vectors



**Democratized access to highly-leveraged trades can threaten the liquidity of exchange operations**



**Limited transparency on leveraged trading volume and capital reserve data can make investor deposits vulnerable to loss**



**Pseudonymous design of the underlying blockchain technology can make credit-worthiness assessments challenging**



**Custody, lending and borrowing offerings can create conflicting incentives for an exchange when facilitating trades**

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

A large cryptocurrency exchange has a growing user base of traditional investors who make multiple levered bets on crypto assets. The exchange is not yet required to disclose daily capital reserve data or customer protection practices. During a period of intense leveraged trading activity, the cryptocurrency exchange cannot meet customer withdrawal requests and puts a freeze on future requests. In response, other investors begin withdrawing funds from other cryptocurrency exchanges in a panic, contributing to a sharp drop in cryptocurrency values.



#### Balance sheet write-offs for large asset managers

Asset managers that have developed cryptocurrency products (e.g. private trusts, crypto-backed loans) and have balance sheet exposure may need to write off values in their balance sheet, which can affect their solvency ratios.

#### Swings in institutional investor portfolios

Institutional investors will unwind funds invested in traditional markets to repay debt and cover their cryptocurrency losses, resulting in sharp swings in traditional markets.

#### Growing credit risk for banks

Investors that lose a significant volume of cryptocurrency value from an insolvent exchange (e.g. life savings, frozen pension funds) may face insolvency, which can threaten their ability to repay bank loans.

### Forces that can amplify and accelerate the risk



#### High fragmentation and inconsistency in crypto-asset regulation



Regions with inconsistent regulations placed on cryptocurrency exchanges increase the risk of redirecting high-risk, low-transparency trades into fewer communities and increasing the concentration of trading risk into fewer economies.



#### Growing adoption of decentralized cryptocurrency exchanges

Decentralized exchanges, which coordinate crypto-asset trading by using automated algorithms and operate outside regulatory perimeters, are beginning to gain market share over centralized exchanges that have recently enforced new crypto regulations and reporting requirements.<sup>20</sup>



 Regional Force  Entity Force



#### Interconnectedness of decentralized finance applications

Because lending collateral can be recycled and reused between different DeFi protocols, insolvencies in one token can lead to rapid second-order impacts on other liquid staking protocols (e.g. terraUSD with Lido, and MIM stablecoin).<sup>21</sup>



## Target mitigation outcomes and opportunity landscape


Mitigation efforts to minimize the contagion from cryptocurrency exchange activities must increase the transparency of exchange solvency for investors and control access to leveraged trading for creditworthy exchanges and investors.

### Target mitigation outcomes

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Protection of investor deposits**



**Controlled access to leveraged trading for investors**



**Transparency on indicators of exchange solvency**

### Mitigation opportunity landscape

- |  |   |  |
|--|---|--|
| <ul style="list-style-type: none"> <li><span style="color: blue;">●</span> Impose usage restrictions on customer deposits held in exchange custody</li> <li><span style="color: blue;">●</span> Establish shared reserve pools across the industry to address isolated liquidity challenges</li> </ul> | <ul style="list-style-type: none"> <li><span style="color: blue;">●</span> Design on-chain credit scores based on publicly available blockchain transaction data</li> <li><span style="color: green;">●</span> Enhance know your customer (KYC) measures for exchanges that verify proof of funds via Open API platforms</li> </ul> | <ul style="list-style-type: none"> <li><span style="color: blue;">●</span> Mandate Proof of Reserve certificates from third-party auditors</li> <li><span style="color: green;">●</span> Mandate real-time Proof of Solvency disclosures using zero-knowledge-proof protocols</li> </ul> |
|--|---|--|

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*



## Current mitigation efforts growing in adoption

With the significant collapse in multiple leading cryptocurrency exchange platforms, the focus of mitigation efforts has been on protecting investor deposits and identifying creditworthiness, while some opportunities to maximize exchange transparency remain untapped.

		Government-initiated	Sector-initiated
<p><b>Impose usage restrictions on customer deposits held in exchange custody</b></p> <p>Securities regulators in regions like Canada and New York have prohibited registered cryptocurrency trading platforms from using customer deposits to fund risky proprietary trading strategies or offering high-leverage derivatives in order to disincentivize risky decision-making.<sup>22</sup></p>	<p><b>Establish shared reserve pools to address isolated liquidity challenges for good actors</b></p> <p>Industry leaders like Binance are driving efforts to design an industry recovery fund to help financially healthy exchanges that face a liquidity squeeze during market distress and investor confidence crises.<sup>23</sup></p>	<p><b>Design on-chain credit scores based on publicly available blockchain transaction data</b></p> <p>DeFi applications like Spectral, Polygon and Amplify use publicly available blockchain transaction data by connecting crypto wallets<sup>24</sup> and zero-knowledge identity methods to assess creditworthiness while maintaining user privacy.<sup>25</sup></p>	<p><b>Mandate Proof of Reserve certificates from third-party auditors</b></p> <p>After the meltdown of the cryptocurrency exchange FTX in November 2022, many exchanges are now beginning to implement Proof of Reserve certificates that can be securely verified using cryptographic methods and attested to by third-party auditors.<sup>26</sup></p>

### Considerations to strengthen existing mitigation efforts

Since many investors trade on unregistered platforms operating in jurisdictions with little to no regulation, more funding should be dedicated to educating investors and discouraging advertising on unregistered platforms.

Regulatory bodies should contribute towards defining the criteria with which cryptocurrency exchanges are deemed eligible for recovery funds during market crises.

On-chain credit scoring protocols should also connect to off-chain credit history (via oracles like Chainlink) to recognize creditworthiness and offer higher yields for new crypto-asset investors with no on-chain credit score.

Proof of Reserve certificates should extend to showcase an exchange's liabilities in real-time to identify solvency issues more efficiently.

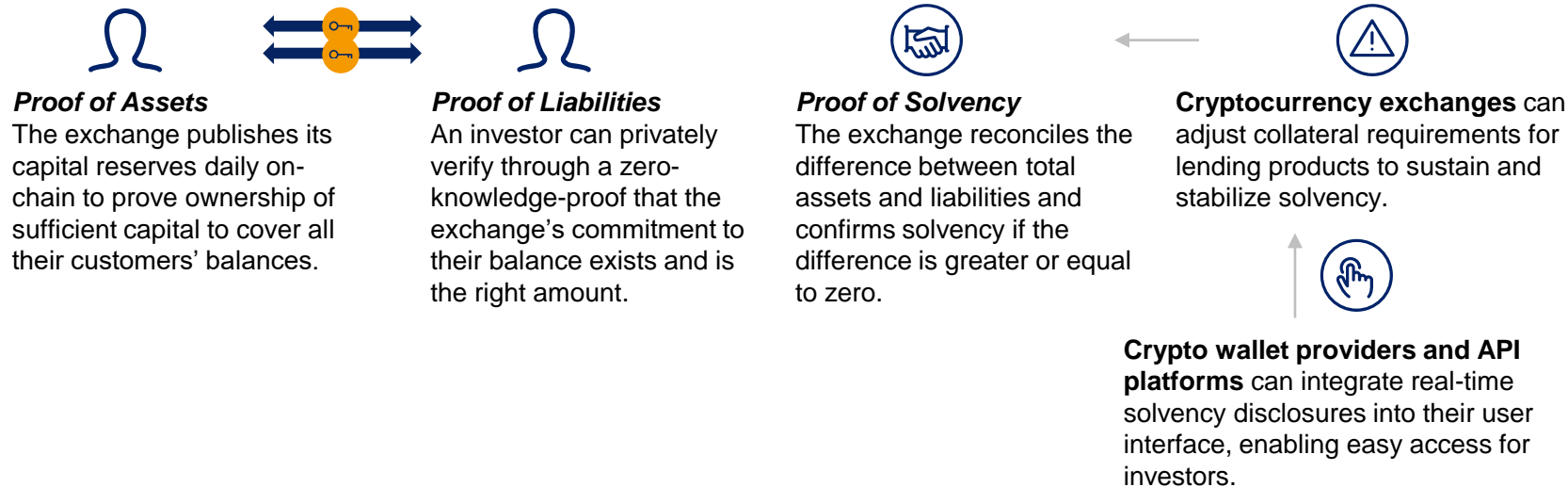
# Mandate real-time Proof of Solvency disclosures using zero-knowledge-proof protocols

## Opportunity overview

The accuracy and transparency of cryptocurrency exchanges' solvency can be maximized through an on-chain, real-time reporting mechanism. This solution can help ensure real-time solvency data is considered in downstream lending products offered by an exchange and can be made accessible to retail and institutional investors. Real-time Proof of Solvency disclosures are less costly than certificates that require third-party audits and can better sustain continuous investor trust in exchange operations.

## How it could work

Proof of Solvency can be designed through the execution of DeFi protocols using zero-knowledge proofs, which verifies an exchange's liabilities while protecting customers' balance data and privacy.<sup>27</sup>



## Conditions necessary for success

Guidance from governments or self-governing bodies on the minimum cadence and degree of solvency required to be disclosed by an exchange

Standardized interoperability design for infrastructure providers and API platforms that integrate cryptocurrency wallets to exchange data (e.g. Zabo, Plaid)

## Relevant case studies



THORChain is a decentralized liquidity network that prioritizes the security of locked assets, and those exchanged on the network. It uses security-enhancing mechanisms like bug bounty rewards and proactive on-chain solvency verification to build trust with users and community members in the network.<sup>28</sup>



CACHE Gold, a DeFi protocol that supports tokenized gold assets, has integrated with Chainlink's Proof of Reserve protocol to enable continuous verification and transparency of the true status of the gold reserves that back their tokens.<sup>29</sup>

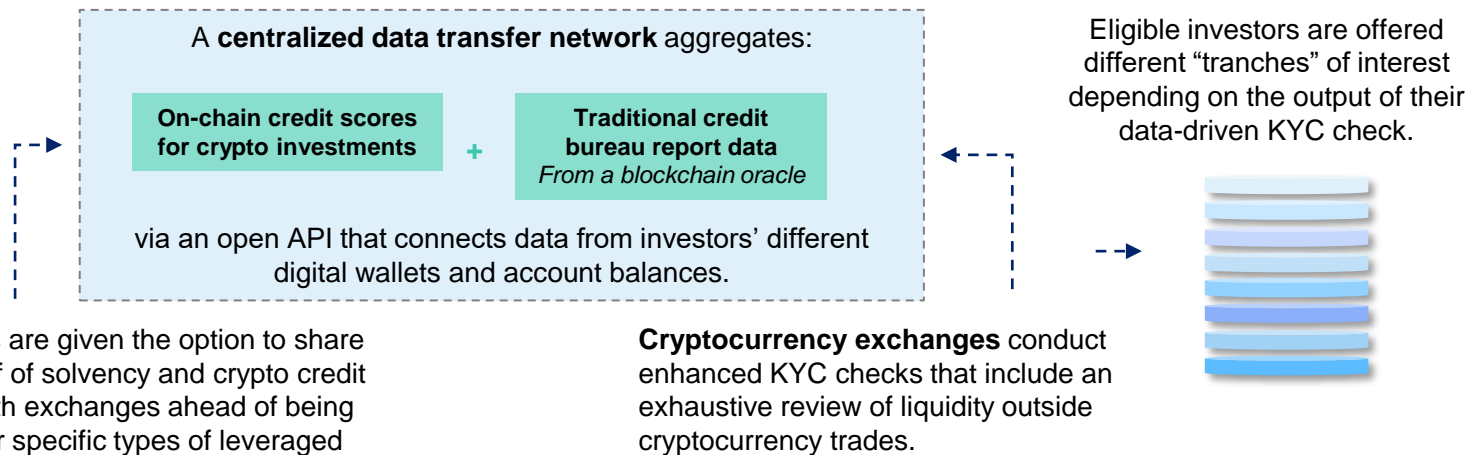
# Enhance KYC measures for exchanges that verify Proof of Funds via open API platforms

## Opportunity overview

Investors should be given the opportunity to share their proof of capital and reserves (including fiat currencies) as part of an enhanced KYC process to gain access to leveraged trades for lower interest in a cryptocurrency exchange. Access to a combination of on-chain credit scores with credit report data outside of cryptocurrency investments can help exchanges better price their interest rates according to risk and offer different tranches of interest based on their investors' creditworthiness.<sup>30</sup>

## How it could work

Today, KYC measures embedded in cryptocurrency exchanges are aimed at preventing illegal activities such as money laundering, terrorist financing and tax evasion.<sup>31</sup>



## Relevant case studies



Plaid offers cryptocurrency exchange support by aggregating a customer's cryptocurrency accounts through an API, giving investors a comprehensive view of their finances. It helps them share crypto account information, asset types, balances and transactions for other services.<sup>32</sup>

## Conditions necessary for success

Interoperability between open API layers and multiple cryptocurrency exchanges to maximize consistency

Mandates from government authorities on capital thresholds required for leveraged cryptocurrency trades



---

# Investment management

## Market volatility from speculation fueled by social media

With retail investor activity reaching record highs and speculation on social media platforms continuing to proliferate, the market volatility introduced by strategies like meme-stock investing could grow to have systemic implications.

### Background

With retail investor activity and meme-stock speculation having reached unprecedented levels in 2022, the influence of both trends on financial markets continues to widen.<sup>33</sup> While the rise of commission-free trading platforms has lowered the barriers for individuals to participate in direct investing, this rise has also resulted in the growth of “meme stocks”, where asset prices are highly disconnected from the underlying value of a company and are often driven by speculation on social media.<sup>34</sup> This dislocation has raised concerns among regulators, leading them to actively investigate the impact of digital engagement practices on market structure conditions.<sup>35</sup>

While social media-driven market effects are not limited to meme-stock activity, their influence is well observed in this space. For example, algorithmically-driven social media platforms (Reddit, Twitter) are pivotal in amplifying stock volatility and heightening individual risk appetites by creating “echo chambers” for investors to frequently communicate with others with similar interests and views, potentially reinforcing speculative investment decisions.<sup>36</sup>

### Emerging risks

- **Meme-stock strategies are now being extended to short-term options positions** where investors place bets on prices with unlimited downside risk.<sup>37</sup> In the third quarter of 2022, S&P 500 options expiring within one day accounted for more than 40% of the total trading volume. Meme-stock episodes may also threaten sectors that depend on consumer trust (e.g. banking) if their upward trajectory continues. In October 2022, a social media post shared with more than 300,000 followers and reshared more than 3,000 times questioned the solvency of Credit Suisse and led to widespread rumours about its bankruptcy across markets. The firestorm resulted in retail investors participating in short trades with no-cap downside, with the bank’s shares plunging nearly 6%, shaving about \$600 million off its market capitalization.<sup>38</sup>
- **The increase in many retail investors’ risk appetites may not be sufficiently calibrated within investment firms’ risk models** to reflect the volatility and market loss that meme-stock episodes may trigger.<sup>39</sup> If meme stock activity continues along this trajectory, well-capitalized institutional investors with well-researched positions may be forced to unwind and liquidate their positions earlier, creating a significant multiplier on the overall market disorder.

## Risk vectors



The democratization of trading complex investment products through online trading platforms can multiply the effects of speculative trading by unsophisticated investors



Social media platforms being recognized as a trusted source of market data by retail investors can create echo chambers that reinforce speculation and bias



Minimally available leading indicators of meme-stock episodes make it difficult for investment firms to update their risk models and for retail investors to make informed investment decisions

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

False rumours about undervalued stocks are shared on social media and spark multiple activist online campaigns on alternative media, leading to herd buying behaviour across retail investors. The resulting meme-stock herd buying behaviour may trigger the following second-order impact:





#### Liquidation of institutional investor portfolios

Large investment firms that underwrite the put/call options that retail investors buy begin liquidating their holdings and cutting short their losses in response to volatile and sudden changes in portfolio value (from long or short positions), creating a second-order effect on market destabilization.

#### Retail investor solvency leads to credit risk for banks

Retail investors that have purchased short-term options and invested on margin against meme-stocks may face a liquidity crunch as markets restabilize, threatening their ability to pay back their liabilities with other lenders in the financial ecosystem.

### Forces that can amplify and accelerate the sector-specific risk

 Regional Force  Entity Force



#### Online trading platforms gamifying trading and encouraging risky trading behaviour

Online trading platform features are designed to maximize user enjoyment, which may be directly correlated with risky trading behaviour.<sup>40</sup> Platforms also redirect investors to high-attention stocks with little access to formal financial advice available for unsophisticated investors.<sup>41</sup>



#### Social media penetration rates across communities

Regions with younger populations and unrestricted access to social media channels (e.g. Brazil, South Africa, Philippines<sup>42</sup>) may be at the most risk of participating in meme-stock trades due to social media-driven speculation.



#### Investors “reverse engineering” meme-stock campaigns

Investors with controlling interest in public companies may be incentivized to spark activist campaigns on social media platforms to boost a company’s stock price as a path to satisfying shareholders instead of increasing the financial viability of a company.<sup>43</sup>



## Target mitigation outcomes and opportunity landscape

Mitigation efforts to protect against the market instabilities introduced by intense speculation should focus on deterrence from participating in speculative trades and the ability for institutional investors to detect meme-stocks proactively

### Target mitigation outcomes

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Deterrence from participating in speculative trades**



**Greater transparency for *institutional investors* on leading meme-stock indicators**

### Mitigation opportunity landscape

- Embed financial literacy programmes within online trading platforms.
- Increase retail shareholder engagement through social media.
- Launch an automated adviser model in online trading platforms for proactive investment recommendations.
- Set up exchange-traded funds (ETFs) and indexes that help investors track emerging meme stocks.
- Use machine learning algorithms to spot warning signs of a meme-stock surge.
- Embed real-time alternative data feeds into institutional investors' risk models.

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*

## Current mitigation efforts growing in adoption

While efforts to identify retail activity through social media tracking, and educate retail investors on stock fundamentals, are growing, new opportunities exist for institutions to proactively support healthy risk-taking behaviours and develop forward-looking indicators to embed in investment risk models.

		Government-initiated	Sector-initiated
<p><b>Embed financial literacy programmes within online trading platforms</b></p> <p>Trading platforms like Robinhood have launched in-app educational experiences (Robinhood Learn) that make financial lessons accessible to all customers across topics like stock trading, options trading, EFTs, initial public offerings and cryptocurrencies.<sup>44</sup></p>	<p><b>Increase retail shareholder engagement through social media</b></p> <p>Firms like RCI Hospitality Holdings have hosted their earnings calls on social media platforms (e.g. Twitter Spaces) to make financial fundamentals more accessible to younger retail investors and to increase their shareholder engagement beyond equity research analysts and fund managers.<sup>45</sup></p>	<p><b>Set up ETFs and indexes that help investors track emerging meme stocks</b></p> <p>Roundhill Investments has launched an ETF that tracks the performance of stocks exhibiting a combination of elevated social media activity and high short interest through data from third-party data providers.<sup>46</sup> Robinhood has also launched an index tracking the performance of stocks most traded by its users.<sup>47</sup></p>	<p><b>Use machine learning algorithms to spot warning signs of meme-stock surge</b></p> <p>Post 2021, many hedge fund managers across North America and Asia regularly use algorithms to scour forums such as r/WallStreetBets or other data sources to spot coordinated buying behaviours. Fintechs are also providing “short squeeze risk” scores to Bloomberg terminal users and selling social media data to fund managers.<sup>48</sup></p>

### Considerations to strengthen existing mitigation efforts

Online trading platforms can consider embedding financial literacy assessments for retail investors as part of onboarding for online trading platforms to tailor their recommendations for investment products.

Attendance and shareholder engagement data from company sessions on social media can serve as valuable input for algorithms to detect early retail investor interest and identify leading meme-stock indicators sooner.

Rebalancing ETFs more frequently (e.g. hourly instead of biweekly) and reducing their market capitalization requirements can increase the likelihood for investors to track the early indicators of meme-stock behaviour.<sup>49</sup>

Data inputs for model algorithms can be in real-time, sourced from third-party data providers to help proactively identify and monitor heightened risk exposure for institutional investors’ existing holdings.

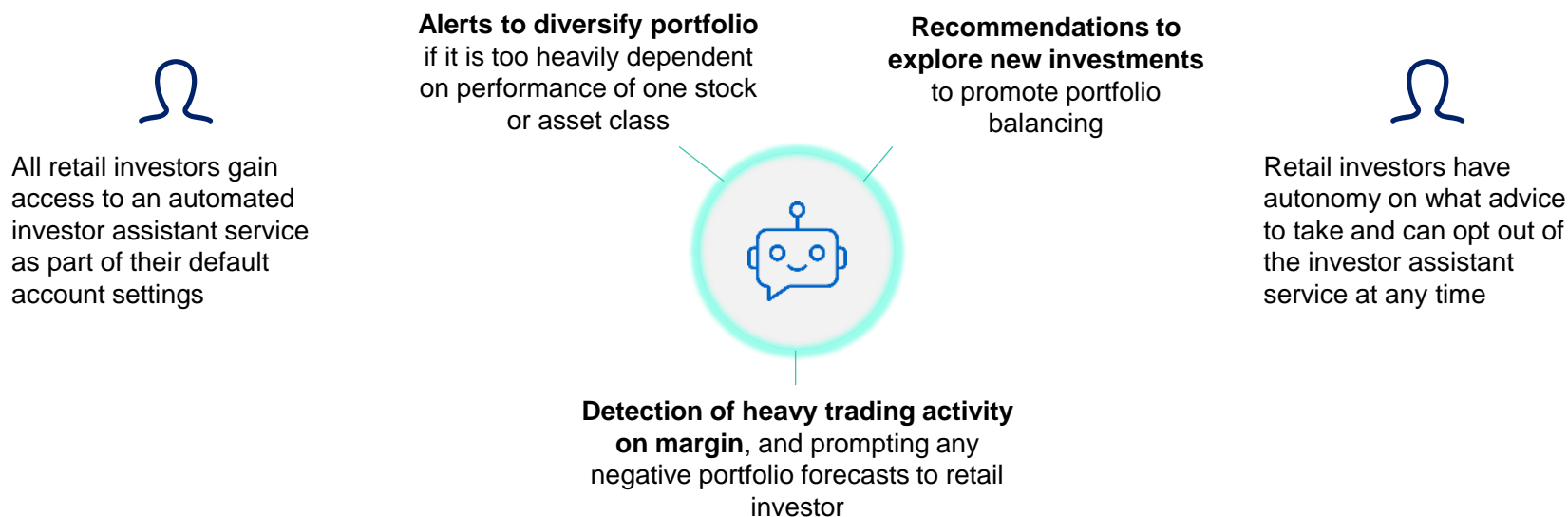


# Launch an automated adviser model in online trading platforms for proactive investment recommendations

## Opportunity overview

The articles, guides and help forums offered by commission-free trading platforms are generally insufficient at proactively managing and identifying risky retail investor activity. To encourage real-time support for retail investors, trading platforms' existing digital engagement prompts can be rebranded to educate investors on making trading decisions that encourage healthy risk-taking behaviour. Platforms can embed investment portfolio software intelligence algorithms within commission-free trading platforms to proactively monitor, identify and offer guidance to investors making trades based on their trading activity, purchasing power and portfolio make-up.

