Financial Markets, Insurance and Pensions

DIGITAL TECHNOLOGIES AND FINANCE

OECD

2020

Financial Markets, Insurance and Pensions

Digital Technologies and Finance

Please cite this publication as:

OECD (2020), *Financial Markets, Insurance and Pensions: Digital Technologies and Finance,* www.oecd.org/finance/financial-markets-insurance-and-pensions-report.htm

Foreword

This is the third edition of *Financial Markets, Insurance and Pensions*. It focuses on the impact of digital technologies in the areas of financial markets, insurance and pensions. Digital technologies and finance are at the core of the work of the OECD Committee on Financial Markets, and the OECD Insurance and Private Pensions Committee. The chapters in this publication are part of the work streams of these two committees. They have benefited from comments from both committees, the G20/OECD Task Force on Financial Consumer Protection, the OECD International Network on Financial Education, and the OECD Working Party on Private Pensions

Technology and digitalisation have been transforming the way in which the financial sector is operating over the past years. The COVID-19 pandemic has accelerated the development of digital technologies in all sectors, in particular in finance, as both households and firms have increasingly relied on digital as opposed to physical services.

This publication contributes to the OECD Going Digital project, which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.

Pablo Antolin and Stéphanie Payet led the editorial team for this edition. Chapter 1 was prepared by Iota Nassr; Chapter 2 by Sebastian Schich; Chapter 3 by Mamiko Yokoi-Arai; Chapter 4 by Joel Paula; and Chapter 5 by Andrea Grifoni. The editorial team would like to thank Flore-Anne Messy for her insight and comments. Editorial and communication support by Pamela Duffin and Edward Smiley is gratefully acknowledged.

Table of contents

Tables

Figures

Boxes

Executive summary

This edition of the *Financial Markets, Insurance and Pensions* publication explores the benefits and risks that selected digital technologies and innovations bring to businesses and consumers in the areas of financial markets, insurance and pensions.

Chapter 1 examines asset tokenisation and the implications of a potential proliferation of such practice for financial markets. Asset tokenisation is the process of representing an existing asset (e.g. financial assets such as stocks and bonds, commodities such as gold, and non-financial assets such as real estate) on a distributed ledger; or of creating 'native' financial assets on the blockchain. The chapter highlights the range of benefits that tokenisation of assets may bring. It could deliver efficiency gains; increase transparency; and improve liquidity and tradability. It could also increase the participation of retail investors in previously restricted asset classes, and enhance access to finance for SMEs. The chapter also discusses hurdles in adopting tokenisation of assets at a large scale. These are related to the underlying technology itself, governance issues, digital identity, and arbitrage opportunities. Wider adoption of asset tokenisation could be considered where justified by efficiencies and related cost reductions; increases in safety, resilience and trust; reduction in complexity and disintermediation; or the absence of existing trading infrastructure for the asset. The chapter then moves to the areas of financial markets that would be most affected by tokenisation of assets, explaining the impact of the adoption of such practices in trading, pricing, and liquidity, as well as clearing and settlement of securities. Finally, the chapter highlights the need to identify and address potential gaps in legal and regulatory frameworks and provide greater clarity around the applicable regulatory frameworks.

Chapter 2 explores the implications of open banking for the structure of banking and payment systems. By requiring banks to open access to their consumers' data in a secure way, open banking initiatives facilitate the unbundling of financial services previously provided by banks, which could result in the provision of better, cheaper or more personalised financial services. However, the opening of an established payments infrastructure to (and the sharing of data with) new participants and the creation of new interlinkages creates new risks. To address these, it is crucial to develop processes, governance mechanisms and regulation in parallel to the development of new technical and data connections, as well as facilitate consumers' understanding of the actual usage of their data. In addition, the entry of Fintech and in particular Bigtech firms into financial services might have desirable effects on contestability and competition over the short term, but over the long run, there is a risk of increased concentration. Micro-prudential regulators should maximise efficiency gains stemming from their entry, while minimising the potential for these new firms to be seen as benefitting from bypassing costs and constraints of regulation.