## How it could work



## Conditions necessary for success

To ensure consistency across platforms and prevent risky trading activity from being redirected, regulatory mandates should be placed on the minimum set of activities for all licensed online trading platforms to monitor.

Data sharing permissions by retail investors to share their investment data anonymously and service the models that enable the smart assistant service.

## Relevant case studies



Belgian bank KBC's digital robotized investment assistant "Matti" offers automatic monitoring of clients' investment portfolios. The smart assistant is available for KBC and Bolero clients and non-customers with a minimum of €1,000 investment. Based on the profile and preferences of an investor, Matti proposes a portfolio and continuously monitors the investor's portfolio. It is up to the investor whether or not to follow Matti's advice.<sup>50</sup>

# Embed real-time data feeds about retail investor activity into institutional investors' risk models

## Opportunity overview

In order to proactively understand the evolving risk appetite of retail investor communities and new risk variables introduced, investment firm risk models should rely more heavily on forward-looking sources of data and real-time data feeds to aid in trade decisions and portfolio rebalancing instead of using historic time series data and batch processing methods.

By supplementing real-time social media mentions and short squeeze activity data with additional forward-looking indicators and rate of change statistics, institutional investors can better track the value of a company as perceived by retail investors and understand what existing sentiment data translates to impact on financial markets.

## Relevant case studies



Hedge funds like Anson Funds are quantifying the risk that comes from retail activity by analysing retail trading activity as a percentage of daily trade volume and gathering evidence of divergence on platforms like Twitter, which signal when investor comments are shifting from positive to negative or vice versa.<sup>53</sup>

## How it could work

### Real-time data pipelines sourced from third-party providers:

- Social media ticker mentions
- Short-squeeze risk scores
- Retail investor attendance to earnings calls
- Investor Index data from online trading platforms (e.g. Robinhood's Investor Index showcases the top stocks owned by users, weighted by the percentage of portfolio)
- Percentage of trade volume for a stock that comes from retail

### Real-time data pipelines<sup>51</sup>

Real-time data pipelines that operationalize data into model algorithms and model outputs instantaneously can help investment managers identify the rate of change in leading indicators for meme-stock behaviour.

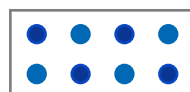


### Batch data pipelines<sup>52</sup>

Batch datasets on company performance, index performance, daily social media mentions

Datasets enter model framework for "batch prediction" at specific time intervals

Recommendations on portfolio balancing to maintain risk tolerance provided in batches



## Conditions necessary for success

Real-time data pipelines that come from trusted data sources from third-party data providers

Thresholds in place within risk models for investment managers to contextualize real-time data feeds and identify when portfolio holdings need to be rebalanced to maintain risk profile

## Investor manipulation from compromised sensor-generated data

As real-time sensor-generated data becomes a mainstream approach for investment firms to improve portfolio alpha, the attack surface for malicious actors to compromise and manipulate market data for financial and political gain is rapidly widening and introducing new opportunities to destabilize markets.

### Background

Two-thirds of hedge funds currently rely on alternative data platforms (most accessible via APIs<sup>54</sup>) to a significant or moderate degree to inform their investment decisions, identify market inefficiencies and predict future market moves.<sup>55</sup> The large-scale use of real-time sensor data in commodity industries (e.g. agriculture, energy, metals, etc.) specifically has led to greater confidence from traders in their investment decisions within commodity markets.<sup>56</sup>

With more than 50% of the global datasphere expected to be generated from sensors by 2025,<sup>57</sup> sensor-generated data from satellites, CCTV footage, smartphones, and consumer and industrial internet of things (IoT) devices will make up a greater share of the datasets that investment firms will rely on to inform their decisions.

### Emerging risks

- **Deploying IoT botnets and tampering with sensor data feeds are becoming low-cost, high-reward methods for cybercriminals to disrupt commodity markets for economic and political gain.** Attack variants like the Manipulation of Demand via IoT (MaDIoT) are becoming financially accessible methods for malicious actors to deploy high-energy consuming botnets to manipulate the total demand of energy to influence global prices in favour of specific market players.<sup>58</sup> Research suggests deploying as few as 50,000 botnets (e.g. infected thermostats, air conditioners, etc.) can successfully impact a region's power grid and influence market prices, creating economic havoc in a region.<sup>59</sup>
- **A growing black market for fake or corrupted sensor data may increase the likelihood and damage of False Data Injection attacks,** which compromise measurements from IoT sensors by small margins such that the manipulated sensor measurements bypass the sensor's basic 'faulty data' detection mechanism.<sup>60</sup> Gartner has forecasted a black market dedicated to selling fake sensor and video data for enabling criminal activity as large as \$5 billion,<sup>61</sup> making IoT attacks on financial markets more lucrative and accessible.

## Risk vectors



Open-source channels help cybercriminals share malware source code quickly and accelerate the rate of new types of IoT attacks



High-speed 5G network infrastructure helps investment managers gain instant access to real-time sensor data feeds



The wide attack surface from managing multiple IoT end points makes comprehensive security oversight challenging<sup>62</sup>



Interconnectedness embedded in sensor architecture makes devices vulnerable if one device is compromised

# Systemic risk scenario and amplifying forces

## Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

If multiple investment firms depend on a shared set of sensor devices that is compromised for a global commodity (either through manipulated or falsified data), misinformed trading decisions can be made across investment firms and hedge funds with the following second-order impact:




### A reinforcing cycle of instability within capital markets

Conflicting information between industry participants and sensor datasets leads to scepticism of the general market intelligence data provider industry, seeding further instability in capital markets and resulting in a withdrawal of capital across multiple commodity businesses due to a lack of trust.

### Investor liquidity challenges

Altered investor sentiment and liquidity challenges as a result of flash-crash events may trigger panic sell-offs from institutional investors and drain the market from significant volumes of funds.

## Forces that can amplify and accelerate the risk

 Regional force  Entity force



### Regions democratizing 5G connectivity between devices

Regions enabling service providers to use non-proprietary components from multiple vendors to connect devices to 5G networks will become more vulnerable to the interoperability risks and security gaps that may come from a more diverse and complex vendor landscape.<sup>63</sup>



### Consolidation and merger trends within the sensing industry

The sensing industry has seen a wave of consolidation between device vendors in 2022,<sup>64</sup> which will reduce the number of vendors that investment firms depend on for devices and can heighten the future collective impact of compromised sensor devices on markets.



### Unregulated data broker industry

There is limited transparency today on the permissions, usage restrictions and data sources for alternative datasets sold to investment firms by the largely unregulated data broker industry. Unregulated data brokers may play a role in contributing to the growth of a black market for fake data sold to cybercriminals.




## Target mitigation outcomes and opportunity landscape


Mitigation efforts against compromised sensor-generated data should focus on increasing data quality sourced from sensors, slowing the spread of malware across a network, and proactively identifying false data injection attacks.

### Target mitigation outcomes

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Increasing data quality sourced from sensors**



**Containing malware contagion across a sensor network**



**Detecting and monitoring false data injection attacks**

### Mitigation opportunity landscape

- Establish global certification and labelling programmes for connected devices.
- Mandate due diligence processes for alternative data vendors.
- Protect sensor data through Entropy-as-a-Service.
- Employ extended detection and response techniques that integrate data across devices.
- Decentralize data due-diligence processes through continuous identification of authenticated devices.

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*

## Current mitigation efforts that are growing in adoption

While mitigation efforts to boost consumer confidence in connected devices are gaining traction, unrealized opportunities remain for investors to trust the devices and the resulting data they receive to make trading decisions.

		Government-initiated	Sector-initiated
<b>Establish global certification and labelling programmes for connected devices</b>	<b>Mandate due diligence processes for alternative data vendors</b>	<b>Protect sensor data through Entropy-as-a-Service</b>	<b>Employ extended detection and response (XDR) techniques that integrate data across devices</b>
Governments in Singapore, Germany and the US have championed government-backed labels that help customers easily recognize, which devices meet the highest security and privacy practices (e.g. default passwords, security updates, functionality when offline). <sup>65</sup>	After recent violations have been placed for analytics firms misusing alternative datasets that are sold to investment firms (e.g. App Annie), the US government is beginning to scrutinize an investment firm’s use of alternative data in the investment decision-making process. <sup>66</sup>	The National Institute of Standards and Technology (NIST) in the US has recommended creating new sources of “entropy” to better secure the data that is held and transferred from sensor devices (e.g. random number generation used for encryption and decryption). Fintechs like Quantropi use quantum computing power to supply businesses with additional encryption keys to protect against IoT attacks. <sup>67</sup>	Large technology companies like VMware are helping companies enhance their visibility into companies’ networks through technology that provides 360-degree visibility on suspicious activity and contextualizes seemingly unrelated attacks identified across different connected devices (XDR). <sup>68</sup>

### Considerations to strengthen existing mitigation efforts

Certifications should be mandated within asset managers’ data vendor due diligence processes and can be made dynamic in response to industry security updates.	Investment firms can use RegTech solutions for vendor management compliance to strengthen their due-diligence processes for alternative data vendors, stay compliant with government guidance and minimize overhead costs from due diligence efforts.	Data providers and companies generating data from sensors should publish their partnerships with entropy providers to establish trust with investment firms and third-party alternative data platforms.	Investment firms should consider the breadth of security capabilities and technologies sensor data providers have (e.g. XDR) when sourcing data for trading decisions.
--	---	---	--

# Decentralizing data due-diligence through continuous identification of authenticated devices

## Opportunity overview

Companies that generate data from sensors can use device identification frameworks (that use a combination of sensor profiling variables and machine learning algorithms) to proactively protect against false data or counterfeit devices deployed in a network to manipulate sensor data feeds. Continuous device identification can verify all IoT devices in a network, their data sources and variance in network traffic to ultimately prevent false data from being sent through maliciously deployed devices.<sup>69</sup>

By embedding these requirements as part of the vendor procurement process for alternative data sourcing, investment firms and alternative data platforms can decentralize due-diligence efforts for IoT devices and minimize the systemic impact of malicious sensor data tampering.

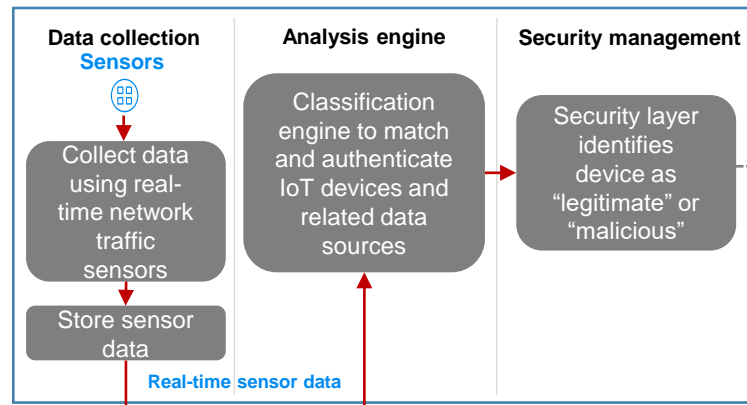
## Relevant case studies



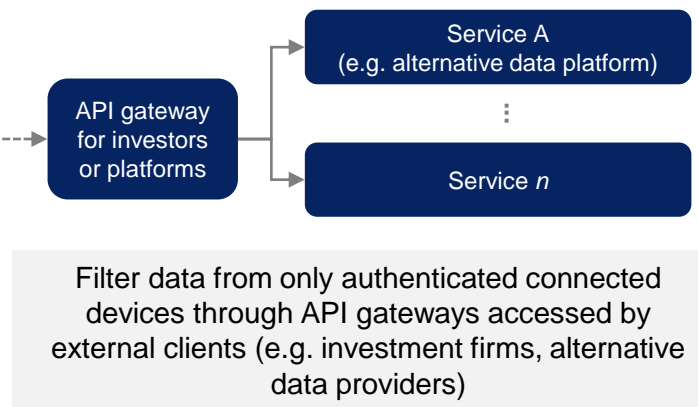
Portnox is a security startup that has launched the first cloud-native IoT fingerprinting and profiling solution, which is helping enterprise and mid-market businesses detect and authenticate all their IoT devices with 95% accuracy.<sup>71</sup>

## How it could work

Illustrative data flow of company producing data (e.g. construction company)<sup>70</sup>



How this can be extended



## Conditions necessary for success

Regulatory mandates for players across the value chain (sensor manufacturers, network controllers in enterprises) to declare security measures in place for device identification.

Interoperability of identification framework and data collection techniques across a majority of sensor vendor providers.



---

# Payments



## Accumulation and securitization of buy now pay later (BNPL) debt

Easy access to BNPL credit coupled with weak underwriting rules may lead to overborrowing and potentially spill over to the financial system through debt securitization.

### Background

Demand for BNPL products, a short-term credit option for consumers looking to pay for purchases in instalments, is on the rise. While BNPL is not a new concept, it has grown in popularity due to lenient credit approval processes and ease of access in e-commerce channels through partnerships between fintechs and retailers. In 2021 alone, BNPL payments hit over \$120 billion and are projected to grow by 24% over the next three years.<sup>72</sup> By 2025, 12% of global e-commerce spend is estimated to come from BNPL transactions.<sup>73</sup> BNPL provides easy credit with the convenience of interest-free instalment payments for consumers who may not qualify for a bank loan or who have overdrawn their savings or credit cards. For merchants, BNPL has been instrumental in boosting sales and acquiring new customers.

### Emerging risks

- **The nature of BNPL credit creates opportunity for overborrowing and the piling up of shadow debts.** BNPL loans appeal to consumers who may not be eligible for loans from traditional channels, have maxed out their credit limits or exhausted savings. Research shows that consumers are inclined to spend spontaneously and are three times more likely to complete their online purchases instead of abandoning them in the cart when presented with a BNPL financing option.<sup>74</sup> Millennials are notably high users of BNPL credits, with the volume of transactions by this age demographic increasing by more than 400% in the last couple of years.<sup>75</sup> According to Barclays, a quarter of BNPL users already feel unsure about their ability to settle their BNPL debt. Additionally, the Federal Reserve Bank report indicates that 18% of young consumers have already fallen behind on their repayments.<sup>76</sup>
- **BNPL default risk may also spill over to the broader financial system through securitization.** As a capital-raising strategy, BNPL providers package outstanding BNPL debt and sell it to investors as securitized assets. In a weak economic cycle, the ability of consumers to repay their loans may be impacted, potentially leading to large delinquencies. Similar to the mortgage-backed security crisis in 2008, if the scale of BNPL securities grows significantly, large-scale defaults may have a spiralling effect on the financial system. Research by S&P has indicated that the volume of securitized BNPL assets is on the rise in Europe,<sup>77</sup> with Fitch sounding the alarm on the credit risks associated with this product.<sup>78</sup>

## Risk vectors



**Weak credit controls create opportunities for impulse buying and easy accumulation of debt**



**Limited reporting requirements for BNPL debt limit the visibility of consumers' total debts**



**Securitization of BNPL debts could create contagion to the wider financial system**



**Conflicting incentives exist, between protecting customer interests and increasing sales which may accelerate debt accumulation levels**

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

If the volume of BNPL debt were to grow to significant levels and a large percentage were securitized as subprime borrower debt, a protracted economic recession event may impact consumers' ability to repay their loans synchronously, resulting in large delinquencies with the following second-order impacts:



#### Bank credit delinquencies

Bank loans given to customers who have accumulated BNPL debts may experience large delinquencies as their ability to repay existing debts diminishes. Banks could also tighten the requirements and willingness to lend credit to customers.



#### Investor losses

Firms that have invested in BNPL-backed assets may absorb large losses when securitized assets decline in value.

#### Decline of consumers' well-being

Consumers that have accumulated large and unsustainable levels of debt may struggle and experience financial distress.

### Forces that can amplify and accelerate the sector-specific risk

 Regional Force  Entity Force



#### Entrance of Big Techs into BNPL credit space

The new BNPL products that Big Tech players are embedding within their existing product ecosystems (e.g. Apple Pay Later, Amazon Pay Later) are rapidly widening the userbase that is exposed to short-term instalment credit.



#### Jurisdictions with regulatory guidelines not covering BNPL loans

The absence of regulatory guidelines in jurisdictions where BNPL finance is offered has created opportunities for arbitrage (exploiting regulatory loopholes across jurisdictions), resulting in lending practices that may be detrimental to consumers' financial well-being.



#### Low financial literacy rates

Consumers in jurisdictions with lower financial literacy rates and inadequate access to money management resources are more susceptible to impulse buying and likely to overborrow.<sup>79</sup>




## Target mitigation outcomes and opportunity landscape


Mitigation opportunities to address the risks from short-term instalment credit products like buy-now-pay-later must protect customers from overborrowing, improve transparency on customers' ability to pay and inform investors on the quality of securitized debt.

### Target mitigation outcomes

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Customer protection  
from overborrowing**



**Transparency on  
customers' ability to pay**



**Transparency on quality  
of securitized debt to  
protect investors**

### Mitigation opportunity landscape

- Design safeguards to protect against overborrowing and misleading advertising.
- Enhance data sharing between BNPL providers.
- Design a rating framework to evaluate and rate securitized BNPL debt portfolios.
- Develop a code of conduct for BNPL providers to support appropriate loan labelling.
- Include BNPL data in credit bureau reporting.
- Use open banking platforms to enhance affordability checks on customers.

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*

## Current mitigation efforts growing in adoption

While current mitigation efforts are focused on minimizing debt accumulation levels, unrealized opportunities remain to protect investors from securitized BNPL investments and enhance transparency for credit providers.

		Government-initiated	Sector-initiated
<p><b>Design safeguards to protect against overborrowing and misleading advertising</b></p> <p>Regulatory authorities across Europe and Oceania are designing safeguards (affordability checks, borrowing limits, fair promotional practices etc.) to protect consumers from overborrowing. Jurisdictions across Asia are also exploring rules prohibiting consumers with unsettled balances from further borrowing (e.g. Singapore).<sup>80</sup> The Financial Conduct Authority (FCA) will now sanction firms breaching financial promotion rules.<sup>81</sup></p>	<p><b>Enhance data sharing between BNPL providers</b></p> <p>Regulatory authorities like the Monetary Authority of Singapore (MAS) are beginning to encourage BNPL providers to exchange data of consumers, including those with past-due obligations, to check against loan stacking and enhance affordability checks.<sup>82</sup> BNPL providers are also using accessible alternative data to adjudicate credit applicants more thoroughly.<sup>83</sup></p>	<p><b>Develop a code of conduct for BNPL providers</b></p> <p>In Australia, BNPL providers are self-organizing to standardize lending practices and ensure minimum operating standards are adopted. The Australian Finance Industry Association (AFIA) published a set of commitments in March 2021 that members are required to comply with to protect consumer interests and ensure transparency.<sup>84</sup></p>	<p><b>Include BNPL data into credit bureau reporting</b></p> <p>To enhance affordability checks, some BNPL providers like Zilch and PayPal are running soft credit checks before loans are approved. Credit bureaus like Equifax, Transunion and Experian have also launched the inclusion of BNPL payment information as part of their credit reporting data requirements.<sup>85</sup></p>

### Considerations to strengthen existing mitigation efforts

Development of regulatory frameworks for BNPL products should include input from BNPL providers and other market participants to ensure buy-in and balancing of consumer and product owner interests.

To protect consumers' interests, data privacy should be prioritized so that data is shared between BNPL providers safely and securely. Due diligence on alternative data sources should also be done to ensure synthetic data from generative AI applications is not used to pass creditworthiness assessments.

Codes of conduct that are developed regionally should be assessed and compared with other regional associations to acknowledge any gaps or contradictions that may encourage arbitrage.

Credit bureau reporting models should consider increasing the frequency of BNPL reporting given the short-term instalment nature of BNPL loans.

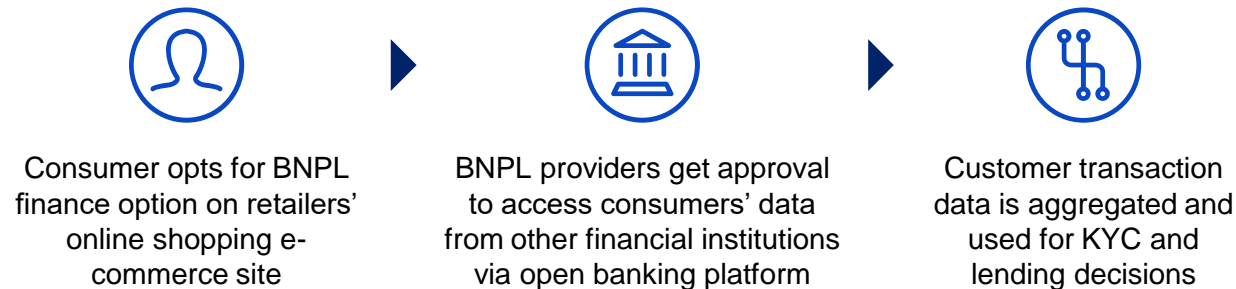
# Make use of open banking platforms to enhance affordability checks on customers

## Opportunity overview

Aggregating data from banks and other players within the open banking ecosystem can provide BNPL providers access to a comprehensive view of the customer's spending habits, which can subsequently feed into their lending decisions. Consumers already overextended with other lenders and at risk of overborrowing can be identified and precluded from new credits until outstanding balances are settled.

## How it could work

Using APIs, BNPL providers could connect with already existing open banking ecosystems to gain secure access to customer data held by other banks. Consumers who consent to their data being accessed and used in the underwriting process may be rewarded with rebates on service costs such as late fees and interest charges.

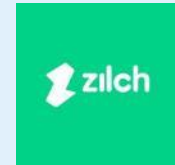


## Conditions necessary for success

Admission of BNPL entities into the open banking ecosystem.

Strong data privacy and security requirements for BNPL providers.

## Relevant case studies



Zilch, a BNPL provider headquartered in London, uses open banking in addition to soft credit checks to connect with consumers' bank accounts to get a real-time view of consumers' spending habits and to gauge affordability before approving BNPL loans.<sup>86</sup>

# Design a rating framework to evaluate and rate securitized BNPL debt portfolios

## Opportunity overview

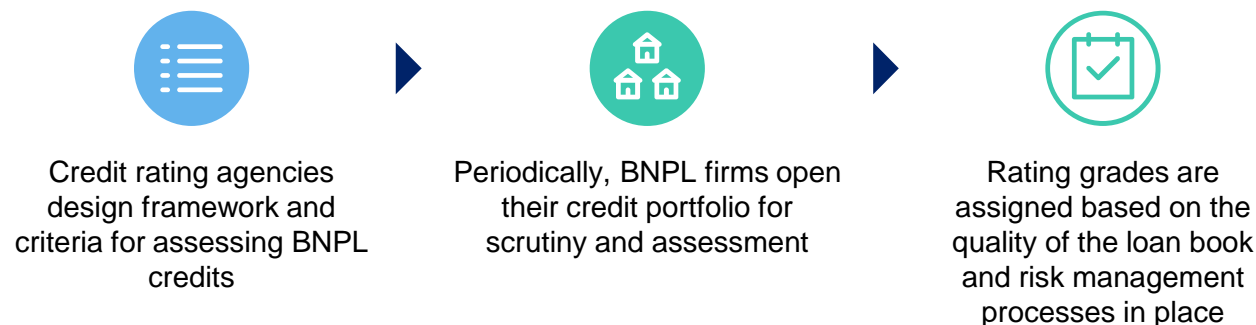
To better assess the quality of underlying debts for BNPL assets issued to investors, rating organizations like Fitch Ratings, Moody's Investors Service, and S&P could incorporate an assessment of BNPL securities as part of their ratings services. Similar to how banks are rated based on the quality of their credit portfolio, BNPL providers with sound credit underwriting processes and risk management in place can be assigned ratings to guide investors in pricing their credits. BNPL firms with positive ratings will be less likely to default and, therefore, more trusted by investors.

## Relevant case studies



Although rating agencies have not yet commenced rating BNPL credits, some are signalling interest in this space. S&P Global, for instance, has indicated that in addition to evaluating BNPL credits on a case-by-case basis, they would likely examine the extent to which BNPL providers rely on third-party services such as a trust account or back-up servicer (a firm that manages portfolio of assets or receivables when the primary servicer is unable to perform).<sup>87</sup>

## How it could work



## Conditions necessary for success

The rating criteria should be clear and transparent, so that investors can understand the basis for the ratings

Credit ratings should be objective and independent without external influence

Credit ratings should be consistent and comparable across different BNPL providers

## Security vulnerabilities of decentralized CBDC architecture

Due to their complexity and the involvement of multiple entities, CBDCs running on decentralized ledger technology widen the attack surface for malicious actors.

### Background

Central bank digital currency (CBDC) is a digital representation of fiat currencies issued and backed by a central bank authority. Central banks are exploring the use of CBDCs for wholesale (e.g. interbank settlement) and retail (e.g. cross-border payments) applications to improve payment efficiency, expand access to the financial system, and facilitate the execution of monetary policy.<sup>88</sup> There is a growing interest in CBDCs, with several central banks in different stages of exploration. As of January 2023, 119 countries are exploring CBDCs, with 11 countries at launch stage.<sup>89</sup>

Several design variants are being considered for CBDC implementation, including centralized, permissioned distributed ledger technology (DLT) and hybrid models. In a **centralized model**, a central authority, typically the central bank, maintains and controls a centralized ledger that records the transactions. In the **DLT model**, cryptographic methods are used to record data across a network with the participation of multiple entities (such as banks). The **hybrid model** combines elements of both the centralized and DLT models.

Several central banks are considering DLT for CBDC deployment as it offers cryptographic security, transparency, decentralization and lower intermediation cost.<sup>90</sup> The number of central banks that have conducted CBDC pilots using DLT network is growing, including the Monetary Authority of Singapore (MAS), the Bank of Thailand and the Bank of Japan (BOJ). While the security profile of the centralized model is known and comparable to existing payment systems, stakeholders should pay attention to the new risks that the DLT model might introduce due to its relative novelty and the evolving understanding of its security profile when deployed in large, global use cases.

### Emerging risks

- **Expanded attack surface:** The involvement of multiple parties within the CBDC network introduces additional endpoints that could be vulnerable to attacks. Even though the number of participants in a permissioned DLT network is restricted, a malicious actor could target participating institutions within the CBDC network to gain unauthorized access to the CBDC system by stealing or forging their credentials.<sup>91</sup>
- **Security risks from flaws in programming:** Programming flaws in the DLT network or the underlying smart contracts that support the programmability features of CBDCs might be exploited by malicious actors to perform unauthorized transactions or steal user data.

## Risk vectors



**Participation of multiple entities in the DLT network broadens the attack surface that hackers could exploit**



**Bugs or malfunction of the DLT platform that supports a CBDC could cripple the system**



**Side-channel attacks could be used to break into user wallets and steal consumer funds<sup>92</sup>**

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

A foreign nation-state launches a distributed denial-of-service (DDoS) cyberattack on the CBDC payment network of another country by targeting a security vulnerability of one of the participating institutions, causing outages of critical services. As a result, the payment system of the country is disrupted, making it difficult for individuals and businesses to conduct transactions and causing the following second-order impacts:



#### Disruption of global trade

Prolonged outage of the CBDC network may impede the settlement of payments for international trade transactions, making it difficult for businesses to meet their obligations.



#### Loss of confidence

The confidence of users in the safety and reliability of the CBDC system might be diminished leading to a decline in its usage and a shift towards privately issued digital currencies for international trade settlement.

#### Financial losses

Individual users might suffer financial losses while participating financial institutions might be liable to cover customer losses. Additionally, the reputation of the central bank and other participating banks could be negatively impacted.

### Forces that can amplify and accelerate the risk

 Regional force  Entity force



#### Complexity of the DLT architecture

The more complex the architecture design of the CBDC network, the harder it is to trace and resolve issues. For example, if the CBDC network uses multiple types of smart contracts with different programming languages, it may be difficult for developers to identify and fix vulnerabilities in a timely manner.



#### Interoperability with other networks

As the CBDC network becomes more interoperable with other networks (such as payment rails or the CBDC of another country), the more vulnerable it is to attacks from those networks. For example, if a CBDC network is connected to a less secure network, attackers can exploit the flaws to compromise the CBDC network.



#### Large number of participating institutions

As more institutions are connected to the CBDC network, the level of cyber vulnerabilities rises due to the increased number of entry points that might be exploited by malicious actors, necessitating the need for robust security protocols.





## Target mitigation outcomes and opportunity landscape

Central banks exploring the implementation of CBDCs using DLT as the underlying technology should prioritize protecting the security and privacy of end users and their data, implementing strong access controls and network security measures and collaborating with other countries to ensure that security protocols are standardized globally.

### Target mitigation outcomes



### Mitigation opportunity landscape

- Strengthen end-user digital wallet protection.
- Establish a tiered ledger system for the CBDC database.
- Design quantum-resistant algorithms for futureproofing CBDC systems.
- Manage the risks of DLT through blockchain sharding.
- Standardize CBDC security protocols.

*The following slides will summarize current mitigation efforts that are growing in adoption and provide thorough analysis of emerging mitigation opportunities for consideration*

## Current mitigation efforts growing in adoption

Efforts are being made to enhance the security of CBDC systems through digital wallet protection, a multi-layered defence strategy, the use of algorithms resistant to quantum computing and the implementation of standardized security protocols.

		Government-initiated	Sector-initiated
<p><b>Strengthen End-user digital wallet protection</b></p> <p>To protect customer funds and data, some CBDC issuers use biometric multi-factor authentication (MFA) to verify users. Several CBDC pilots, such as those in the Bahamas (Sand Dollar), Sweden (e-krona) and China (digital Yuan), have included a form of MFA in their CBDC design. Additionally, there is growing interest in using tamper-resistant hardware devices with offline capabilities for CBDC wallets to ensure secure and uninterrupted access during power and network outages.<sup>93</sup></p>	<p><b>Establish a tiered ledger system for CBDC database</b></p> <p>Some stakeholders are exploring a tiered CBDC ledger system, which restricts user access within the network based on the authorization level. For example, only the central bank and a select group of banks may be authorized for CBDC issuance and redemption on the top tier. Other financial institutions using CBDCs for transactions may be part of the second tier with more restricted access and capabilities. The general public, who may use CBDCs, could make up the third tier.<sup>94</sup></p>	<p><b>Design quantum-resistant algorithms for futureproofing CBDC systems</b></p> <p>Quantum computers, which have the potential to break common cryptographic algorithms, can be used to decrypt certain CBDC systems.<sup>95</sup> To futureproof CBDC systems from these attacks, quantum-resistant algorithms are being included in the design of CBDC systems.<sup>96</sup> NIST has selected a set of quantum resistant algorithms to become part of its post-quantum cryptographic standard.<sup>97</sup></p>	<p><b>Standardize CBDC security protocols</b></p> <p>The fragmented nature of CBDC implementation has created challenges in creating a unified global security design standard. Although some CBDC systems can use existing standards, such as FIPS-140<sup>98</sup> and Payment Card Industry Data Security Standard,<sup>99</sup> they are not exhaustive of all CBDC system architectures. As DLT and CBDCs evolve, it will be crucial to mobilize an international platform to set common security standards.<sup>100</sup></p>

### Considerations to strengthen existing mitigation efforts

Consumer education on securely using digital wallets should be prioritized before mass deployment. Given the novelty of the technology, consumers should be well informed about common security risks, such as phishing scams and malware attacks, that might be targeted at them.

Stringent risk management processes should be applied to participating financial institutions, central bank authorities or developers with administrative privileges to ensure the security and integrity of the CBDC system. This should be backed up by regular audits.

Quantum-resistant algorithms should be thoroughly reviewed and vetted by members of the international cryptographic community, such as the NIST, The International Association for Cryptologic Research (IACR) or the European Association for Cryptologic Research (EACR).

The interoperability of CBDC systems with other digital currency systems (e.g. RippleNet) and traditional payment systems (e.g. SWIFT, Target2, Fedwire) across regions should be a primary consideration to ensure uniformity of security standards.

# Manage the risks of DLT through blockchain sharding

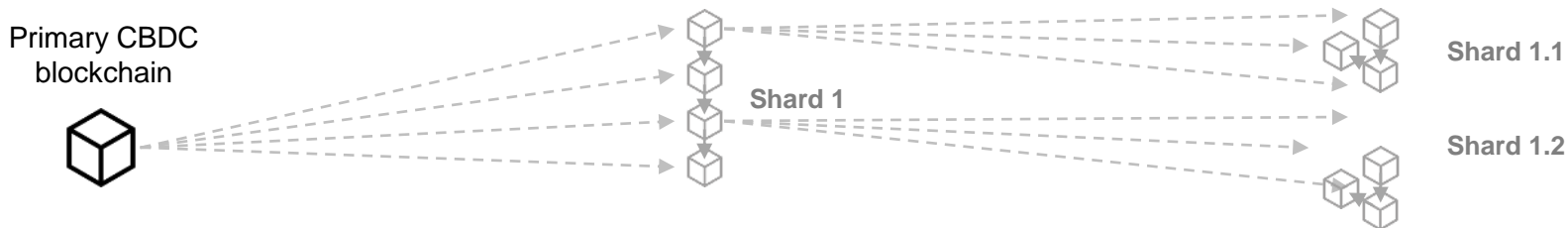
## Opportunity overview

The participation of multiple institutions in a DLT CBDC system expands the attack surface, which might make the network more susceptible to cyberattacks. To address this issue, blockchain sharding could be used to improve the security of the blockchain and enhance its scalability. Sharding is a technique that allows for a blockchain network to be divided into smaller sub-networks (known as shards), with each shard responsible for maintaining a portion of the overall ledger.

Access to certain shards is granted to participating financial institutions (nodes) without providing access to the whole network.<sup>101</sup> Distributing the network across multiple shards will minimize a single-point risk failure and make it more difficult for hackers to penetrate the entire system by targeting a particular location in the network. It will also enhance anonymity by enabling the disclosure of customer transactions to specific network participants on a need-to-know basis rather than the entire network.<sup>102</sup>

## How it could work

A CBDC blockchain is split into partitions (shards) of various transaction components with each participating entity (central bank, banks, validators, end users) only given access to relevant ledgers.



## Conditions necessary for success

Transparent governance system in place for each shard to manage decision-making and issue resolutions.

Strong authentication mechanism to forestall hijacking of the shards by hackers or bad actors within the network.

## Relevant case studies



ethereum 2.0

The Ethereum 2.0 upgrade plans to use sharding – partitioning the system into many sub-networks, or shards – to enhance the network’s scalability and security. Each shard will maintain a portion of the distributed ledger, allowing for parallel processing and scalability enhancements. The beacon chain, which was introduced in 2020, will support the maintenance of the shards to be launched in 2024.<sup>103</sup>



Zilliqa is a blockchain platform that uses sharding to solve problems with scaling and processing transactions. Sharding is used in the Zilliqa blockchain ecosystem as a scaling solution to improve speed and performance.



---

# Banking

## Risk exposure from BaaS offerings

While BaaS introduces innovation to the banking sector, the increasing reliance on API-enabled interconnectivity introduces vulnerabilities that can pose risks to banks.

### Background

BaaS enables non-banking entities (e.g. fintechs, neobanks) to provide some traditional banking services by connecting to the infrastructure of regulated banking institutions using APIs. They do so without becoming fully regulated and licensed financial institutions themselves. BaaS providers can be either traditional banks or fintech companies. For example, the Uber Pro card, branded as an Uber product to customers, is powered by Branch and issued by Evolve Bank & Trust. Similarly, Goldman Sachs has partnered with Stripe to allow businesses to seamlessly integrate financial services on their platforms.<sup>104</sup> Other financial institutions such as Wells Fargo, Starling bank and BBVA also have in-house BaaS platforms that enable businesses to offer financial products and services to their customers directly through their platforms. "As-a-service" business models have matured, enabling financial innovations that are now disaggregating several aspects of the banking value chain controlled mainly by traditional banks. It is projected that BaaS providers will reach \$11 billion in revenue over the next five years.<sup>105</sup>

The BaaS ecosystem involves multiple partners, which can limit the oversight capability of banks on the management of customer data and the security protocols of their partners, potentially exposing the banks to compliance and operational risks.

### Emerging risks

- **Data breach vulnerabilities:** Fintech players in the BaaS network handling customer data may have inadequate security measures compared to traditional financial institutions with strict data and privacy regulations, increasing the risk of data and privacy breaches for sensitive customer information.
- **Concentration risk of few BaaS providers:** Banks relying on few BaaS providers face the risk of contagion in case of a hack or prolonged outage affecting BaaS platforms used by multiple financial institutions.
- **Security risks from API connections:** Insecure API connections between banks and BaaS platforms may expose banks to security and data breaches as malicious actors attempt to access sensitive customer information or other critical infrastructure.

## Risk vectors



Customers' sensitive data and funds may be at risk from phishing and social engineering attacks



Flawed APIs might provide a back door entry for hackers to penetrate banks' systems



Non-compliance with data privacy rules by BaaS providers might expose partner banks to reputational risks

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

A malicious actor exploits an API vulnerability of a BaaS provider by launching a distributed denial-of-service (DDoS) attack. The attack overwhelms the system, making it unavailable for customers to access their accounts or perform transactions, resulting in the following second-order impacts:



#### Operational disruptions and financial losses

The affected bank may experience service disruptions requiring them to compensate customers. Additional costs might also be incurred to investigate and remediate the damage caused by the attack.



#### Market instability

Investors may lose confidence in the bank's security, causing its stock to decline. This could potentially trigger other stock sell-offs as investors become concerned about the overall security of the financial system if multiple banks are simultaneously affected.

#### Insurance premium cost

The bank will face a hike in cyber insurance premiums if it is found to have been negligent in protecting customer data, in addition to probable fines from regulatory authorities.

### Forces that can amplify and accelerate the risk

 Regional force  Entity force



#### Complexity of the BaaS stack

An attack on a bank's systems through an API might be more difficult to detect and react to in a timely manner if the bank has a complex BaaS stack involving several interconnected components and parties, which can make it more challenging to identify the exact source of the attack.



#### Limited redundancy measures

Without adequate redundancy measures (such as failover systems) in place, an API attack might significantly impact a bank's systems, especially if the bank heavily relies on the affected APIs to enable critical services.



#### Lack of input validation

Without input validation, attackers may inject malicious code into a bank's systems through its APIs, which can be used to steal sensitive customer data or access critical backend systems.




## Target mitigation outcomes and opportunity landscape

Mitigation outcomes should focus on cybersecurity, third-party due diligence and capacity building for BaaS providers with whom banks have partnered.

### Target mitigation outcomes



**Strong security for BaaS platforms and API connectivity**



**Properly vetted BaaS partners**



**Institutional knowledge transfer from banks to BaaS partners**

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration

### Mitigation opportunity landscape

- Implement input validation mechanisms.
- Apply network segmentation and access control measures.
- Implement AI penetration testing and simulation systems.
- Perform enhanced due diligence on BaaS providers.
- Offer capacity building for partner BaaS providers.

*The following slides will summarize current mitigation efforts that are growing in adoption and provides in-depth analyses of emerging mitigation opportunities for consideration.*

## Current mitigation efforts growing in adoption

Ongoing mitigation efforts to tackle risks from BaaS include input validation mechanisms, network segmentation and access controls, enhanced due diligence and capacity building from established banks.

		Government-initiated	Sector-initiated
<p><b>Implement input validation mechanisms</b></p> <p>Input validation protocols ensure that the data received by APIs meet the required format and established rules to mitigate against security vulnerabilities such as cross-site scripting and Structured Query Language (SQL) injection attacks.<sup>106</sup> Several input validation frameworks have been developed, such as <i>Bean Validation</i>,<sup>107</sup> which is used to validate input data in Java-based applications and <i>OWASP Validation Regex Repository</i>,<sup>108</sup> used to validate input data such as phone numbers, credit card numbers and addresses.</p>	<p><b>Apply network segmentation and access control measures</b></p> <p>Network segmentation is part of a layered security plan to protect BaaS platforms and API connectivity. Separating important systems and data makes it more difficult for an attacker to move laterally across the network.<sup>109</sup> Security solutions such as firewalls, access control and zero-trust networks are being used by banks to reinforce network security.</p>	<p><b>Perform enhanced due diligence on BaaS providers</b></p> <p>To mitigate the risks introduced by BaaS partnerships, banks are enhancing due diligence procedures when evaluating the operational and security practices of BaaS providers. This includes ensuring compliance with regulations and industry standards and evaluating security measures and incident response plans in place. The Office of the Comptroller of the Currency in the US has developed guidance for community banks on conducting due diligence on external parties, including assessment of internal control environments.<sup>110</sup></p>	<p><b>Offer capacity building for partner BaaS providers and other ecosystem players</b></p> <p>Banks are supporting BaaS providers and other fintechs within the ecosystem they have partnered with through training and provisioning tools on risk management and compliance. Due to their size, some newer players in the BaaS space may not have the capabilities to meet certain rules and industry standards. For example, BBVA, a BaaS platform provider, offers several features (e.g. KYC) to ensure that parties using their platform adhere to laws and regulations.<sup>111</sup></p>

### Considerations to strengthen existing mitigation efforts

Independent security audits should be conducted periodically to verify that appropriate security measures are in place for third-party access to the BaaS network.

Security training should be provided to employees to minimize successful phishing attacks. Simulated phishing attacks should be conducted to identify weaknesses and assess the effectiveness of training programmes.

Banks that depend on BaaS providers for mission-critical services should have a plan in place to transition away from BaaS providers if they fail to satisfy their compliance responsibilities or go out of business.

Banks should conduct periodic audits to ensure that partner fintechs and other players within the BaaS ecosystem are complying with regulatory requirements and industry standards.