Chapter 3 examines the benefits and risks big data and artificial intelligence (AI) bring to the insurance industry. Big data provides the ability to exploit granular and diverse data, with the potential to transform the insurance production process. However, the granularity of data can lead to the exclusion from insurance offerings for certain groups. AI application in the insurance sector can improve the efficiency of processing data and decision-making, including contracting and claims processing. However, there remain aspects of AI that raise questions related to data collection, privacy and ethical issues, as well as regulation. The chapter presents actions that policy markers may wish to consider to ensure that the

insurance sector can reap the benefits from big data and AI, while also being abreast of any unintentional consequences. These include encouraging the sector to engage actively with big data and AI, using regulatory sandboxes or innovation hubs; addressing the skill shortage; keeping abreast of developments in big data and AI; monitoring closely competition in the market; ensuring that vulnerable populations are not excluded from affordable insurance; learning from international guidelines on AI; and engaging in international cooperation.

Chapter 4 explores how blockchain, integrated with other technologies like the internet of things (IoT) and AI, could enable investment in sustainable infrastructure and accelerate a cost-effective low-carbon transition. Blockchain could enable greater standardisation in data collection, monitoring and reporting, with the aim to more effectively manage risks. In the context of sustainable infrastructure, the technology may also effectively facilitate climate mitigation and adaptation measures, especially in the energy, transport and agriculture industries, and facilitate further investment in infrastructure. The chapter provides a roadmap with steps to implement blockchain technology to enable sustainable infrastructure. It also argues that for a successful low-carbon transition enabled by blockchain technology, policy makers could focus on: supporting education and research and development; improving legal and regulatory environments; and encouraging co-innovation and collaboration.

Finally, Chapter 5 looks at the implications of using personal data in financial services from the point of view of the consumer of financial services. The chapter introduces the technological, economic and societal developments that have led to an exponential increase in personal data generation, and an improved capacity of financial services providers to capture, store, combine and analyse a much greater variety of consumer data. The positive outcomes of these developments include potentially cheaper and more relevant financial products, and access to credit for those without any traditional credit record. However, consumers may not be aware of the extent to which their data is being used, or abused. They may be marginalised because of opaque and potentially unfair data mining practices or even find themselves victims of fraud and cybercrime. The chapter calls for policy makers to address the use of personal data within financial education programmes and, in doing so, to coordinate or consult with the authorities in charge of personal data protection and financial consumer protection as well as with Fintech providers. The chapter also identifies specific financial literacy competencies that would benefit individuals and entrepreneurs in this domain, providing new elements pertaining to personal data in support of the implementation of the G20/OECD INFE Policy Guidance Note on Digitalisation and Financial Literacy.

1 Tokenisation of assets: financial market implications

Asset tokenisation has become one of the most prominent use-cases of distributed ledger technologies (DLTs) in financial markets, for assets including securities (e.g. stocks and bonds), commodities (e.g. gold) and other non-financial assets (e.g. real estate). A potential proliferation of asset tokenisation would have potential cross-cutting implications for financial market practices and participants, market infrastructure and regulators across a large range of financial instruments and asset classes.

This chapter examines the benefits of asset tokenisation and the challenges to its wider adoption; sheds light on the conditions necessary for tokenisation to be meaningful; analyses the potential disruptive effect on trading, liquidity, pricing, clearing and settlement; and discusses the policy implications of tokenisation for financial markets.

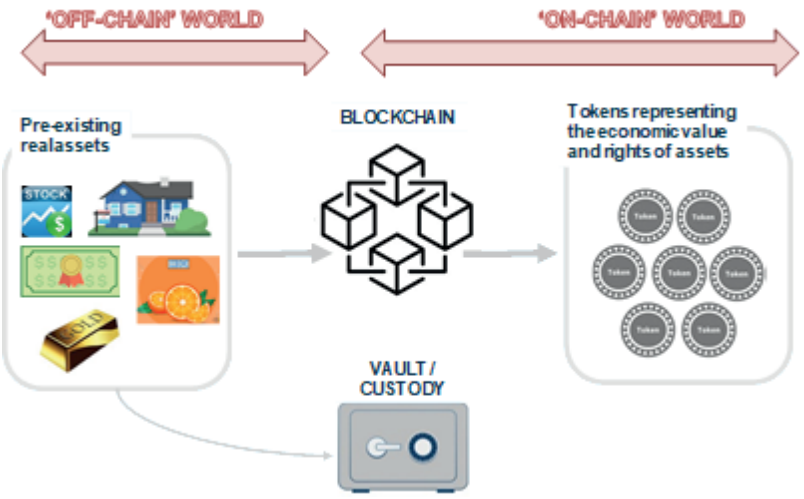
What is tokenisation of assets and why is it important?