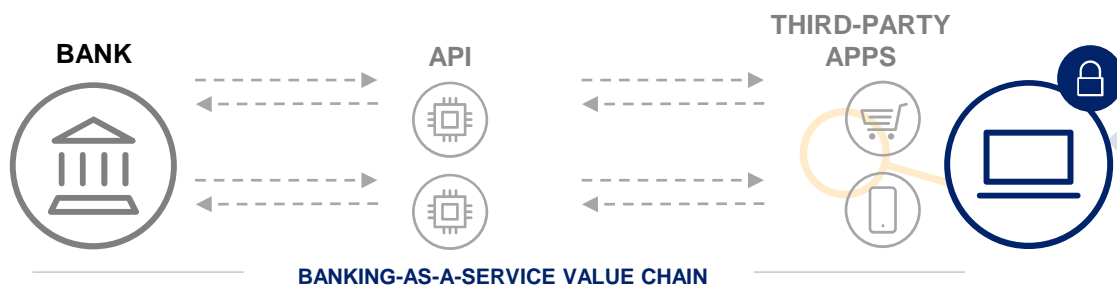


# Implement AI penetration testing and simulation systems

## Opportunity overview

AI-enabled penetration testing and simulation may be used to secure APIs and protect sensitive financial data and transactions within the BaaS stack. Algorithms for AI-enabled penetration testing have the capability to simulate and test various attack scenarios, such as those involving a hacker attempting to get into a system or malware infecting a network.<sup>112</sup> The goal is to identify and remedy system vulnerabilities before they can be exploited by malicious actors, such as authentication and authorization system flaws and SQL injection issues. The AI-powered penetration testing system can monitor API updates and modify its testing processes, resulting in more dynamic and extensive security testing. Some of the benefits include automating monotonous testing processes, managing an enormous amount of data, multiple systems testing and responding to emerging threats in real-time.<sup>113</sup> Penetration testing is a cybersecurity process requirement in some jurisdictions. For example, the New York State Department of Financial Services (NYDFS) requires all financial services organizations in the state to have a full cybersecurity program that includes regular penetration testing.<sup>114</sup>

## How it could work



### AI penetration testing system embedded within the BaaS ecosystem

AI-based penetration systems could be trained to detect and exploit flaws in a target API within the BaaS ecosystem by using a dataset of known vulnerabilities and attack patterns. Using genetic algorithms, new attack scenarios could be generated, and new weaknesses discovered.

## Conditions necessary for success

High-quality and diverse data are needed for AI penetration testing systems to continuously learn and adapt.

An audit of AI periodically is critical to ensure that the algorithms perform as designed.

## Relevant case studies



Deep Instinct is a cybersecurity firm that uses artificial intelligence to combat cyberattacks. Their AI-powered platform performs penetration testing, can identify malware and offers real-time cyberthreat prevention. The Deep Instinct platform can also perform automated threat hunting and incident response, ensuring complete network and data protection. The endpoint security capabilities can be deployed to secure API connectivity within the BaaS network.

## Inadequate stability mechanisms for stablecoin arrangements

Lack of adequate stability mechanisms in stablecoin arrangements can heighten the probability of a run, which may impact both consumers and the broader financial system.

### Background

Stablecoins are digital assets whose value is tied to another asset, such as fiat currencies or commodities (e.g. gold). They are designed to mimic fiat currencies but without the backing of a central bank. Stablecoins generally run on distributed ledger technologies and are used in several ways, including as a store and transfer of value, collateral for crypto derivatives and facilitating payments.<sup>115</sup> Three main forms of stablecoins exist today – **public reserve** backed by fiat or cash equivalent (e.g. Tether, USD Coin); **public algorithmic**, which are uncollateralized and uses smart contracts to maintain the value of the token (e.g. Frax, Ampleforth); and **private stablecoins**, which are issued on permissioned blockchains by private institutions (e.g. JPM coin).<sup>116</sup>

Stablecoins have grown significantly, with the market capitalization increasing from just over \$2 billion in early 2018 to \$164 billion in March 2022.<sup>117</sup> Although it has decreased to \$137 billion as of February 2023,<sup>118</sup> renewed adoption by individuals and institutions is probable, potentially deepening its linkages with the broader financial system and introducing contagion risks.

### Emerging risks

- The failure of a significant stablecoin issuer could shock the short-term liquidity funding market, as issuers who are large holders of short-term debt instruments may scramble to sell off reserve assets to meet redemption requests.<sup>119</sup> Tether and Circle alone hold about 2% of the US treasury bills.<sup>120</sup>
- Investment in risky assets by stablecoin issuers could result in a mismatch of customer liabilities and liquid assets, which may precipitate a loss of consumer confidence if the information were to become public, potentially resulting in a run. Although holdings in risky assets provide revenue opportunities, they increase the fragility of stablecoin arrangements.
- The absence of a strong stability back-stop mechanism such as deposit insurance exposes consumers to irreparable losses if a stablecoin issuer becomes bankrupt. Compared to demand deposits, consumers have little recourse to recover their funds. The collapse of the TerraUSD algorithmic stablecoin in May 2022 resulted in more than \$60 billion in losses to consumers and investors.<sup>121</sup>
- Inadequate anti-money laundering procedures may undermine the financial system’s integrity as illicit funds could be converted into stablecoins and moved across borders, bypassing traditional financial system controls.

## Risk vectors



**Governance and regulatory gaps could engender the perpetuation of illicit activities that might threaten the integrity of the broader financial system**



**Structural vulnerabilities of novel technologies used for minting and managing stablecoins are exposed to security risks**



**Absence of a stability mechanism reinforces the fragility of stablecoin arrangements and increases the risk of a run**

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

In the event that a significant stablecoin issuer is unable to promptly honour large customer withdrawal requests due to insufficient, or the mismanagement of, reserve assets, consumers' trust in the solvency of the stablecoin issuer could quickly diminish with the resulting panic spread on social media, spiralling into a run and eventual collapse of the stablecoin arrangement.



#### Disruption of short-term funding market

To meet sudden large redemption requests, stablecoin issuers may scramble to liquidate reserve assets in the money market through fire sales which could disrupt the market's liquidity flow.<sup>122</sup>

#### Consumer and investor losses

Consumers may be unable to redeem the face value of their token if the stablecoin issuer becomes insolvent. Additionally, institutional investors that have provided capital for stablecoin issuers may be forced to mark down their investments or write them off entirely.

#### Payment system disruption

Payment processors using stablecoins may face settlement risk if a major stablecoin collapses. The UK, for instance, is exploring the recognition of stablecoins as a form of payment<sup>123</sup> that could boost the usage of stablecoins by individuals and households.

### Forces that can amplify and accelerate the risk



#### Weak regulatory environment

Jurisdictions with weak regulatory standards are more susceptible to stablecoin runs and have limited capability to respond in the event of a stablecoin collapse.



#### Stringent capital controls

Individuals in jurisdictions with stringent capital controls or weak currencies are likely to park their assets in global stablecoins that are pegged to stable currencies such as the US dollar.



Regional force



Entity force



#### Technology and operational gaps

Unsecure systems and poorly managed internal processes could increase the risk of security breaches which could compromise the integrity of the stablecoin arrangement.



## Target mitigation outcomes and opportunity landscape

Mitigation efforts to address stablecoin risks must prioritize the safety of consumers and investors, standardization of rules and transparency of capital reserves.

### Target mitigation outcomes

- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



### Mitigation opportunity landscape

- Establish crypto anti-money laundering and counter-terrorist financing (AML/CFT) standards.
- Enable embedded supervision of stablecoin arrangements.
- Offer insurance coverage for stablecoins.
- Enforce responsible marketing rules and consumer education.
- Ensure transparency and audit of reserve assets.

*The following slides will summarize current mitigation efforts that are growing in adoption and provides in-depth analyses of emerging mitigation opportunity for consideration*

## Current mitigation efforts growing in adoption

Ongoing initiatives are geared towards increasing trust by strengthening stablecoin arrangements through transparency, governance and consumer education.

		Government-initiated	Sector-initiated
<p><b>Offer insurance coverage for stablecoins</b></p> <p>Insurance coverage for stablecoin tokens is being considered to protect consumers should a stablecoin issuer become bankrupt. For instance, the United States Federal Deposit Insurance Corporation (FDIC) is exploring the feasibility of offering insurance coverage for banks holding custody of reserve assets to protect consumers if a stablecoin issuer becomes insolvent.<sup>124</sup></p>	<p><b>Ensure transparency and audit of reserve assets</b></p> <p>Some regulatory authorities now require stablecoin issuers to conduct periodic audits and stress testing of their reserve assets. The NYDFS has mandated stablecoin issuers operating in New York to carry out a monthly independent audit of capital reserves to ascertain the sufficiency and quality of their reserve assets.<sup>125</sup></p>	<p><b>Enforce responsible marketing rules and consumer education</b></p> <p>Regulators in some jurisdictions, like the Monetary Authority of Singapore, are discouraging the advertising of crypto assets to the general public.<sup>126</sup> Also, Thailand now requires crypto ads to have investment risk warnings.<sup>127</sup> Similarly, to increase consumer awareness, the US Department of Treasury has rolled out campaigns on crypto risks.<sup>128</sup></p>	<p><b>Establish crypto AML/CFT standards</b></p> <p>To battle financial crime and strengthen market integrity, the Financial Action Task Force (FATF) has rolled out a set of standards that jurisdictions and Virtual Asset Service Providers (VASPs) are encouraged to implement. The recommendation requires that proper controls be put in place to cover customer due diligence, reporting of suspicious transactions and international collaboration.<sup>129</sup></p>

### Considerations to strengthen existing mitigation efforts

At the onset, stablecoin insurance may need to be covered by government-backed insurance institutions rather than private insurance firms due to the evolving nature of the risks surrounding stablecoins.

In addition to a periodic audit of reserve assets, stablecoin issuers could explore the option of publishing, in real-time, the balance of collateral held by custodians to further strengthen transparency.

Stablecoin issuers who have not done so can develop training materials tailored to different consumer categories, ensuring that customers have access to learning resources that clearly outline the associated risks of cryptocurrencies.

Like banks, stablecoin issuers should have strong AML and KYC procedures and systems to ensure that their stablecoins are not used to facilitate illicit transactions.

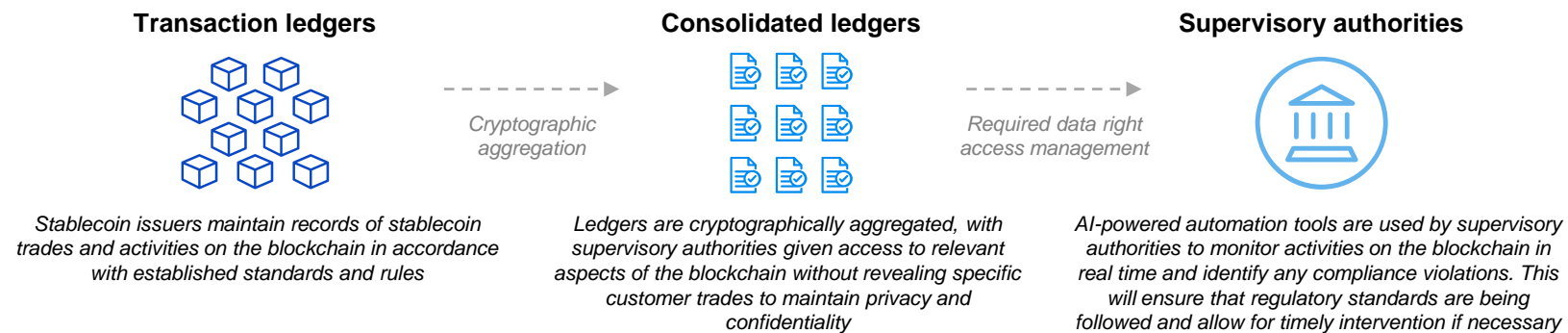
# Embedded supervision of stablecoin arrangements

## Opportunity overview

Due to the immediate settlement nature of stablecoin transactions and the absence of intermediaries, real-time monitoring of transactions on the underlying blockchain is critical to safeguarding consumers and protecting the financial system’s integrity. To achieve this, regulators could explore embedded supervision to automate compliance monitoring, verification of reserve assets, monitoring of transaction flows and investigation of suspicious transactions on the ledger.<sup>130</sup> In addition to the increased oversight capacity of regulators that will be achieved through embedded supervision, stablecoin issuers will be able to meet compliance requirements at a significantly reduced cost.

## How it could work

Instead of relying on historical reporting from stablecoin issuers, supervisory authorities could be plugged into the relevant aspect of the stablecoin blockchain with real-time access to conduct on-demand oversight functions.<sup>131</sup>



## Conditions necessary for success

Robust collaboration and cooperation between stablecoin issuers, regulators and other sector players will be pivotal to ensure that the necessary information and resources are available to support effective supervision.

Implementing embedded supervision will require a clear and comprehensive regulatory framework that lays out clear guidelines and outlines the expectations of different parties, as well as the necessary legal and regulatory powers for enforcement.

## Relevant case studies



The European Union, under the Directorate-General for Financial Stability, Financial Services and Capital Markets Union (FISMA), is exploring a proof of concept to evaluate and test technological solutions for embedded supervision of decentralized finance (DeFi) activity on the Ethereum blockchain. The pilot will focus on exploring automated data gathering directly from the blockchain for supervisory monitoring of real-time DeFi activities. The outcome of the pilot will be used to inform future DeFi-related policy decisions and the use of technology for supervision.<sup>132</sup>



# Insurance

## Vulnerabilities in parametric insurance smart contracts

Given that smart contracts are designed to execute automatically, any programming flaws or security vulnerabilities could result in substantial losses.

### Background

Smart contracts are self-executing agreements configured on a distributed ledger system that allows multiple parties to reach an accurate, timely and consensus-verifiable shared result. Interest is growing in applying smart contracts within the insurance sector, especially for automating parametric insurance. Unlike typical indemnity policies that compensate policyholders based on the number of losses, parametric insurance pays a fixed amount based on the severity of the insured event, making smart contracts a feasible and low-cost option for insurers.<sup>133</sup> For example, under one type of parametric crop insurance, payouts are made to farmers if the volume of rainfall falls below a predetermined level.

Many insurers are investing in smart contracts since it is expected to save them over \$21 billion in yearly operational costs.<sup>134</sup> Allianz and Nephila Capital successfully piloted the execution of natural catastrophe bond transactions using blockchain smart contracts.<sup>135</sup> Additionally, Axa, a global insurance company, launched parametric insurance in 2017 for delayed flights, using the Ethereum blockchain to compensate travellers for delays using global air traffic databases.<sup>136</sup> Similarly, Arbol uses smart contract technology to provide weather insurance, globally leveraging open-source, decentralized climate data (dClimate).

As the adoption of smart contracts accelerates, insurers must fully grasp the risk that smart contracts may introduce into their operations as the risks associated with the technology continues to evolve.

### Emerging risks

- **Data integrity:** As smart contract execution is contingent on off-chain data (such as the quantity of rainfall) from third parties, the security of the connection to external systems and integrity of the data used to trigger payouts are critical, as any breach will result in undesirable outcomes. For example, the data pulled from IoT sensors used for measuring the volume of rainfall may be maliciously manipulated to feed the wrong data to the smart contract.
- **Blockchain platform vulnerabilities:** Blockchain platforms (such as Ethereum, Quorum, Corda, etc.) are vulnerable to defects or bugs, which can negatively impact the integrity and performance of smart contracts hosted on their networks. These vulnerabilities could stem from weak protocols, coding errors or malicious acts, such as the injection of “backdoors”, which could be later exploited. In 2017, hackers stole \$30 million worth of Ethereum by exploiting a security flaw in a smart contract run by Parity Technologies.<sup>137</sup>

## Risk vectors



Smart contracts could be undermined by bugs in blockchain networks that support them



The immutability feature of smart contracts adds complexity when attempting to resolve errors promptly



Reliance on external data sources, which could be manipulated, exposes smart contracts to risks



The evolving nature of the regulatory and legal landscape creates uncertainty around the enforcement of smart contract agreements



## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

In the event that the volume of parametric insurance policies programmed on smart contracts was to grow to significant levels, manipulation of external data provided by a third party and used by multiple insurers could lead to fraudulent claims, resulting in financial losses to insurers with the following second-order impacts:



#### Financial loss and market volatility

Insurance companies may experience significant losses from wrongful payouts, affecting financial stability. Market liquidity could be distorted as insurers scramble to sell their asset reserves to pay for claims.

#### Loss of customer trust

A breach in an insurance smart contract could lead to a loss of trust in the insurer, as policyholders may question the security of the insurer's systems. This could lead to policyholders cancelling or not renewing their policies, possibly impacting the insurer's business and threatening its stability.

#### Reputational damage

An insurance smart contract hack could harm the insurer's reputation and brand. This could lead to a decline in business and potentially long-term financial consequences for the insurer.

### Forces that can amplify and accelerate the risk



#### Ambiguity of legal and regulatory environment

Disputes and legal challenges may be more likely to arise in jurisdictions where the legal and regulatory standards governing digital contracts are unclear. This could lead to a lack of trust and create uncertainty about when and how digital contracts are enforced.



#### Underdeveloped technological infrastructure

Smart contract implementation may be more challenging in regions or institutions with less developed technological infrastructures. Furthermore, areas with high exposure to cyberthreats will be more susceptible to attacks from hackers and other bad actors.



#### Limited technological expertise

Inadequate knowledge of, or experience with, smart contracts can make it harder to spot and address potential threats. Inadequate security measures or improper implementation of the contracts, for example, can leave the system vulnerable to attacks from malicious actors.



Regional force



Entity force

## Target mitigation outcomes and opportunity landscape

To effectively address the risks associated with smart contracts, the focus should be on enhancing cyber resilience, implementing strong governance practices, and ensuring adequate regulatory and legal coverage.

### Target mitigation outcomes



### Mitigation opportunity landscape

- Conduct an audit of smart contract code.
- Adopt best practices and use safe programming languages.
- Implement zero-trust security architecture.
- Reinforce an issuing party's governance mechanisms when deploying smart contracts.
- Include smart contracts in regulatory and legal frameworks.

*The following slides will summarize current mitigation efforts that are growing in adoption and provides in-depth analyses of emerging mitigation opportunities for consideration.*

## Current mitigation efforts growing in adoption

Risk mitigation measures should cover governance, legal and regulatory frameworks, programming best practices and auditing of smart contract source codes.

		Government-initiated	Sector-initiated
<p><b>Reinforce an issuing party's governance mechanisms when deploying smart contracts</b></p> <p>Due to the immutability of smart contracts, governance mechanisms are crucial to establishing procedures for making contract changes. The governance process should be well documented and include a voting system to authorize contracts and provide greater transparency to communities when protocol security processes change.<sup>138</sup></p>	<p><b>Include smart contracts in existing regulatory and legal frameworks</b></p> <p>Existing legal frameworks may not be well-suited to adjudicate smart contracts since the present financial system is based on intermediaries, unlike blockchains, which are self-executing. To safeguard users and ensure speedy resolution of disputes, current legal frameworks must be updated to accommodate smart contracts. In May 2018, the state of Vermont passed a law recognizing smart contracts in state courts.<sup>139</sup></p>	<p><b>Adopt best practices and use safe programming languages</b></p> <p>The use of established design patterns, adherence to security best practices, and programming code simplicity are measures that developers should consider in designing smart contracts. In addition, certain programming languages are regarded as more secure because they are less prone to specific vulnerabilities. Rust and Vyper, for instance, are widely used due to their strong security.<sup>140</sup></p>	<p><b>Conduct audits of smart contract source codes</b></p> <p>The source code of the smart contract must be audited both before and after deployment to ensure that the smart contract is operating as intended and is free of security flaws. Smart contracts may be audited in various ways: a basic code review that examines each line of code in detail, a security audit that identifies security flaws or a functional audit that confirms the contract is operating as intended. Several fintechs, such as Hacken and Solidproof, already provide smart contract audit services.<sup>141</sup></p>

### Considerations to strengthen existing mitigation efforts

Insurance companies should factor in approaches to managing risks from the underlying blockchain platform as part of governance procedures, including strategies to respond to data breaches.

International cooperation is crucial to the harmonization of laws that regulate smart contracts. This will be necessary to speed up the resolution of disputes from smart contracts executed across borders.

For insurance companies seeking to integrate smart contract systems with other internal applications, it will be important to ensure that the code is compatible and safe to prevent threats to the rest of the enterprise.

Companies using smart contracts should conduct thorough independent penetration testing in addition to code audits to ensure that programming flaws and bugs are detected and fixed before deployment.

# Implement zero-trust security architecture

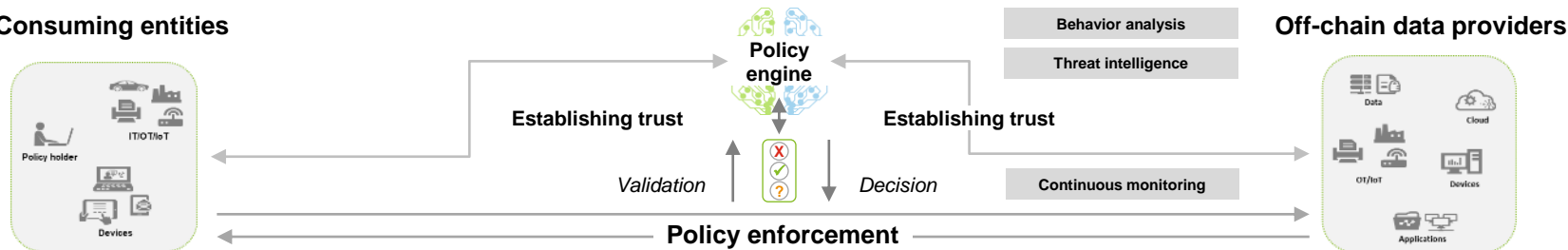
## Opportunity overview

The integrity of external data and the security of the underlying blockchain are critical for smart contract execution. Access to the underlying code poses security concerns that, if not addressed, can be exploited by malicious parties. As smart contracts for parametric insurance involve several parties – insurance companies (administrators), policyholders (who need access to the smart contract), and third parties (who provide external data) – the attack surface is expansive. Instead of relying on a perimeter-based architecture, which trusts assets within the perimeter, insurance companies should consider a zero-trust architecture (ZTA) approach to effectively manage access to systems, networks and data while maintaining control.

## How it could work

All users (administrators, policyholders, and third-party providers) must pass through the same security layer to access the smart contract network. Each user or device will be assigned unique permission within the network, with administrators given full access. Users or endpoint devices will be authenticated for each session on the network and approved by all nodes present in the blockchain. Data consumed by the smart contract will be encrypted end-to-end with need-to-know access.

### Consuming entities



## Conditions necessary for success

Regular security assessments and audits can help identify vulnerabilities and potential weaknesses in the zero-trust architecture and allow organizations to take steps to address them.

Administrator rights and privileges should be closely monitored as they are vital to preserving the integrity of the smart contract. Malicious updates or changes could have adverse effects.

## Relevant case studies



To ensure the safety of its cloud-based video streaming service, Netflix has implemented a security strategy based on zero-trust architecture. The approach protects against potential cyberattacks by including preventative measures such as network segmentation and constant monitoring.<sup>142</sup>

## Growing protection gap for catastrophic cyberattacks

Financial institutions' ability to recover from large-scale cyberattacks may diminish as insurers limit their exposure.

### Background

The rise in frequency and impact of cyberattacks on financial institutions (ransomware, data breaches and service disruptions) has spiked institutional demand for cyber insurance and created a highly dynamic threat landscape for cyber insurance providers.

A significant share of cybercrimes is now considered state-sponsored and driven by hacktivist campaigns with political motivations,<sup>143</sup> as the coordination between military warfare strategies and cybercrimes increases.<sup>144</sup> A survey including over 500 cybersecurity decision-makers working in critical national infrastructure has found that over 70% reported increased attacks since Russia's invasion of Ukraine.<sup>145</sup>

The growing probability of attacks and magnitude of financial loss have led to higher costs to insure against cyberthreats (up to 200% for insurers since the beginning of the Russia-Ukraine war<sup>146</sup>). In response, insurers are questioning the viability of offering cyber insurance products. Insurer group Lloyd's of London, which provides approximately 20% of the global cyber market,<sup>147</sup> plans to exclude catastrophic state-backed attacks from cyber insurance policies starting in March 2023,<sup>148</sup> and attacks that occur during wars, whether declared or not.<sup>149</sup> The scale of state-backed financial resources that can fuel future cyberattacks will increase the probability of cyber catastrophes that no single reinsurer has the capital reserves to absorb.

### Emerging risks

- **Supply and demand imbalance:** The rise in state-backed cyber warfare and the difficulty in tracing cyberattacks to state-backed sources is leading to insurer reluctance to provide cyber insurance products in general. The imbalance between the supply and demand for cyber insurance has created a protection gap that may leave financial institutions and systemically significant entities within the financial services ecosystem (e.g. critical third-party providers) vulnerable in a state-backed cyberattack.
- **Data limitations:** The limitations in forward-looking data that is currently available to predict the likelihood of occurrence and the magnitude of loss for cyberthreats may continue to lower the affordability of cyber insurance products, making cyberattacks effectively uninsurable for institutions in the future.<sup>150</sup>

## Risk vectors



Cyber warfare tactics are increasingly being used to accelerate geopolitical tensions between nation states



Generative AI applications are lowering the barriers to entry for cyber criminals (e.g. using ChatGPT to create malware)<sup>151</sup>



Funding made available from nation states enables sophisticated and high-impact attacks



There is limited visibility and on signals that predict large-scale cyberattacks, contributing to affordability challenges

## Systemic risk scenario and amplifying forces

### Potential systemic risk scenario *(if the sector-specific risk is not mitigated)*

If a cyberattack cripples multiple banks or critical third-party providers that are covered by a common insurer, there can be significant second-order impact if there are limitations to institutions' insurance policies or insufficient insurer reserves available to cover the losses when multiple claims are triggered in parallel:



#### Downstream insolvency of institutions within an entity's network

If a financial institution becomes insolvent due to coverage limitations, the solvency of partner institutions and third-party providers it has loan agreements with may be threatened.

#### Liquidation of investments to offset a financial institution's losses

As insolvent insurers struggle to honour insurance claims, impacted financial institutions will withdraw large sums of investments to gain access to capital to offset their losses; other investors will be affected by sharp price swings, potentially destabilizing capital markets.

#### Impacts on government budgets

Governments may have to provide unplanned financial aid to support financial institutions impacted by claims that insolvent insurers cannot cover, changing competitive dynamics between players and affecting government budgets.

### Forces that can amplify and accelerate the sector-specific risk



#### Size of an institution's third-party network

Financial institutions that depend on a large network of third-party vendors for their services are more vulnerable to the damage of successful cyberattacks against their vendor network.<sup>152</sup>



#### Limited availability of cybersecurity diagnostic data

Regions that don't mandate a financial institution to disclose data breaches or security hygiene practices will have limited diagnostic data available for insurers and reinsurers to confidently price the risk of providing cyber insurance, widening regional protection gaps.



#### Poor cross-border government alliances

Regions that don't participate in international organizations (e.g. NATO, ASEAN) may have more difficulty contributing to cyber data-sharing schemes that aid in preventing and detecting state-sponsored cyberattacks quickly.



Regional force



Entity force



## Target mitigation outcomes and opportunity landscape

Mitigation efforts to address the protection gap from cyber insurance limitations should focus on increasing the financial capacity of insurers, designing public-private regimes to absorb systemic losses and increasing the confidence in forward-looking cyber data for insurers' risk models.

### Target mitigation outcomes


- Current mitigation efforts growing in adoption
- Emerging mitigation opportunities for consideration



**Alternative sources of capital to cover growing cyber risks**



**Public-private support to prevent or absorb cyberattack damage**



**Intelligence on cyberattack damage**

### Mitigation opportunity landscape

- Raise funds in private markets through insurance-linked securities (ILS).
- Conduct stress testing for cyber underwriting risk and resilience.
- Establish centralized resource centres for private entities to collectively build cyber resilience.
- Quantify cyber risk damage to measure portfolio exposure to cyberthreats.
- Use digital twin models to offer risk-based pricing for policyholders and threat intelligence for governments

*The following slides will summarize current mitigation efforts that are growing in adoption and provides in-depth analyses of emerging mitigation opportunities for consideration.*

## Current mitigation efforts growing in adoption

Efforts to strengthen insurers' financial capacity, risk modelling accuracy and cyber risk stress testing are underway, creating new opportunities for sector-initiated, cross-border initiatives that can protect critical infrastructure from systemic cyber catastrophes.

		Government-initiated	Sector-initiated
<p><b>Raise funds in private markets through insurance-linked securities (ILS)</b></p> <p>Beazley, an insurer of Lloyd's of London, has launched the first cyber catastrophe bond, which pays interest to bondholders and triggers a payout if total claims from a cyberattack on its policyholders exceed \$300 million, helping protect the insurer's balance sheet.<sup>153</sup></p>	<p><b>Conduct stress testing for cyber underwriting risk and resilience</b></p> <p>The European Insurance and Occupational Pensions Authority has published a discussion paper on assessing the requirements for a new insurer stress-testing framework, including tests for cyber underwriting risk and financial resilience under severe cyber incident scenarios.<sup>154</sup></p>	<p><b>Establish centralized resource centres for private entities to collectively build cyber resilience</b></p> <p>Cybersecurity centres for financial institutions have been established regionally (e.g. Africa Cybersecurity Resource Centre, National Cybersecurity Centre in Switzerland) and are promoting cooperation between private entities and authorities on strategic and operational cybersecurity issues, including access to cost-effective training opportunities through cyber exercises and crisis simulations for members.</p>	<p><b>Quantify cyber risk damage to measure portfolio exposure to cyberthreats</b></p> <p>CyberCube is a cloud-based platform that helps insurers quantify cyber risk and assess the damage of different cyberattack scenario classes.<sup>155</sup> They have also launched the world's first set of exposure databases, enabling reinsurers and brokers to conduct benchmarking, sensitivity and real-time analyses for cyber risks.<sup>156</sup></p>

### Considerations to strengthen existing mitigation efforts

To promote confidence in, and predictability of, the risk profile for cyber catastrophe bonds, issuers should provide transparency on variables that control the risk exposure for investors (e.g. industry and regional diversification).

Cyber resilience frameworks and stress testing methods should be applied against reinsurers and syndicates and standardized across jurisdictions to mitigate against regional exposures to cyberattacks.

Resource centres can partner with cybersecurity service vendors that offer volume discounts to members for access to cybersecurity tools and services; they can also partner with regulators to provide government-sponsored rebates for investing in cyber monitoring capabilities and to champion employer education initiatives.

Scenario classes and risk variables can be enriched with future successful cyberattacks enabled by popular generative AI applications like ChatGPT that are making cybercrime inexpensive, easy and lucrative.<sup>157</sup>



# Use digital twin models to offer risk-based pricing for policyholders and threat-intelligence for governments

## Opportunity overview

A digital twin is a virtual representation of a physical asset used to simulate scenarios and collect data on how the physical asset might respond. While digital twins have been adopted by equipment-intensive industries (e.g. manufacturing, aviation, mining), some governments are beginning to simulate critical infrastructure providers' network infrastructure to predict and build response plans for likely cyberattack scenarios.<sup>158</sup> Digital twins can represent a holistic view of an organization's network data and interactions to help analysts identify compromising cyberthreat scenarios and develop predictive defence responses.

There is an opportunity for insurers to increase the viability of cyber insurance products and minimize the magnitude of loss for policyholders by:

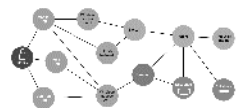
1. Promoting custom threat intelligence services and risk-based pricing for its policyholders
2. Designing data-sharing partnerships with governments to inform cybersecurity policy decisions.

## Relevant case studies



Teams at NATO's most recent Cyber Coalition used a novel cybersecurity defence software to develop knowledge graphs of critical infrastructure across borders, and reveal cyberattack patterns, network traffic and target systems that need protection to avoid a systemic shock event.<sup>160</sup>

## How it could work



1. Design a computerized model, or "knowledge graph" of a policyholder's network infrastructure to create a digital twin of the network.<sup>159</sup>

2. Connect models to cyberthreat intelligence databases of the latest threats and attack vectors (e.g. CyberCube).



3. Digital twin data model assesses network patterns, predicts attack paths and defence responses for network activity and can provide intrusion detection alerts.



4. Introduce variable pricing options based on the degree of threats faced by a policyholders' network and managed threat intelligence services to policyholders.



5. Share anonymized digital twin datasets as part of a data monetization regime with governments across jurisdictions for scenario planning and informing policy decisions.

## Conditions necessary for success

Data privacy regimes and sharing platforms that ensure the safe exchange of live network data between policyholders and insurance providers.

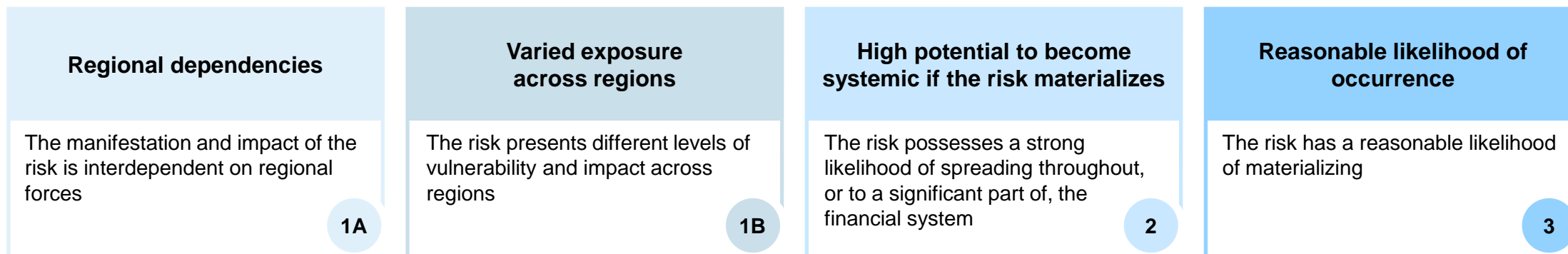
Anonymized digital twin data-sharing schemes with industry peers and across regions to elevate global threat intelligence at the industry level for policyholders (e.g. identifying the top attack scenarios for healthcare clients in Asia vs Europe)

# Regional risks and mitigation

---

The following section discusses risks that cut across the financial system, and either have regional dependencies or have varied exposure across regions

In order to be classified as a regional risk, it must meet criterion 1A or 1B in addition to criteria 2 and 3 as outlined below:



Three regional risks have been identified (non-exhaustive), and will be explored in the following section:



Increasing complexity of cyberthreats



Tech talent shortage



Mispriced climate-related financial risk

*The following pages examine the regional forces that shape the trajectory of these risks across different regions and lay out some of the ongoing mitigation approaches explored by the public and private sectors. Opportunities to enhance mitigation efforts are then offered.*

## Increasing complexity of cyberthreats across regions

The financial system in various regions is experiencing an increase in cybersecurity threats due to rising geopolitical tensions, widening attack surface, and advancement of cyberattack tools

### BACKGROUND

The first phase of this study, published in 2021, examined new forms of cyber-attacks and the driving risk factors associated with them, including inadequate cybersecurity procedures, compromised technical infrastructure, digital identity misrepresentation and authentication weaknesses. Since then, cyberattacks have continued to escalate and remain a significant threat to the financial system across the globe. Compared to 2021, the number of global cyberattacks in 2022 increased by 38%,<sup>161</sup> with the average data breach cost hitting a record high of \$4.35 million.<sup>162</sup> Some regions have been disproportionately affected by the frequency and severity of these attacks.

### EVOLVING RISK DRIVERS



#### Growing geopolitical tensions

As nations use cyberwarfare in response to geopolitical conflicts, the risk that financial services will be caught in the crossfire is increasing. Warring countries increasingly use cyberattacks to disrupt networks and critical infrastructure that financial services rely upon. As noted earlier in the report, insurance companies are now excluding coverage of state-backed cyberattacks, increasing the cost of cybersecurity risks to the financial system.



#### Expanding attack surface

As the use of APIs to connect systems and institutions increases, the number of entry points that malicious actors can exploit to gain access to the financial services system is expanding. This makes it harder to quickly identify the source of an attack and contain it in a timely manner. On average, it takes about 197 days for an organization to identify a data breach.<sup>163</sup>

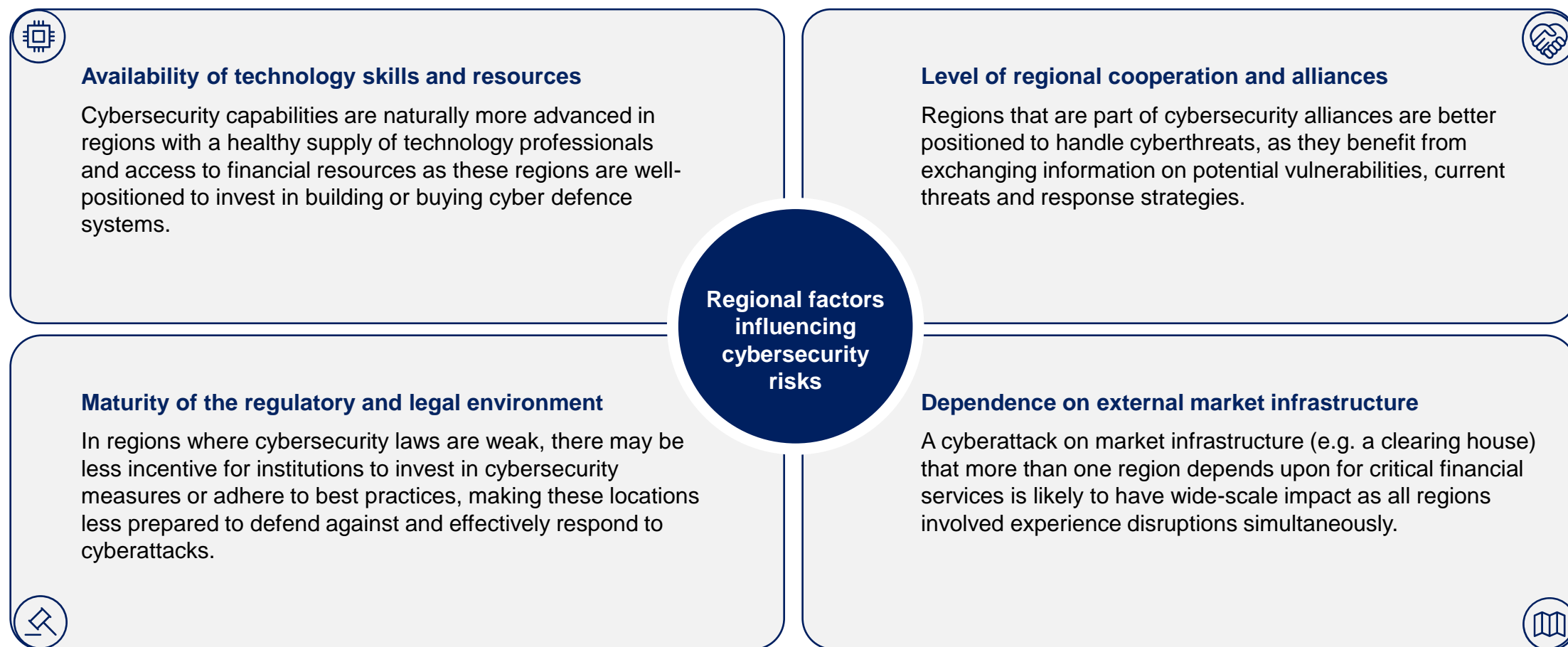


#### Proliferation of hacking tools

The advancement and proliferation of cyber hacking tools have increased the capability of cybercriminals to launch more targeted attacks. In combination with AI serving as an attack enabler, the emergence of "ransomware as a service", which allows bad actors to use pre-made tools to launch an attack is increasing cybersecurity risk.<sup>164</sup> Additionally, the ability to collect ransom payments in cryptocurrency is reducing the barrier of entry for cybercriminals.

## Forces that affect cybersecurity risks across regions

Several factors across regions contribute to the emergence of cybersecurity risks and the impact of an event should it occur.



## Mitigation of cybersecurity risks across regions

Efforts are underway to improve global and regional cybersecurity, including harmonizing cyber regulations, greater accessibility of cybersecurity tools, partnerships between the public and private sectors, and cross-border technical support.

### ONGOING MITIGATION EFFORTS

#### Harmonization of cybersecurity initiatives and laws

The fragmented nature of cybersecurity regulation and initiatives has made it challenging to pursue a coordinated global cybersecurity agenda.<sup>165</sup> The EU is one of the regions that has been working to address this through its Digital Operational Resilience Act (DORA). This act was officially published in December 2022 and seeks to bring order and uniformity to regulation across the EU to ensure all components of operational resilience, including cybersecurity and incident reporting, are properly managed.<sup>166</sup>

#### Democratization of cybersecurity tools and techniques

For access to cybersecurity tools in resource-constrained regions, organizations can use open-source software such as Snort and OpenVPN and security platforms from big tech companies like AWS Security Hub and Google Cloud Security Command Center. These options offer cost-effective access to basic cybersecurity services and help spread cybersecurity resources across regions.

#### Public-private joint incident response and partnerships

A coordinated effort between the public and private sectors is necessary to tackle cyberthreats. The Bank of Canada, for example, is leading a collaboration initiative with the private sector under the Canadian Financial Sector Resiliency Group (CFRG) to coordinate a sector-wide response to systemic-level operational incidents.<sup>167</sup> Similarly, the Swiss Bankers Association (SBA), in partnership with other groups, set up the Swiss Financial Sector Cybersecurity Centre (FS-CSC) to strengthen cyber resilience within the financial system.<sup>168</sup>

#### Cross-border capacity building

Several countries are leading technical training and offering cyber education to other regions to improve cybersecurity capabilities. For example, the Australian Cyber Security Centre (ACSC) provides training to countries in the Indo-Pacific region. Similarly, the UK Global Cybersecurity Capacity Centre (G3C) provides cybersecurity training programmes to various developing countries. The EU is also funding the Latin America and Caribbean Cyber Competence Centre (LAC4) to strengthen cybersecurity education in the region.

### OPPORTUNITIES TO ENHANCE MITIGATION EFFORTS



About 95% of cybersecurity breaches are caused by human error,<sup>169</sup> indicating public and private sector entities need to step up cyber awareness initiatives, such as social media campaigns, to ensure a broad understanding of cyberthreats.



Increased collaboration to help organizations carefully evaluate the risks posed by open-source tools and implement the necessary safeguards would be highly valuable. Similarly, greater support in addressing identified security flaws until a patch is designed would be beneficial.



Partnerships between the public and private sector should include increased funding of research and development efforts to identify and address emerging cyberthreats. By combining resources and expertise, the cybersecurity posture within their respective regions could be strengthened sectors.



Public and private sector players could organize innovative approaches such as cybersecurity competitions to provide hands-on experience to participants and simulate real-world security scenarios in a safe, controlled environment.

## Growing tech talent shortages across regions

With the growing reliance on technology and a shortage of tech talent, industry players across regions are experiencing challenges in finding the talent they need to drive innovation or maintain core operations.

### BACKGROUND

Financial institutions (FIs) rely on tech talent to maintain and support their core infrastructure while delivering innovative products to improve customer experience and operational efficiency. However, the shortage of tech talent is becoming increasingly challenging for FIs as they struggle to recruit skilled professionals to meet these objectives. The competition for tech talent is fierce, with organizations in other industries also vying for a limited pool of skilled tech professionals. Traditional FIs with legacy systems that require specialized knowledge and expertise to maintain them are facing additional difficulties. Regionally, challenges are especially felt in areas that tend to be less developed and resourced, as they have reduced opportunities to hire and retain top talent.

The consequences of talent shortages can be widespread, particularly given the interconnected nature of the financial system. When a region that delivers critical services to other parts of the financial system experiences service disruptions due to talent shortages, it could have a ripple effect across regions. Operations of FIs in other regions can be severely impacted, although some are more vulnerable than others. Related, when a significant percentage of financial services entities depend on a particular type of tech talent that is clustered in a certain region, concentration risk develops. For example, many FIs rely heavily on India for IT services and talent, meaning that disruptions to the Indian tech talent pool could have far-reaching effects on other regions that depend on them to deliver critical services.