Tokenisation of real assets that exist off-the-chain

Tokenisation is the process of digitally representing an existing real asset on a distributed ledger (Hileman and Rauchs, 2017[1]). The Financial Stability Board (FSB) defines tokenisation as the representation of traditional assets – e.g. financial instruments, a basket of collateral or real assets – on distributed ledger technology (DLT) (FSB, 2019[2]). Asset tokenisation involves the representation of pre-existing real assets on the ledger by linking or embedding by convention the economic value and rights derived from these assets into digital tokens created on the blockchain.

Tokens issued in asset tokenisation exist on the chain and carry the rights of the assets they represent, acting as store of value. The real assets on the back of which the tokens are issued continue to exist in the "off-chain" world and, in the case of physical real assets, those would typically need to be placed in custody to ensure that the tokens are constantly backed by these assets (Figure 1.1). This points to an increasingly important role of custodianship of assets in tokenisation transactions.

Figure 1.1. Tokenisation of real assets that exist off-the-chain



Source: (OECD, 2020[3]).

Communication between the "off-chain" (traditional financial market infrastructures) and "on-chain" environments is crucial for assets that continue to exist off the chain.

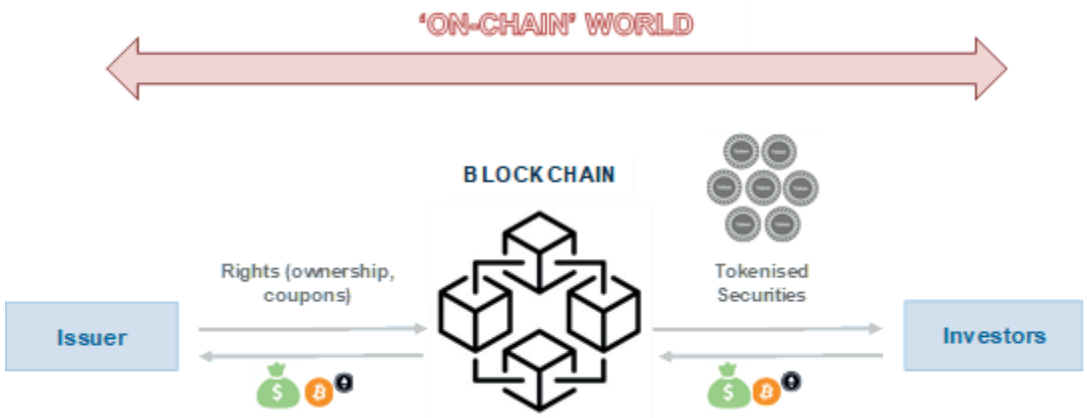
In theory, any asset can be tokenised and rights to such asset be represented on a distributed ledger. Issuance of tokens backed by fiat currencies, which is one form of "stable coins", has rapidly increased with many new stable coins being issued and with a market capitalisation that is growing. Real assets that are being tested in pilots or at concept stage involve real estate assets; commodities such as gold (e.g. https://ekon.gold/); or art. Intangible assets, such as intellectual property, could also be tokenised, creating new innovative digital assets and markets.

An easy way to understand tokenisation of assets that exist in the off-chain world is to use the parallel of a DLT-based asset-backed securitisation. Through both processes, illiquid financial assets are converted into liquid marketable securities, funded by and tradable in the capital markets.[1]

Tokenisation of assets native to the blockchain

Important distinctions need to be made between tokenised assets that exist off-the-chain and tokens that are "native" to the blockchain. "Native" tokens are built directly on-chain and live exclusively on the distributed ledger (Figure 1.2). The Bitcoin and other cryptocurrencies and payment tokens are examples of "native" tokens. "Native" tokens derive their value in and of themselves and are defined by their existence on the blockchain.

Figure 1.2. Tokenisation of assets "native" to the blockchain



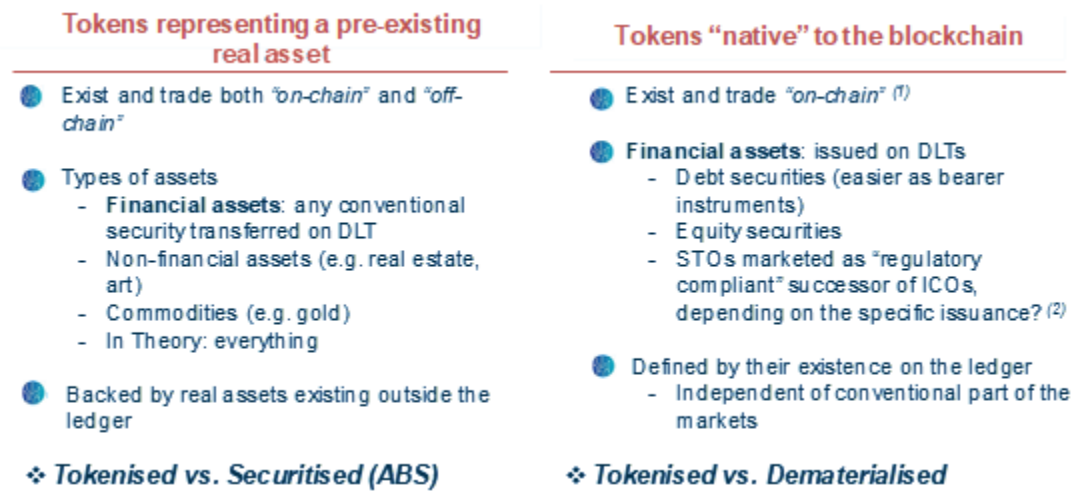
Source: (OECD, 2020[3]).

Tokens issued in initial coin offerings (ICOs) are another example of "native" tokens. ICOs consist of the creation of digital tokens by start-up companies and their distribution to investors in exchange for funds for the purposes of fundraising (OECD, 2019[4]). Tokens issued in ICOs are generated within the blockchain and are not backed by an off-chain security or other asset. This has important implications for market structure and governance, given that tokens issued in ICOs are independent of the conventional, off-chain part of the market.

Examples of tokenisation of assets native to the blockchain include tokenisation of the equity of a non-listed company, where the free float of the company is digitally represented by tokens and placed to investors on the blockchain. Such a transaction would constitute the equivalent of a digitalised on-chain private placement of securities. A similar structure would apply to private debt placements (Figure 1.3).

Investment funds and alternatives such as private equity and venture capital funds, as well as real estate investment vehicles, are also considered suitable for tokenisation given the near-total absence of liquidity of participation in such funds/vehicles.

Figure 1.3. The two types of asset tokenisation



Notes: (1) Tokens native to the blockchain can also trade between and among customers of platforms within the platforms' omnibus account. (2) STOs are marketed as more "regulatory compliant" forms of token issuances, however, such determination will only depend on the specific issuance on a case-by-case basis.
Source: (OECD, 2020[3]).

Tokenising financial assets: equity and debt

When it comes to financial assets, tokenisation of securities (equity and/or debt) is seen by the market as the sector with the most imminent potential for growth. This is mainly driven by the recent hype around tokens issued in, mostly unregulated, ICOs and the currently trending "Security Token Offerings" (STOs) and "Security Tokens". STOs have been marketed as a more "regulatory-compliant" successor of ICOs aiming to raise capital, while Security Tokens represent existing securities in secondary DLT markets. Both the above designations are self-defined by market participants and the designation of an issuance as regulatory compliant will only depend on the particular issuance on a case-by-case basis.

STOs are securities offerings consisting of the issuance of DLT-based tokens that aim to comply with the securities regulatory framework at the jurisdiction of issuance and at the jurisdictions where the offering is marketed to investors. Regulations applying to the offering and throughout the security lifecycle are digitally represented on the blockchain through programmable enforcement of ownership and trading restrictions, for instance ("programmable securities"). STOs are self-defined as there is no formally agreed classification for such token offerings. Security Tokens, also self-defined, are tokenised versions of securities that are already issued by conventional methods (existing share certificates) which aim to bring these assets onto the secondary on-chain market in digital form. Whether the issuance will be regulatory compliant does not depend on the designation/use of a particular "label" but will be determined on a case-by-case basis.

The electronification of financial markets and the use of automation for the issuance and trading of financial instruments is not new; securities have existed in electronic-only format for a long time in what is described as "dematerialised" form. Tokenised securities could be seen as a form of cryptography-enabled dematerialised securities that are based and recorded on a decentralised ledger powered by DLTs, instead of electronic book-entries in securities registries of central securities depositories. The decentralisation of tokenised securities, coupled with the ability to automatically transact and settle without trusted intermediaries, may be where most of the disruptive potential of tokenisation lies. Tokenised securities eliminate the need for the use of intermediaries or proxies in the distribution of dividends or votes, giving investors full control of the equity they own.