### EVOLVING RISK DRIVERS



#### Increased demand for tech skills

The financial services industry increasingly relies on technological innovation to deliver its products and services to customers. As financial institutions execute their digital transformation strategy, the demand for tech professionals (such as data scientists, cybersecurity specialists, and database and network professionals) continues to expand.<sup>170</sup>



#### Competition from adjacent industries

The shortage of tech talent is felt across industries resulting in intense competition within and outside financial institutions. Organizations, especially those within emerging innovation spaces (such as fintechs), may be more appealing to tech talent due to factors such as the novelty of the technology, flexible work arrangements and equity ownership.



#### Socio-economic dislocations

Socioeconomic factors such as income, education, business and political climate can exacerbate tech talent shortages in some regions. For example, talent in regions experiencing economic or political difficulties may choose to migrate to other countries (human capital flight), reducing the available tech talent pool.

## Forces that influence shortages of tech talent across regions

The availability of training programmes, socioeconomic factors, atmosphere for innovation and immigration policies influences the severity of tech talent shortages in a region.



### Availability of educational and training programmes

The standard and accessibility of educational and training programmes influence the availability of tech talent in an area. Areas with great technology-based education and training opportunities will have a larger pool of tech talent for organizations in that region to recruit. Access to top-notch education and training programmes allows in-demand tech skills to be developed locally, thereby reducing the need to rely on other regions to bridge the skills shortage.



### Economic and social factors

Unfavourable and unpredictable economic, social and political situations in certain regions may make it more difficult to attract and retain skilled tech professionals. These regions often experience a higher rate of human capital flight as tech professionals seek better opportunities elsewhere. From 2015 to 2019, at least 70,000 ICT professionals from low- to middle-income nations migrated to higher-income countries.<sup>171</sup>



### Presence of innovation and technology hubs

A region's ability to attract tech professionals can be boosted by a favourable environment for innovation, such as the existence of technology hubs. Tech hubs provide a rich pool of tech talent with supporting infrastructure enabling innovation. Places like California, London, Beijing, Nairobi and Singapore are prime examples of innovation centres with a thriving tech ecosystem, attracting tech talent working on cutting-edge innovations.



### Progressive immigration policies

Immigration policies are crucial in attracting highly skilled technology workers to a region. Progressive immigration policies adopted by some countries such as Canada, Australia, New Zealand, Germany and Sweden help provide financial organizations with a richer pool of skilled workers from which to recruit. For example, Canada's Express Entry programme offers a fast-track permanent residency visa programme for skilled workers from other countries.

Regional forces  
influencing tech  
talent shortages



## Ongoing initiatives to mitigate tech talent shortages across regions

Efforts are underway to address the shortage of tech talent, including collaborations with academia, reskilling programmes, implementation of no-code and low-code platforms, and creation of technology hubs.

### ONGOING MITIGATION EFFORTS

#### Partnership with academia

Financial services organizations are joining forces with academic institutions to address the shortage of tech talent and prepare the next generation for the rapidly advancing technological landscape. They achieve this by offering internship opportunities to students and working with schools to redesign their curricula to match the evolving technology skills demand. For example, JPMorgan Chase's Tech for Social Good initiative aims to bridge the tech skills gap by providing education, coding and mentorship opportunities for young people.<sup>172</sup>

#### Reskilling existing employees

By introducing reskilling initiatives (such as job rotations and virtual learning portals), financial services organizations support current employees in developing new tech skills instead of focusing exclusively on external hiring to meet tech talent demand. Reskilling is a cost-effective option costing about \$20,000 less compared to hiring and training new recruits.<sup>173</sup> HSBC Malaysia created the Digital Black Belt Development Programme, a virtual programme to reskill its employees, helping them acquire digital data analytics, machine learning and automation skills.<sup>174</sup>

#### Utilization of no-code and low-code platforms

Financial institutions are embracing no-code and low-code technologies to tackle the challenge of tech talent shortages. By allowing non-technical users to build and launch applications with minimal coding, these platforms help accelerate software development and reduce dependency on a small pool of technology talent. For example, AXA, a leading global insurance firm, used OutSystems, a low-code platform, to successfully modernize its claims processing system in just three months, reducing the large volume of calls to the contact centre.<sup>175</sup>

#### Establishment of technology hubs

To attract and retain talent in a competitive labour market, financial services institutions are establishing technology hubs in cities with large tech talent pools. By having a presence in these locations, they can tap into the existing talent pool or attract professionals interested in relocating to these areas. These hubs serve as the centre for designing and implementing innovative technology solutions. For example, BMO, one of the large Canadian banks, is setting up tech hubs across North America and plans to hire over 250 people through 2023.<sup>176</sup> Also, Citi opened its Global Tech Hub in Bahrain with a goal of creating 1,000 tech jobs in the next decade.<sup>177</sup>

### OPPORTUNITIES TO ENHANCE MITIGATION EFFORTS



To increase the attractiveness of a region to tech talent, both public and private institutions must collaborate to build a thriving technology innovation ecosystem by making investments in critical infrastructure such as high-speed internet, data centres and co-working spaces.



As organizations leverage AI to automate tasks that were previously performed by humans, it is crucial to prepare their workforce to effectively collaborate with AI. To accomplish this, organizations should provide training opportunities to develop new skills such as data analysis, programming and structured questioning to optimize the value from the technology.



By supporting diversity, equity and inclusion (DEI) initiatives, various regions can position themselves as inclusive environments appealing to a diverse pool of tech talent. This can be achieved through promoting gender diversity, supporting underrepresented groups in tech, and fostering diversity in the workplace.

## Systemic mispricing of climate-related financial risk due to data challenges

Limitations in the availability and accessibility of data on the physical and transition risks of climate change create challenges for financial institutions to accurately embed the price of climate-related financial risk within their products.

### BACKGROUND

Amid global pledges to meet net-zero commitments over the next three decades, financial institutions are facing limitations in accessing reliable and granular datasets required to price the physical and transitional effects of climate change on their clients. These limitations can accelerate systemic mispricing of climate-related risk across loan adjudication decisions, insurance policies and asset valuations.

The most significant limitations will come from private small- and medium-sized client bases with limited resources, capabilities or incentives to collect and report data relevant to climate-related financial risk. With small- and medium-sized enterprises representing one-fifth of annual global banking revenues,<sup>178</sup> the data gap can expose financial institutions offering banking, insurance and investment management services to significant financial risk. Regional differences in net-zero goals, access to talent pools and capital allocation will further influence a financial institution's exposure to climate-related financial risk.

As financial institutions today have limited control over generating granular climate risk data for their client base, they may instead play a critical role in using technology-enabled mitigation opportunities to access and verify data relevant to climate risk for their clients.

### EVOLVING RISK DRIVERS



#### Inconsistent standards and disclosure requirements

Banks are sourcing climate disclosures from clients individually and with taxonomies and templates in certain regions (e.g. North America). For small multi-banked companies, this can translate to a high burden of proof in the form of higher costs of disclosure and transparency. This trend may further challenge a financial institution's ability to access and share standardized data.<sup>179</sup>



#### Growing frequency and magnitude of loss for climate shock events

Many recent studies, including those from the US Environmental Protection Agency (EPA) in August 2022, conclude that with rising global average temperature, climate shock events will become frequent,<sup>180</sup> and with a greater magnitude of loss. Limitations in translating these effects into financial risk for businesses will increase the impact on financial institutions.

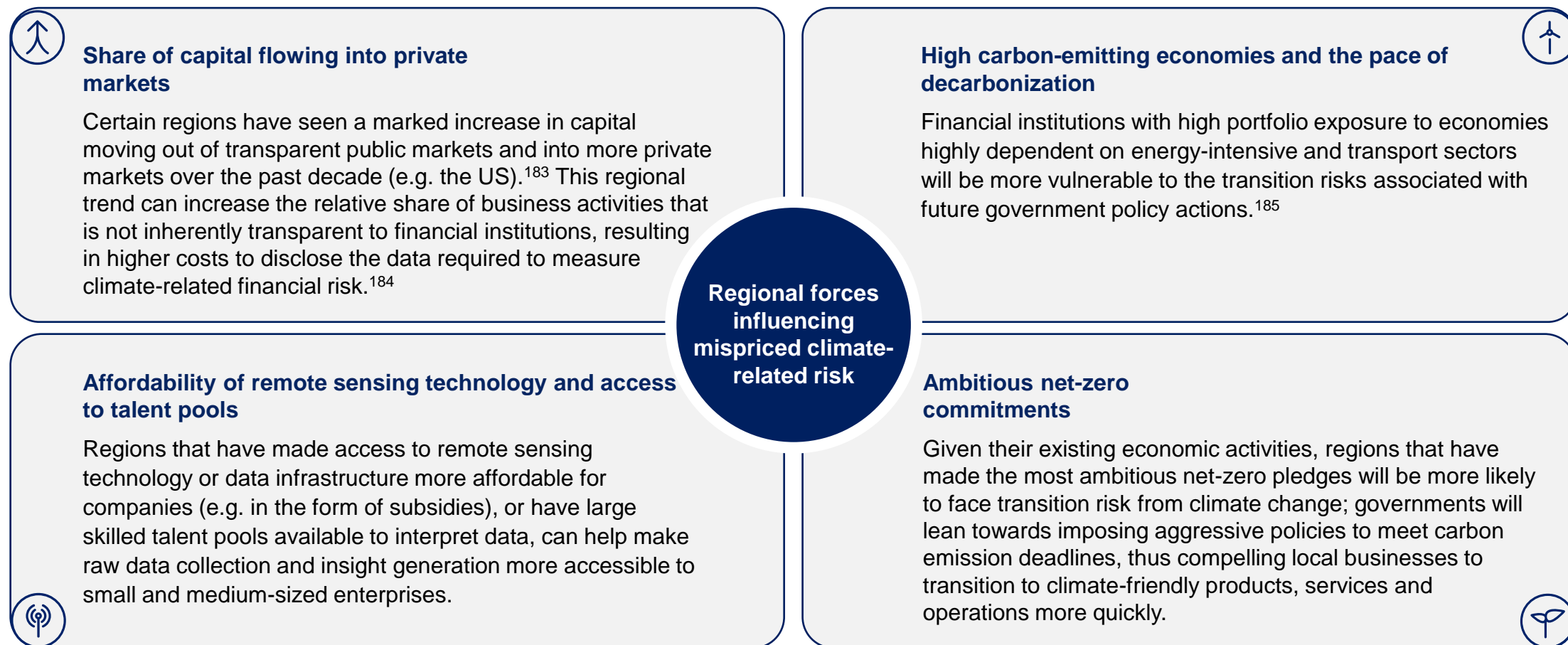


#### Reliance on proxy datasets that are subject to misinterpretation

Banks' current projections for climate stress tests have relied heavily on proxy data (e.g. country-sector level data on environmental externalities that replaces company-level emissions data<sup>181</sup>), which has led to widely diverging data reported by banks and likely inaccurate estimations of climate risk within products.<sup>182</sup> Proxy datasets can be vulnerable to various interpretations and inconsistencies.

## Forces that influence regional exposure to mispricing climate-related financial risk

Regional differences in net-zero goals, access to talent pools and capital allocation can significantly influence a financial institution's exposure to climate-related financial risk.



## Mitigation landscape for closing the data gap for climate risk

Current mitigation initiatives focus on standardizing the reporting of climate-related data and increasing platforms available for multiple financial institutions to access shared data. Opportunities remain for emerging technology to drive these outcomes.

### ONGOING MITIGATION EFFORTS

#### Climate hub initiatives for small and medium enterprises

The SME Climate Hub is a non-profit global initiative that empowers small to medium-sized companies to take climate action and build resilient businesses for the future. The hub provides free access to tools, resources and templates to help small businesses measure their full carbon footprint and tap into new funding opportunities through climate data reporting (e.g. bank loans, government grants).

#### Publication of climate-related statistical indicators

The European Central Bank has published experimental and analytical indicators that illustrate the impact of climate-related risks on the financial sector. Analytics indicators will share information on the carbon intensity of financial institutions' securities and loan portfolios and the financial sector's exposure to counterparties with carbon-intensive business models. They also cover climate-related physical risks and analyse the impact of natural hazards on the performance of loans, bonds and equities portfolios.<sup>186</sup>

#### Establishment of global private-public data utilities

The Net-Zero Data Public Utility is under development and expected to be the first public platform that aims to be a trusted central source of verifiable transition data. The utility will depend on private sector commitments to contribute standardized greenhouse gas emissions data from primary corporate and sovereign entities.<sup>187</sup>

#### Localized insights and regional predictions from complex climate models

The Climate Risk and Resilience Portal is a new publically available tool that reveals how future climate scenarios can impact US cities and towns. The tool transforms complex, large climate datasets into local reports that non-technical audiences can understand and apply for numerous purposes; dynamical downscaling integrates regional forecasting with global climate models.<sup>188</sup>

## OPPORTUNITIES TO ENHANCE MITIGATION EFFORTS



Automated climate data collection techniques coupled with API-enabled sharing methods can reduce data generation costs for companies and data accessibility costs for financial institutions to access real-time climate data.



Public-private data utilities can explore leveraging synthetic datasets generated by AI based on currently available info about businesses to build predictive models while minimizing the cost of raw data collection.



Financial institutions can use remote sensing tools (e.g. IoT devices, satellite imagery) to generate high-resolution data directly to inform investment decisions on clients and regions. Data from remote sensing tools can capture robust data on climate patterns, natural processes and human activities that can act as accurate proxies to assess progress on climate change mitigation.<sup>189</sup>

# Conclusion

---

## CONCLUSION

A sharpened understanding of the origination and proliferation of technology-driven risk from sectors and regions to the broader financial system better informs public and private sector players of targeted mitigation opportunities available to them

What examples of opportunities exist for private and public players to better address technology-driven systemic risk?

### Private sector players can...

- **Reinforce their role as trusted partners in consumers' financial decisions.** They can capitalize on opportunities to support and guide consumers in financial decision-making as patterns of distrust and uncertainty emerge from an increasingly fragmented financial landscape.
- **Include a diverse group of stakeholders in risk assessment.** Players can consider the influence and impact of adjacent players, alternative media providers, and data brokers when assessing an institution's degree of exposure to technology-driven risk originating from outside the traditional financial system.

### Public sector players can...

- **Use existing technologies to map common pools of risk.** They can tap into existing "open" data platforms and privacy-enhancing technologies to securely access real-time and verifiable insights on common clusters of risk at the ecosystem level.
- **Educate beyond financial literacy.** Players can prioritize media literacy alongside financial literacy for consumers to stabilize and neutralize sources of distrust in financial markets that are strengthening from alternative media platforms and data deception tools.

### Private and public sector players can collaborate to...

- **Lead international resilience experiments.** They can champion international experiments against technology-driven risk through cross-regional simulation techniques and autonomous intelligence that can forecast response requirements for global resiliency efforts.
- **Further invest in shared resource pools.** Players can identify opportunities to contribute to shared pools of capital and talent that can supplement public funding schemes and strengthen buffers available to absorb the effects of future technology-driven systemic shock events.

**As technology-driven risks remain highly dynamic, technology-enabled mitigation opportunities and collaboration efforts will depend on a constant stream of knowledge exchange and experimentation across jurisdictions and sectors to be effective and sustainable.**

# Acknowledgements

---

## Contributors

The project team would like to express their gratitude to the following subject matter experts who contributed valuable perspectives through interviews and by participating in workshop and roundtable discussions (in alphabetical order):

<b>Hassan Y. Aly</b>	Nile University	<b>Jon Frost</b>	Financial Stability Board
<b>Emilios Avgouleas</b>	University of Edinburgh	<b>Lesly Goh</b>	The World Bank
<b>Pavle Avramović</b>	Financial Conduct Authority	<b>Austan D. Goolsbee</b>	University of Chicago, Booth School of Business
<b>Andries Berendsen</b>	Rabobank	<b>Liza Lovdahl Gormsen</b>	Financial Conduct Authority
<b>Luther Bian</b>	China Construction Bank	<b>Kimberly Grauer</b>	Chainalysis
<b>Pedro Bizarro</b>	Feedzai	<b>Magnus Haglund</b>	Nasdaq
<b>Matthew Brush</b>	DST Global	<b>Tom Hammond</b>	Monzo Bank
<b>Kelly Buchanan</b>	Truist Financial Corporation	<b>Martin K. Hess</b>	Swiss Bankers Association
<b>Ross P. Buckley</b>	University of New South Wales	<b>Chris Hutton</b>	Callsign
<b>Jessica Camus</b>	Diginex Solutions	<b>Gilbert Kamieniecky</b>	Investcorp Holdings
<b>Anne-Sophie Cartray</b>	Citi	<b>Matthew Katz</b>	Blackstone
<b>Robin Castelli</b>	Citi	<b>Evelyne Kanini Kilonzo</b>	Central Bank of Kenya
<b>Reuben K. Chepngar</b>	Central Bank of Kenya	<b>Ronald Kohn</b>	Diginex Solutions
<b>Adam Clark</b>	Commonwealth Bank of Australia	<b>Trisha Kothari</b>	Unit21
<b>David Crofts</b>	Mubadala Investment Company	<b>Miki Kuusinen</b>	Bank of Finland/Suomen Pankki
<b>Michael Crumpler</b>	Credit Benchmark	<b>Brian Lam</b>	Hong Kong Monetary Authority
<b>Charles Delingpole</b>	ComplyAdvantage	<b>Jason Lee</b>	Algorand Foundation
<b>Rocio Diaz</b>	Pomelo	<b>Nick Lee</b>	OakNorth
<b>Laura Dirtadian</b>	Affirm	<b>Alex Low</b>	Suade Labs
<b>Matheus Lazzaris Duarte</b>	Banco Bradesco	<b>Kevin Madura</b>	AlixPartners
<b>Maximilian Dyck</b>	Suade Labs	<b>Sarkis Mazmanian</b>	Deutsche Bank
<b>Khaled Eid</b>	Nile University	<b>Gitau Mburu</b>	Central Bank of Kenya
<b>Misha Esipov</b>	Nova Credit	<b>Pascal Millaire</b>	Cybercube
<b>Valerie Fasquelle</b>	Central Bank of France	<b>Willie Myburgh</b>	Development Bank of Southern Africa
<b>Luan Ferreira</b>	Deloitte	<b>Suchitra Nair</b>	Deloitte



# Contributors

The project team would like to express their gratitude to the following subject matter experts who contributed valuable perspectives through interviews and by participating in workshop and roundtable discussions (in alphabetical order):

<b>Aditya Narain</b>	International Monetary Fund	<b>Jonathan Welburn</b>	RAND Corporation
<b>Harish Natarajan</b>	The World Bank	<b>Danielle Winandy</b>	BNP Paribas
<b>Ali Niknam</b>	Bunq	<b>Zhang Yi</b>	Ant Group
<b>Pinar Ozcan</b>	Saïd Business School, Oxford University		
<b>Diana Paredes</b>	Suade		
<b>Nick Pastoressa</b>	Credit Benchmark		
<b>Anju Patwardhan</b>	CE Innovation Capital		
<b>Marc Pavese</b>	Lord Abbett		
<b>Miles Pelham</b>	Diginex Solutions		
<b>Jean-Louis Perrier</b>	Africa Cybersecurity Resource Centre		
<b>Thomas Pologruto</b>	Blackstone		
<b>Christina Qi</b>	Databento		
<b>Oleksiy Rachok</b>	Aegon		
<b>Antonio Ribeiro</b>	Mubadala Investment Company		
<b>Alexander Richards</b>	OakNorth		
<b>Martin Schmalz</b>	Saïd Business School, Oxford University		
<b>James Shafe</b>	Monzo Bank		
<b>Vikram Sharma</b>	QuintessenceLabs		
<b>Mariana Simão</b>	LexisNexis Risk Solutions		
<b>Susan Slocum</b>	Reserve Bank of Australia		
<b>Yefei Song</b>	Ant Group		
<b>Nathan Stevenson</b>	Forwardlane		
<b>Carrie Suen</b>	Ant Group		
<b>Lukasz Szpruch</b>	The Alan Turing Institute		
<b>Marcelo Tardelli</b>	Banco Bradesco		

# Endnotes

---

# Endnotes

1. Fernando, Roshen, et al., "Global economic impacts of climate shocks, climate policy, and changes in climate risk assessment", *Brookings Institution*, 31 March 2021, <https://www.brookings.edu/research/global-economic-impacts-of-climate-shocks-climate-policy-and-changes-in-climate-risk-assessment/>.
2. Chouinard, Tommy, "Hydro-Québec guards against a Russian cyberattack", *Actual News Magazine*, April 2022, <https://actualnewsmagazine.com/english/cybersecurity-hydro-quebec-guards-against-a-russian-cyberattack/>.
3. "3 talent trends BFSI employers need to supercharge digital skills acquisition and retention", *Randstad Sourceright*, 21 February 2023, [https://insights.randstadsourceright.com/banking-financial-services/talent-trends-banking-finance?utm\\_medium=referral&utm\\_source=PR&utm\\_campaign=Global\\_2022\\_TTR\\_Finance](https://insights.randstadsourceright.com/banking-financial-services/talent-trends-banking-finance?utm_medium=referral&utm_source=PR&utm_campaign=Global_2022_TTR_Finance).
4. Boushey, Heather, et al., "New Tools Needed to Assess Climate-Related Financial Risk", *The White House Council of Economic Advisors*, 3 November 2021, <https://www.whitehouse.gov/cea/written-materials/2021/11/03/new-tools-needed-to-assess-climate-related-financial-risk-2/>.
5. "Financial Data Aggregators Are Paving the Future of Financial Services", *Finicity Blog*, 26 February 2021, <https://www.finicity.com/blog/financial-aggregators-future-of-financial-services/>.
6. "Mastercard and Interos launch partnership to address fast-changing global risk landscape", *Mastercard*, 12 April 2022, <https://www.mastercard.com/news/press/2022/april/mastercard-and-interos-launch-partnership-to-address-fast-changing-global-risk-landscape/>.
7. Mordor Intelligence, "Deepfake content on the internet is growing at the rate of a whopping 400% year on year", *GlobeNewswire*, 27 October 2022, <https://www.globenewswire.com/en/news-release/2022/10/27/2542944/0/en/Deepfake-content-on-the-internet-is-growing-at-the-rate-of-a-whopping-400-year-on-year.html>.
8. Tuttle, Kerry and Jessica Bettencourt, "VMware Report Warns of Deepfake Attacks and Cyber Extortion", *Business Wire*, 8 August 2022, <https://www.businesswire.com/news/home/20220808005186/en/VMware-Report-Warns-of-Deepfake-Attacks-and-Cyber-Extortion>.
9. Bateman, Jon, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios", *Carnegie Endowment for International Peace*, 8 July 2020, <https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237>.
10. Grounds, Kelly and Madelyn Koff, "Disinformation, Disruption, and the Shifting Media Ecosystem in the 2022 Philippines Election", *Asia Pacific Foundation of Canada*, 5 May 2022, <https://www.asiapacific.ca/publication/election-watch-philippines-dispatch-4-social-media-use>.
11. "The 2022 Code of Practice on Disinformation", *European Commission*, 16 June 2022, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.
12. Pratap, Aayushi, "Deepfake Epidemic Is Looming—And Adobe Is Preparing For The Worst", *Forbes*, 29 June 2022, <https://www.forbes.com/sites/aayushipratap/2022/06/29/deepfake-epidemic-is-looming-and-adobe-is-preparing-for-the-worst/?sh=32bf6cbf5b81>.
13. Suntinger, Hildegard, "AI identifies fake news in seconds with complete transparency", *Innovation Origins*, 15 November 2022, <https://innovationorigins.com/en/ai-identifies-fake-news-in-seconds-with-complete-transparency/>.
14. Market Research Future, "Identity Verification Market Valuation is Expected to Garner USD 21.9 Billion by 2026 at 37.29% CAGR", *GlobeNewswire*, 26 July 2021, <https://www.globenewswire.com/en/news-release/2021/07/26/2268886/0/en/Identity-Verification-Market-Valuation-is-Expected-to-Garner-USD-21-9-Billion-by-2026-at-37-29-CAGR-Report-by-Market-Research-Future-MRFR.html>.
15. Butterfill, James, "Volume 112: Digital Asset Fund Flows Weekly Report", *Coinshares Blog*, 4 January 2023, <https://blog.coinshares.com/volume-112-digital-asset-fund-flows-weekly-report-e00679d7fea6>.
16. Pechman, Marcel, "Bitcoin aims for \$25K as institutional demand increases and economic data soothes investor fears", *Cointelegraph*, 30 January 2023, <https://cointelegraph.com/news/bitcoin-aims-for-25k-as-institutional-demand-increases-and-economic-data-soothes-investor-fears>.
17. Robinson, Edward, "Why the Crypto World Should Embrace the Feds' Crackdown", *Institutional Investor*, 23 February 2023, <https://www.institutionalinvestor.com/article/b8xkpx75k74k2y/Why-the-Crypto-World-Should-Embrace-the-Feds-Crackdown>.

18. Szalay, Eva, "Crypto exchanges' multiple roles raise conflict worries", *Financial Times*, 14 November 2021, <https://www.ft.com/content/8b8e6d72-b1d2-435c-88c1-4611e3a98da5>.
19. European Securities and Markets Authority, *Crypto-assets and their risks for financial stability*, 4 October 2022, [https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251\\_crypto\\_assets\\_and\\_financial\\_stability.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf).
20. Canny, Will, "Citi Says Decentralized Crypto Exchanges Are Gaining Market Share From Centralized Peers", *CoinDesk*, 3 October 2022, <https://www.coindesk.com/business/2022/10/03/citi-says-decentralized-crypto-exchanges-are-winning-market-share-from-centralized-peers/>.
21. Canny, Will, "Goldman Sachs Says DeFi's Interconnections Can Increase Systemic Risk", *CoinDesk*, 23 May 2022, <https://www.coindesk.com/markets/2022/05/23/goldman-sachs-says-defis-interconnections-can-increase-systemic-risk/>.
22. Wiley, Blair, "FTX's crypto crisis would not have happened under Canada's regulatory framework", *The Globe and Mail*, 17 November 2022, <https://www.theglobeandmail.com/business/commentary/article-ftx-crypto-crisis-canada-regulation/>.
23. Uppal, Rachna, "Binance CEO Zhao: Significant interest in crypto industry recovery fund", *Reuters*, 16 November 2022, <https://www.reuters.com/technology/binance-ceo-zhao-significant-interest-crypto-industry-recovery-fund-2022-11-16/>.
24. Vigliarolo, Brandon, "DeFi credit scores: Coming soon to a blockchain near you", *The Register*, 25 August 2022, [https://www.theregister.com/2022/08/25/defi\\_credit\\_scores\\_blockchain/](https://www.theregister.com/2022/08/25/defi_credit_scores_blockchain/).
25. Gogo, Jeffrey, "Decentralized Credit Scores: Polygon Looks to Disrupt Market With Its New Identity System", *BeInCrypto*, 17 November 2022, <https://beincrypto.com/polygon-looks-to-disrupt-market-with-its-new-id-system/>.
26. Stevens, Robert, "Proof of Reserves Explained", *CoinDesk*, 10 February 2023, <https://www.coindesk.com/learn/proof-of-reserves-could-it-have-prevented-the-ftx-meltdown/>.
27. Dagher, Gaby G. et al., "Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges", *Stanford University and Concordia University*, 26 October 2015, <https://eprint.iacr.org/2015/1008.pdf>.
28. "Cryptocurrency News: Big Eyes Top Crypto Experts' Watchlists Alongside Cosmos And Thorchain", *Bitcoinist*, October 2022, <https://bitcoinist.com/cryptocurrency-news-big-eyes-top-crypto-experts-watchlists-alongside-cosmos-and-thorchain/>.
29. Thuo, Charles, "CACHE Gold integrates Chainlink Proof of Reserve on Polygon mainnet", *CoinJournal*, 11 October 2022, <https://coinjournal.net/news/cache-gold-integrates-chainlink-proof-of-reserve-on-polygon-mainnet/>.
30. McGirk, James, "Anyone Can Start a Hedge Fund: How On-Chain Credit Changes the Crypto Economy", *CoinDesk*, 25 October 2022, <https://www.coindesk.com/layer2/2022/10/24/anyone-can-start-a-hedge-fund-how-on-chain-credit-changes-the-crypto-economy/>.
31. "What is KYC in crypto?", *Veriff*, 26 July 2022, <https://www.veriff.com/blog/what-is-kyc-in-crypto>.
32. Schwartz, Leo, "Financial services giant Plaid makes first foray into crypto", *Fortune Crypto*, 20 October 2022, <https://fortune.com/crypto/2022/10/20/financial-services-giant-plaid-makes-first-foray-into-crypto/>.
33. "The Evolution of Retail Investment Activity", *Chicago Board Options Exchange*, 12 September 2022, <https://www.cboe.com/insights/posts/the-evolution-of-retail-investment-activity/>.
34. Li, Yun, "The \$300 billion meme stock that makes GameStop look like child's play", *CNBC*, 3 August 2022, <https://www.cnbc.com/2022/08/03/the-300-billion-meme-stock-that-makes-gamestop-look-like-childs-play.html>.
35. U.S. Securities and Exchange Commission, *Staff Report on Equity and Options Market Structure Conditions in Early 2021*, 14 October 2021, <https://www.sec.gov/files/staff-report-equity-options-market-struction-conditions-early-2021.pdf>.
36. Smialek, Jeanna, "The Fed warns of social media 'echo chambers' that pump up meme stocks", *The New York Times*, 8 November 2021, <https://www.nytimes.com/2021/11/08/business/fed-meme-stocks-social-media-volatility.html>.

37. Smialek, Jeanna, "The Fed warns of social media 'echo chambers' that pump up meme stocks", *The New York Times*, 8 November 2021, <https://www.nytimes.com/2021/11/08/business/fed-meme-stocks-social-media-volatility.html>.
38. Farrell, Maureen et al., "How One of Switzerland's Oldest Banks Became a Meme Stock", *The New York Times*, 17 October 2022, <https://www.nytimes.com/2022/10/17/business/credit-suisse-meme-stock.html>.
39. Smialek, Jeanna, "The Fed warns of social media 'echo chambers' that pump up meme stocks", *The New York Times*, 8 November 2021, <https://www.nytimes.com/2021/11/08/business/fed-meme-stocks-social-media-volatility.html>.
40. Gawai, Harsh et al., "It's more than memes: User risk appetite and app enjoyment predict simulated mobile trading app behavior", *Dalhousie University*, October 2022, <https://aisel.aisnet.org/confirm2022/16/>.
41. Barber, Brad M. et al., "Attention-Induced Trading and Returns: Evidence from Robinhood Users", *Journal of Finance*, October 2021, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3715077](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715077).
42. DataReportal, *Social Media Usage by Country* [Graph], <https://www.oberlo.ca/statistics/social-media-usage-by-country>.
43. Wirz, Matt, "Meme-Stock Traders Embrace Avaya Despite Wall Street Fears", *The Wall Street Journal*, 19 September 2022, <https://www.wsj.com/articles/meme-stock-traders-embrace-avaya-despite-wall-street-fear-s-11663540636>.
44. "Democratizing Access to Financial Literacy For All", *Robinhood Blog*, 29 April 2022, <https://blog.robinhood.com/news/2022/4/29/democratizing-access-to-financial-literacy-for-all>.
45. Estrada, Sheryl, "An entertainment company is using Twitter Spaces for its next earnings call—with 'Litquidity' as the moderator", *Fortune*, 25 April 2022, <https://fortune.com/2022/04/25/entertainment-company-twitter-spaces-earnings-call/>.
46. "MEME ETF Launches", *Roundhill Investments*, 8 December 2021, <https://www.prnewswire.com/news-releases/meme-etf-launches-301439814.html>.
47. Smith, Connor, "Robinhood Reveals Its Users Love Tesla, Big Tech and Meme Stocks. Go Figure", *Barron's*, 9 September 2022, <https://www.barrons.com/articles/robinhood-stock-index-51662742174>.
48. Fletcher, Laurence and Madison Darbyshire, "Hedge funds rethink tactics after \$12bn hit from meme stock army", *Financial Times*, 25 June 2021, <https://www.ft.com/content/dcd86860-09ed-420e-a5cc-d6d281863c03>.
49. The Sunday Investor, "MEME ETF: A Mistake That Will Likely End Badly", *Seeking Alpha*, 10 December 2021, <https://seekingalpha.com/article/4474611-meme-etf-a-mistake-that-will-likely-end-badly>.
50. "KBC introduces smart investment assistant Matti", *NS Banking*, 21 January 2020, <https://www.nsbanking.com/news/kbc-matti/>.
51. Iannone, Olivia, "Real-time vs batch data pipelines: a comprehensive introduction", *Estuary*, 7 September 2021, <https://www.estuary.dev/real-time-and-batch-data-processing-an-introduction/>.
52. Ibid.
53. Wolinsky, Jacob, "How One Hedge Fund Manager Is Using The Retail Investing Frenzy To Turn A Profit", *Forbes*, 24 January 2022, <https://www.forbes.com/sites/jacobwolinsky/2022/01/24/how-one-hedge-fund-manager-is-using-the-retail-investing-frenzy-to-turn-a-profit/?sh=3d3bb8901921>.
54. "Navigating the alt-data avalanche", *Hedgeweek*, 27 April 2022, <https://www.hedgeweek.com/2022/04/27/314114/navigating-alt-data-avalanche>.
55. Pitaro, Vincent, *Survey Finds Widespread and Growing Use of Alternative Data*, Hedge Fund Law Report, 27 January 2022, [https://www.lowenstein.com/media/7657/hflr\\_survey-finds-widespread-and-growing-use-of-alternative-data.pdf](https://www.lowenstein.com/media/7657/hflr_survey-finds-widespread-and-growing-use-of-alternative-data.pdf).
56. Duguet, Gaspard, "How technological innovation has disrupted the commodity trading industry", *TechNative*, 24 March 2022, <https://technative.io/how-technological-innovation-has-disrupted-the-commodity-trading-industry/>.
57. Reinsel, David et al., *The Digitization of the World From Edge to Core*, International Data Corporation and Seagate Technology, 2018, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>.

58. Shekari, Tohid et al., "MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets", *Association for Computer Machinery*, 13 November 2021, <https://dl.acm.org/doi/10.1145/3460120.3484581>.
59. Kovacs, Eduard, "High-Wattage IoT Botnets Can Manipulate Energy Market: Researchers", *SecurityWeek*, 5 August 2020, <https://www.securityweek.com/high-wattage-iot-botnets-can-manipulate-energy-market-researchers/>.
60. Mode, Gautam Raj et al., "False Data Injection Attacks in Internet of Things and Deep Learning enabled Predictive Analytics", *University of Missouri*, 13 December 2019, <https://arxiv.org/pdf/1910.01716.pdf#:~:text=In%20false%20data%20injection%20attack,to%20the%20sensor%20output%20undetected>.
61. Swinhoe, Dan, "Why fake data is a serious IoT security concern", *CSO Online*, 7 November 2018, <https://www.csoonline.com/article/3318569/why-fake-data-is-a-serious-iot-security-concern.html>.
62. Morrison, Ryan, "Hackers increasingly targeting Internet of Things devices", *Tech Monitor*, 26 October 2022, <https://techmonitor.ai/technology/cybersecurity/hackers-targeting-internet-of-things-devices>.
63. Layton, Roslyn, "Round Up Of New Reports On OpenRAN Security", *Forbes*, 26 October 2022, <https://www.forbes.com/sites/roslynlayton/2022/10/26/round-up-of-new-reports-on-openran-security/?sh=61d5c311258a>.
64. Shah, Neil, "Fragmentation, Consolidation Mark Changing IoT Landscape", *Counterpoint Research*, 16 December 2022, <https://www.counterpointresearch.com/fragmentation-consolidation-mark-changing-iot-landscape/>.
65. Purdy, Kevin, "Everything we know about the White House's IoT security labeling effort", *Ars Technica*, 20 October 2022, <https://arstechnica.com/gadgets/2022/10/everything-we-know-about-the-white-houses-iot-security-labeling-effort/>.
66. U.S. Securities and Exchange Commission, *2022 Examination Priorities*, 2022, <https://www.sec.gov/files/2022-exam-priorities.pdf>.
67. "Quantropi makes history by quantum-securely distributing true random numbers over vast distances using existing network infrastructure", *Quantropi*, 26 August 2021, <https://www.quantropi.com/quantropi-makes-history-by-quantum-securely-distributing-true-random-numbers-over-vast-distances-using-existing-network-infrastructure/>.
68. Bathgate, Rory, "VMware brings XDR capabilities to Carbon Black in a push for lateral security", *ITPro*, 9 November 2022, <https://www.itpro.co.uk/security/network-security/369481/vmware-brings-xdr-to-carbon-black-push-lateral-security>.
69. Yousefnezhad, Narges et. al "Automated IoT Device Identification Based on Full Packet Information Using Real-Time Network Traffic", *National Center for Biotechnology Information*, 10 April 2021, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8069928/>.
70. Ibid.
71. Camilo, Erica, "Portnox Debuts First Cloud-Native IoT Fingerprinting and Profiling Solution", *Business Wire*, 12 October 2022, <https://www.businesswire.com/news/home/20221012005038/en/Portnox-Debuts-First-Cloud-Native-IoT-Fingerprinting-and-Profiling-Solution>.
72. Howcroft, Elizabeth, "Analysis: Buy Now Pay Later business model faces test as rates rise", *Reuters*, 10 June 2022, <https://www.reuters.com/technology/buy-now-pay-later-business-model-faces-test-rates-rise-2022-06-10/>.
73. Das, Neelanjit, "High Use Of BNPL By Gen-Z Shoppers Dictates E-Commerce Trends", *Outlook India*, 7 April 2022, <https://www.outlookindia.com/business/high-use-of-bnpl-by-gen-z-shoppers-dictates-e-commerce-trends-news-189911>.
74. PayPal, "For Retailers, a Direct Link from 'Buy Now, Pay Later' to the Bottom Line", *Harvard Business Review*, 21 June 2022, <https://hbr.org/sponsored/2022/06/for-retailers-a-direct-link-from-buy-now-pay-later-to-the-bottom-line>.

75. Kapron, Zennon, "Buy Now Pay Later In Asia: The Drivers And Issues", *Forbes*, 2 November 2022, <https://www.forbes.com/sites/zennonkapron/2022/11/02/buy-now-pay-later-in-asia-the-drivers-and-issues/?sh=5323796226c3>.
76. "Barclays calls for more robust regulation of all buy-now-pay-later products", *Barclays*, 14 February 2022, <https://home.barclays/news/press-releases/2022/02/-barclays-calls-for-more-robust-regulation-of-all-buy-now-pay-la/>.
77. Paterson, Doug and Volker Laeger, "Buy Now, Pay Later Securitizations: What Are The Risks?", *S&P Global Ratings*, 9 March 2022, <https://www.spglobal.com/ratings/en/research/articles/220309-buy-now-pay-later-securitizations-what-are-the-risks-12297760#ContactInfo>.
78. Cohan, Peter, "Stock Down 93%, Affirm's BNPL Model Suffers As Funding Costs Rise", *Forbes*, 22 June 2022, <https://www.forbes.com/sites/petercohan/2022/06/22/stock-down-93-affirms-bnpl-model-suffers-as-funding-costs-rise/?sh=65e266512d37>.
79. Sevim, Nurdan et al., "The effects of financial literacy on the borrowing behaviour of Turkish financial consumers", *International Journal of Consumer Studies*, 21 August 2012, <https://onlinelibrary.wiley.com/doi/10.1111/j.1470-6431.2012.01123.x>.
80. "Reply to Parliamentary Question on Buy Now Pay Later Loans", *Monetary Authority of Singapore*, 21 September 2022, <https://www.mas.gov.sg/news/parliamentary-replies/2022/reply-to-parliamentary-question-on-bnpl>.
81. "FCA warns Buy Now Pay Later firms about misleading adverts", *Financial Conduct Authority*, 19 August 2022, <https://www.fca.org.uk/news/press-releases/fca-warns-buy-now-pay-later-firms-about-misleading-adverts>.
82. "Reply to Parliamentary Question on Buy Now Pay Later Loans", *Monetary Authority of Singapore*, 21 September 2022, <https://www.mas.gov.sg/news/parliamentary-replies/2022/reply-to-parliamentary-question-on-bnpl>.
83. Hintze, John, "Buy-Now-Pay-Later and Alternative Data Bring Disruption to Retail Credit", *Global Association of Risk Professionals*, 14 October 2022, <https://www.garp.org/risk-intelligence/credit/buy-now-pay-later-221014>.
84. "AFIA Buy Now Pay Later (BNPL) Code of Practice", *Australian Finance Industry Association*, 1 March 2021, <https://afia.asn.au/AFIA-Buy-Now-Pay-Later-Code-of-Practice#:~:text=AFIA%27s%20BNPL%20Code%20of%20Practice,sector%20and%20strengthening%20consumer%20protections>.
85. "'Buy Now, Pay Later' Credit Reporting", *Equifax*, 9 May 2022, <https://www.equifax.com/newsroom/all-news/-/story/-buy-now-pay-later-credit-reporting/>.
86. "Zilch Continues to Lead Responsible Lending in the Payments and BNPL Space", *Business Wire*, 7 April 2022, <https://www.businesswire.com/news/home/20220406006039/en/Zilch-Continues-to-Lead-Responsible-Lending-in-the-Payments-and-BNPL-Space>.
87. Paterson, Doug and Volker Laeger, "Buy Now, Pay Later Securitizations: What Are The Risks?", *S&P Global Ratings*, 9 March 2022, <https://www.spglobal.com/ratings/en/research/articles/220309-buy-now-pay-later-securitizations-what-are-the-risks-12297760#ContactInfo>.
88. "Central bank digital currencies: foundational principles and core features", *Bank for International Settlements*, 9 October 2020, <https://www.bis.org/publ/othp33.pdf>.
89. "Central Bank Digital Currency Tracker", *Atlantic Council*, December 2022, <https://www.atlanticcouncil.org/cbdctracker/>.
90. "Blockchain & Distributed Ledger Technology (DLT)", *The World Bank*, 12 April 2018, <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt>.
91. Minwalla, Cyrus, "Security of a CBDC", *Bank of Canada*, June 2020, <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/>.
92. Fanti, Giulia et al., "Missing Key: The challenge of cybersecurity and central bank digital currency", *Atlantic Council*, 15 June 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/>.

93. Stewart, Jeff, "ProgressSoft: Offline Use in Central Bank Digital Currencies - Between a Rock and a Hard Place", *Central Bank Payments News*, 23 August 2022, <https://cbpn.currencyresearch.com/blog/2022/08/23/between-a-rock-and-a-hard-place-offline-use-in-central-bank-digital-currencies>.
94. Fanti, Giulia et al., "Missing Key: The challenge of cybersecurity and central bank digital currency", *Atlantic Council*, 15 June 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/>.
95. Bank for International Settlements, *BIS Innovation Hub announces new projects and expands cyber security and green finance experiments* [Press release], 17 June 2022, <https://www.bis.org/press/p220617.htm>.
96. Wintermeyer, Lawrence and Marcos Allende Lopez, "CBDCs, DEFI, And Web 3.0 Must Prepare Now For The Coming Quantum Cyber Threat", *Global Leaders Today*, 14 December 2022, <https://globalleaderstoday.online/cbdcs-defi-and-web-3-0-must-prepare-now-for-the-coming-quantum-cyber-threat/>.
97. National Institute of Standards and Technology, *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms* [Press release], 5 July 2022, <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>.
98. National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, 2002, <https://csrc.nist.gov/publications/detail/fips/140/2/final>.
99. "PCI DSS Requirements: What Your Business Needs to Know", *Security Boulevard*, 28 February 2023, <https://securityboulevard.com/2023/02/pci-dss-requirements-what-your-business-needs-to-know/>.
100. Minwalla, Cyrus, "Security of a CBDC", *Bank of Canada*, June 2020, <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/>.
101. Mearian, Lucas, "Sharding: What it is and why many blockchain protocols rely on it", *Computerworld*, 28 January 2019, <https://www.computerworld.com/article/3336187/sharding-what-it-is-and-why-so-many-blockchain-protocols-rely-on-it.html>.
102. Buterin, Vitalik, "Why sharding is great: demystifying the technical properties", *Vitalik Buterin's website*, 7 April 2021, <https://vitalik.ca/general/2021/04/07/sharding.html>.
103. Gu, Michael, "Ethereum 2.0 – Here's what you NEED to know", *Boxmining*, 2 February 2023, <https://boxmining.com/ethereum-2/>.
104. Teboul, Luc and Angelos Anastasiou, *The Embedded Finance Journey: Innovation That Differentiates the Customer Experience*, Goldman Sachs, 2022, <https://www.goldmansachs.com/what-we-do/transaction-banking/insights/baas.pdf>.
105. "Banking-as-a-service: a \$38B industry in five years?", *Banking Exchange*, 3 October 2022, <https://m.bankingexchange.com/news-feed/item/9439-banking-as-a-service-a-38b-industry-in-five-years?Itemid=424#:~:text=The%20banking%2Das%2Da%2D,than%20%2438%20billion%20by%202027>.
106. "Security Frame: Input Validation | Mitigations" *Microsoft Learn*, 20 December 2022, <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-input-validation>.
107. "Bean Validation", *IBM*, 13 February 2023, <https://www.ibm.com/docs/en/was-nd/8.5.5?topic=validation-bean>.
108. "Input Validation Cheat Sheet", *Open Worldwide Application Security Project*, 2021, [https://cheatsheetseries.owasp.org/cheatsheets/Input\\_Validation\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html).
109. "Network Segmentation Using Zones", *Palo Alto Networks*, 13 February 2023, <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/network-segmentation-using-zones>.
110. "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks", *Office of the Comptroller of the Currency*, 27 August 2021, <https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-40.html>.
111. Misra, Kamal, "Turn up the BaaS: How banks are rising to the occasion to embrace a discerning business model", *Finextra*, 19 February 2023, <https://www.finextra.com/blogposting/23773/turn-up-the-baas-how-banks-are-rising-to-the-occasion-to-embrace-a-discerning-business-model>.



112. Farao, Esteban, "How Artificial Intelligence Will Drive the Future of Penetration Testing in IT Security", *ERMPProtect*, 24 October 2022, <https://ermprotect.com/blog/how-artificial-intelligence-will-drive-the-future-of-penetration-testing/>.
113. Froehlich, Andrew, "AI pen testing promises, delivers both speed and accuracy", *TechTarget*, April 2020, <https://www.techtarget.com/searchsecurity/tip/AI-pen-testing-promises-delivers-both-speed-and-accuracy>.
114. New York State Department of Financial Services, *Cybersecurity requirements for financial services companies*, 2017, [https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity\\_Requirements\\_Financial\\_Services\\_23NYCRR500.pdf](https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf).
115. President's Working Group on Financial Markets and Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, *Report on Stablecoins*, 2021, [https://home.treasury.gov/system/files/136/StableCoinReport\\_Nov1\\_508.pdf](https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf).
116. Liao, Gordon Y. and John Caramichael, *Stablecoins: Growth Potential and Impact on Banking*, Board of Governors of the Federal Reserve System, 2022, <https://www.federalreserve.gov/econres/ifdp/files/ifdp1334.pdf>.
117. De Best, Raynor, "Market capitalization of the 10 biggest stablecoins from January 2017 to June 19, 2022", *Statista*, 29 June 2022, <https://www.statista.com/statistics/1255835/stablecoin-market-capitalization/>.
118. "Stablecoins by Market Cap and Volume", Coincodex, February 2023, <https://coincodex.com/cryptocurrencies/sector/stablecoins/>.
119. "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements", *Financial Stability Board*, 7 October 2021, <https://www.fsb.org/2021/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements-progress-report-on-the-implementation-of-the-fsb-high-level-recommendations/>.
120. Chipolina, Scott, "Stablecoin issuers hold \$80bn of short-dated US government debt", *Financial Times*, 20 August 2022, <https://www.ft.com/content/ab02119a-7696-4292-a2f6-578a13469992>.
121. Faux, Zeke and Muyao Shen, "A \$60 Billion Crypto Collapse Reveals a New Kind of Bank Run", *Bloomberg*, 19 May 2022, <https://www.bloomberg.com/news/articles/2022-05-19/luna-terra-collapse-reveal-crypto-price-volatility>.
122. President's Working Group on Financial Markets and Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, *Report on Stablecoins*, 2021, [https://home.treasury.gov/system/files/136/StableCoinReport\\_Nov1\\_508.pdf](https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf).
123. HM Treasury, *UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets*, 2022, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1088774/O-S\\_Stablecoins\\_consultation\\_response.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088774/O-S_Stablecoins_consultation_response.pdf).
124. DiCamillo, Nate, "US FDIC Said to Be Studying Deposit Insurance for Stablecoins", *CoinDesk*, 6 October 2021, <https://www.coindesk.com/policy/2021/10/06/us-fdic-said-to-be-studying-deposit-insurance-for-stablecoins/>.
125. Harris, Adrienne A., "Guidance on the Issuance of U.S. Dollar-Backed Stablecoins", *New York State Department of Financial Services*, 8 June 2022, [https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/il20220608\\_issuance\\_stablecoins](https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220608_issuance_stablecoins).
126. Lim, Shawn, "Crypto ad ban in Singapore: How have platforms changed their marketing strategy?", *Campaign*, 11 August 2022, <https://www.campaignasia.com/article/crypto-ad-ban-in-singapore-how-have-platforms-changed-their-marketing-strategy/480923>.
127. Nguyen, Anuchit, "Thailand Tightens Crypto Advertising Rules After Market Rout", *Bloomberg*, 1 September 2022, <https://www.bloomberg.com/news/articles/2022-09-01/thailand-tightens-crypto-advertisement-rules-after-zipmex-freeze>.
128. Lang, Hannah, "U.S. Treasury Launches Campaign to Educate Public About Crypto Risks", *Reuters*, 10 March 2022, <https://money.usnews.com/investing/news/articles/2022-03-10/u-s-treasury-launches-campaign-to-educate-public-about-crypto-risks>.

129. Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf>.
130. Auer, Raphael, *Embedded Supervision: How to Build Regulation into Blockchain Finance*, Federal Reserve Bank of Dallas, October 2019, <https://www.dallasfed.org/~media/documents/institute/wpapers/2019/0371.pdf>.
131. Auer, Raphael, *Embedded supervision: how to build regulation into decentralised finance*, Bank for International Settlements, September 2019, <https://www.bis.org/publ/work811.pdf>.
132. "Study on Embedded Supervision of Decentralised Finance", *European Commission*, 28 September 2022, <https://ted.europa.eu/udl?uri=TED:NOTICE:542418-2022:TEXT:EN:HTML>.
133. Da Costa, Rick and Gordon Goodman, "The One Where Insurance meets Blockchain and Parametrics", *Cassels*, 14 April 2022, <https://cassels.com/insights/the-one-where-insurance-meets-blockchain-and-parametrics/>.
134. Capgemini Consulting, *Smart Contracts in Financial Services: Getting from Hype to Reality*, 2017, [https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart\\_contracts\\_paper\\_long\\_0.pdf](https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf).
135. Allianz and Nephila, *Blockchain technology successfully piloted by Allianz Risk Transfer and Nephila for catastrophe swap* [Press release], 15 June 2016, [https://www.allianz.com/content/dam/onemarketing/azcom/Allianz.com/migration/media/press/document/Press\\_Release\\_ART\\_Blockchain\\_pilot\\_final.pdf](https://www.allianz.com/content/dam/onemarketing/azcom/Allianz.com/migration/media/press/document/Press_Release_ART_Blockchain_pilot_final.pdf).
136. "AXA goes blockchain with fizzy", *AXA*, 13 September 2017, <https://www.axa.com/en/news/axa-goes-blockchain-with-fizzy>.
137. Zhao, Wolfie, "\$30 Million: Ether Reported Stolen Due to Parity Wallet Breach", *CoinDesk*, 19 July 2017, <https://www.coindesk.com/markets/2017/07/19/30-million-ether-reported-stolen-due-to-parity-wallet-breach/>.
138. "Smart Contract Security Guidelines #4: Strategies for Safer Governance systems", *OpenZeppelin Security*, 12 October 2021, <https://blog.openzeppelin.com/smart-contract-security-guidelines-4-strategies-for-safer-governance-systems/>.
139. Kimpel, Scott H. and Christopher Adcock, "The State of Smart Contract Legislation", *Blockchain Legal Resource*, 5 September 2018, <https://www.blockchainlegalresource.com/2018/09/state-smart-contract-legislation/>.
140. "Top 5 Programming Languages to Build Smart Contracts", *ImmuneBytes*, 29 November 2022, <https://www.immunebytes.com/blog/top-5-programming-languages-to-build-smart-contracts/>.
141. Howell, James, "5 Best Smart Contract Auditing Companies", *101 Blockchains*, 24 November 2022, <https://101blockchains.com/best-smart-contract-auditing-companies/>.
142. "Zero-Trust Networking Enhances Security in Research and Education Environments", *Corporation for Education Network Initiatives in California*, 9 July 2019, <https://cenic.org/blog/zero-trust-networking>.
143. Maundrill, Beth, "Geopolitical Tensions Expected to Further Impact Cybersecurity in 2023", *Infosecurity*, 29 December 2022, <https://www.infosecurity-magazine.com/news/geopolitical-tensions-impact/>.
144. McMillan, Robert, "Google Sees Russia Coordinating With Hackers in Cyberattacks Tied to Ukraine War", *The Wall Street Journal*, 26 September 2022, <https://www.wsj.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801?mod=djemalertNEWS>.
145. Hill, Michael, "NATO tests AI's ability to protect critical infrastructure against cyberattacks", *CSO Online*, 5 January 2023, <https://www.csoonline.com/article/3684730/nato-tests-ai-s-ability-to-protect-critical-infrastructure-against-cyberattacks.html>.
146. Smith, Ian, "Reinsurance costs rise up to 200% as Ukraine war and extreme weather bite", *Financial Times*, 3 January 2023, <https://www.ft.com/content/f5f9d450-c539-47a7-bc5c-44a8db57e74e>.
147. Kotoulas, Yiannis, "Lloyd's of London resets systems following potential cyber attack", *Insurance Times*, 6 October 2022, <https://www.insurancetimes.co.uk/news/lloyds-of-london-resets-systems-following-potential-cyber-attack/1442579.article#:~:text=Lloyd's%20is%20a%20leading%20provider.its%20own%20standalone%20cyber%20syndicate>.

148. Hill, Michael, "Lloyd's of London to exclude state-backed attacks from cyber insurance policies", *CSO Online*, 22 August 2022, <https://www.csoonline.com/article/3670571/lloyd-s-of-london-to-exclude-state-backed-attacks-from-cyber-insurance-policies.html>.
149. Woollacott, Emma, "Should the government contribute to the costs of cyber insurance? Experts are conflicted", *Cybernews*, 8 January 2023, <https://cybernews.com/security/should-government-contribute-to-costs-of-cyber-insurance/>.
150. Smith, Ian, "Cyber attacks set to become 'uninsurable', says Zurich chief", *Financial Times*, 26 December 2022, <https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d>.
151. Muncaster, Phil, "Experts Warn ChatGPT Could Democratize Cybercrime", *Infosecurity*, 13 December 2022, <https://www.infosecurity-magazine.com/news/experts-warn-chatgpt-democratize/>.
152. Bernard, Stan, "Financial services firms have a lot to lose from a cyber attack", *Zurich Insurance Group*, 28 May 2021, <https://insights.zurichna.com/financial-services-firms-have-a-lot-to-lose-from-a-cyber-attack>.
153. Smith, Ian, "Insurer Beazley launches first catastrophe bond for cyber threats", *Financial Times*, 8 January 2023, <https://www.ft.com/content/a945d290-a7f1-427c-84a6-b0b0574f7376>.
154. "EIOPA consults on cyber component in its insurance stress testing framework", *European Insurance and Occupational Pensions Authority*, 24 November 2022, [https://www.eiopa.europa.eu/media/news/eiopa-consults-cyber-component-its-insurance-stress-testing-framework\\_en](https://www.eiopa.europa.eu/media/news/eiopa-consults-cyber-component-its-insurance-stress-testing-framework_en).
155. Plumb, Taryn, "How CyberCube helps assess risk for cyber insurance", *VentureBeat*, 19 December 2022, <https://venturebeat.com/security/how-cybercube-helps-assess-risk-for-cyber-insurance/>.
156. "CyberCube Launches World's First Exposure Databases to Enrich Cyber Modeling", *Business Wire*, 24 October 2022, <https://www.businesswire.com/news/home/20221024005548/en/CyberCube-Launches-World%E2%80%99s-First-Exposure-Databases-to-Enrich-Cyber-Modeling>.
157. Bloomberg, Jason, "Cybercrime: So Simple Anyone Can Do It", *Forbes*, 6 January 2019, <https://www.forbes.com/sites/jasonbloomberg/2019/01/06/cybercrime-so-simple-anyone-can-do-it/?sh=1e3c7735401a>.
158. Gregorio, Tracy, "Digital Twins Key to Cyber Resilient Infrastructure", *Government Technology*, 16 December 2022, <https://www.govtech.com/opinion/digital-twins-key-to-cyber-resilient-infrastructure>.
159. "Graphs for Cybersecurity: Knowledge Graph as Digital Twin", *Neo4j Blog*, 26 July 2022, <https://neo4j.com/blog/graphs-cybersecurity-knowledge-graph-digital-twin/>.
160. Hill, Michael, "NATO tests AI's ability to protect critical infrastructure against cyberattacks", *CSO Online*, 5 January 2023, <https://www.csoonline.com/article/3684730/nato-tests-ai-s-ability-to-protect-critical-infrastructure-against-cyberattacks.html>.
161. "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks", *Check Point Research*, 5 January 2023, <https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/>.
162. "Allianz: Cyber risks the most important risk globally", *Safety 4 Sea*, 27 January 2023, <https://safety4sea.com/allianz-cyber-risks-the-most-important-risk-globally/>.
163. "Cost of a data breach 2022: A million-dollar race to detect and respond", *IBM*, July 2022, <https://www.ibm.com/reports/data-breach>.
164. Harford, Isabella, "Does AI-powered malware exist in the wild? Not yet", *TechTarget*, September 2022, <https://www.techtarget.com/searchsecurity/tip/Does-AI-powered-malware-exist-in-the-wild-Not-yet#:~:text=Unlike%20malware%20that%20targets%20a,its%20victims%20and%20their%20systems>.
165. Higbee, Amy et al., "Why global harmonisation of cybersecurity would be music to everyone's ears", *World Economic Forum*, 28 March 2022, <https://www.weforum.org/agenda/2022/03/why-global-harmonisation-of-cybersecurity-regulations-would-be-like-music-to-our-ears/>.
166. "The Digital Operational Resilience Act (DORA)", *Digital Operational Resilience Act*, 27 December 2022, <https://www.digital-operational-resilience-act.com/>.
167. "Bank of Canada announces partnership to improve resilience in financial sector", *Bank of Canada*, 27 June 2019, <https://www.bankofcanada.ca/2019/06/bank-of-canada-announces-partnership-improve-resilience-financial-sector/>.

168. "Strengthening cyber resilience in the Swiss financial center", *Swiss Financial Sector Cyber Security Centre*, September 2022, <https://fscsc.ch/fr/>.
169. World Economic Forum, *The Global Risks Report 2022 17th Edition*, 2022, <https://www.weforum.org/reports/global-risks-report-2022/>.
170. World Economic Forum, *The Future of Jobs Report*, 2020, [https://www3.weforum.org/docs/WEF\\_Future\\_of\\_Jobs\\_2020.pdf?\\_gl=1\\*4osnuo\\*\\_up\\*MQ..&gclid=CjwKCAiA85efBhBbEiwAD7oLQHwybunozbsBRdjNzu0XlpRnCPYsJ8soVE\\_HgdvdL6616ktRjPnwBoCQysQAvD\\_B\\_wE](https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf?_gl=1*4osnuo*_up*MQ..&gclid=CjwKCAiA85efBhBbEiwAD7oLQHwybunozbsBRdjNzu0XlpRnCPYsJ8soVE_HgdvdL6616ktRjPnwBoCQysQAvD_B_wE).
171. Kigotho, Wachira, "North Africa hit by brain drain of ICT graduates", *University World News*, 29 April 2021, <https://www.universityworldnews.com/post.php?story=20210421131853553>.
172. JPMorgan Chase & Co, *Tech for Social Good*, 2023, <https://www.jpmorganchase.com/impact/people/mentoring-skilled-volunteerism/tech-for-social-good>
173. Cross, Miriam, "Banks address tech talent shortage with 'reskilling,' 'upskilling' programs", *12ft*, 25 June 2021, <https://12ft.io/proxy?q=https%3A%2F%2Fwww.americanbanker.com%2Fnews%2Fbanks-take-on-tech-talent-shortage-with-reskilling-upskilling-programs>.
174. Sunil, Priya, "HSBC Malaysia rolls out digital upskilling initiative for first batch of employees", *Human Resources Online*, 20 July 2021, <https://www.humanresourcesonline.net/hsbc-malaysia-rolls-out-digital-upskilling-initiative-for-first-batch-of-employees>.
175. Cruz, Eduardo, "3 reasons low code software is helping IT departments be superheroes", *App Developer Magazine*, 1 December 2016, <https://appdeveloper magazine.com/3-reasons-low-code-software-is-helping-it-departments-be-superheroes/>.
176. Balsara, Samira, "BMO to focus on closing tech talent gap by attracting diverse candidates from across Canada", *IT World Canada*, 4 August 2022, <https://o.canada.com/technology/bmo-to-focus-on-closing-tech-talent-gap-by-attracting-diverse-candidates-from-across-Canada>.
177. "Citi Global Tech Hub in Bahrain is on track to employ 1000 Bahraini coders", *Bahrain Economic Development Board*, 11 January 2023, <https://www.newswire.ca/news-releases/citi-global-tech-hub-in-bahrain-is-on-track-to-employ-1000-bahraini-coders-843222845.html>.
178. "McKinsey's Global Banking Annual Review", *McKinsey & Company*, 1 December 2022, <https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review>.
179. Wass, Sanne, "Banks risk damaging customer relationships as they address climate data gap", *S&P Global Market Intelligence*, 15 December 2022, <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/banks-risk-damaging-customer-relationships-as-they-address-climate-data-gap-73469666>.
180. "Climate Change Indicators: Weather and Climate", *United States Environment Protection Agency*, 1 August 2022, <https://www.epa.gov/climate-indicators/weather-climate#:~:text=Rising%20global%20average%20temperature%20is,with%20human%2Dinduced%20climate%20change>.
181. Dijk, Justin et al., *How proxies and publicly available data can be used to construct indicators on transition risk, physical risks and green taxonomies*, Bank for International Settlements, 2021, [https://www.bis.org/ifc/publ/ifcb56\\_27.pdf](https://www.bis.org/ifc/publ/ifcb56_27.pdf).
182. Wass, Sanne, "What US banks and their supervisors can learn from Europe's climate stress tests", *S&P Global Market Intelligence*, 18 October 2022, <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/what-us-banks-and-their-supervisors-can-learn-from-europe-s-climate-stress-tests-72517451>.
183. JPMorgan Chase & Co, *2021 Annual Report*, 2022, <https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2021.pdf>.
184. Lee, Allison Herren, "Going Dark: The Growth of Private Markets and the Impact on Investors and the Economy", *U.S. Securities and Exchange Commission*, 12 October 2021, <https://www.sec.gov/news/speech/lee-sec-speaks-2021-10-12>.
185. Bank of Canada and Office of the Superintendent of Financial Institutions, *Using Scenario Analysis to Assess Climate Transition Risk*, 2022, <https://www.bankofcanada.ca/wp-content/uploads/2021/11/BoC-OSFI-Using-Scenario-Analysis-to-Assess-Climate-Transition-Risk.pdf>.

186. "ECB publishes new climate-related statistical indicators to narrow climate data gap", *European Central Bank*, 24 January 2023, <https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230124~c83dbef220.en.html>.
187. "Climate Data Steering Committee Proposes Recommendations for the Development of First-Ever Publicly Accessible Climate Data Utility", *Net-Zero Data Public Utility*, 21 September 2022, <https://www.nzdpu.com/climate-data-steering-committee-proposes-recommendations-for-the-development-of-first-ever-publicly-accessible-climate-data-utility/>.
188. Nunez. Christina et al., "Applications for a newly developed risk and resilience tool", *Phys.org*, 8 February 2023, <https://phys.org/news/2023-02-applications-newly-resilience-tool.html>.
189. Hsu, Angel et al., "Next-Generation Digital Ecosystem for Climate Data Mining and Knowledge Discovery: A Review of Digital Data Collection Technologies", *Frontiers in Big Data*, 10 September 2020, <https://www.frontiersin.org/articles/10.3389/fdata.2020.00029/full>.

WORLD  
ECONOMIC  
FORUM

The logo for the World Economic Forum, featuring the text "WORLD ECONOMIC FORUM" in a bold, sans-serif font. A blue arc is positioned behind the text, starting from the top left of the word "WORLD" and curving around to the bottom right of the word "FORUM".