Depending on the jurisdiction, tokenised securities can be either directly issued on the blockchain or issued as conventional securities that are tokenised at a second stage. Direct issuance on DLTs is more straightforward for bonds, given that these are "bearer" assets on which no ownership information is recorded and whose possession accords ownership, but this will ultimately depend on the jurisdiction. Direct issuance of equities, as registered securities, is more cumbersome; the majority of current applications of equity tokenisation involve the digital representation of the rights to a share. Changes in corporate legislation would be required for equity tokens issued on DLTs to be recognised as such and not as the digital representation of share certificates.[2] The State of Delaware in the United States has updated its General Corporation Law to allow any company to issue equity in the form of a token and for tokenised stock or share to be legally admissible as evidence of ownership (Delaware State Senate, 2017[5]).

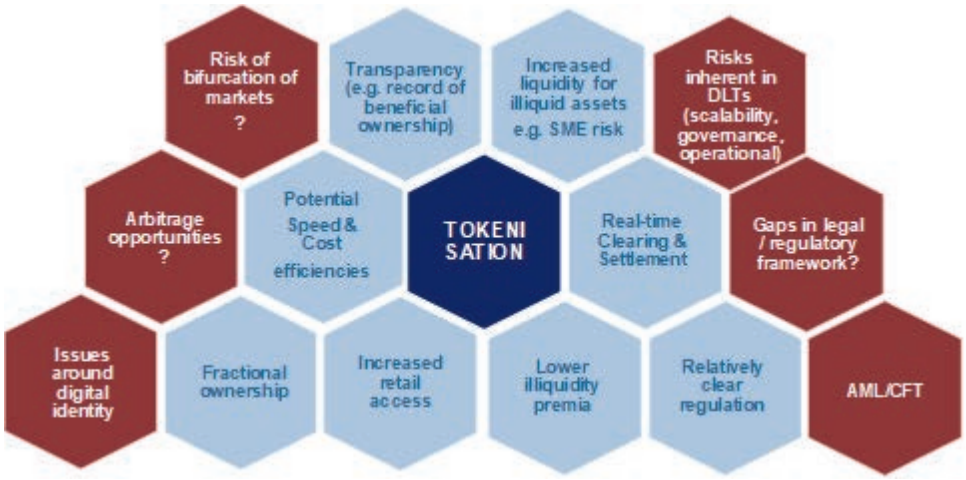
Examples of tokenised securities issued directly on the blockchain include the Ethereum-denominated bond that Nivaura issued, cleared, settled and registered on a public blockchain infrastructure using the UK Financial Conduct Authority (FCA) regulatory sandbox (Allen & Overy, 2017[6]), or the issuance, admission and trading of tokenised equity by 20/30 on the London Stock Exchange's Turquoise platform. Examples of traditional securities issued on conventional platforms and transferred on the blockchain to be tokenised include the Schuldschein bond that Daimler issued in conventional form and with the use of blockchain technology in parallel (Daimler, 2017[7]), and the tokenisation of Mt Pelerin's shares in Switzerland, in compliance with the Swiss regulatory framework. Importantly, the Mt Pelerin's shares never existed in certificated form: these were issued in book entry form and then recorded and linked to tokens.

Benefits of tokenisation and challenges to its wider adoption

Benefits of asset tokenisation

The application of DLTs in asset tokenisation may deliver *efficiency gains* through the transfer of value without the need for trusted centralised intermediaries and/or through the efficient automation of processes, resulting in faster, potentially cheaper and frictionless transactions driven by disintermediation and automation (Figure 1.4). The use of smart contracts may reduce the cost of issuing and administering securities, further reducing the cost of transactions, increasing speed of execution and streamlining transactions. Smart contracts may facilitate corporate actions (e.g. coupon or dividend payments, voting), escrow arrangements (e.g. release of funds) and collateral management (e.g. exchange of ownership interest). Custody chains typically involved in traditional securities holdings may be shortened and their transparency increased, avoiding potential liquidity problems for market participants in case of operational issues or financial distress of sub-custodians (FSB, 2019[2]).

Figure 1.4. Benefits and risks of asset tokenisation



Source: (OECD, 2020[3]).

Automation introduced in the issuance, distribution, and management of securities but also around securities servicing and corporate actions may reduce costs throughout the securities transaction lifetime, benefiting issuers and investors alike. The distributed nature of the network with no single "point of failure", the immutability of the ledger and the application of cryptography may add to the resilience and safety of the infrastructure. This of course depends on the applicable consensus mechanism and the governance model of each DLT, which may give rise to other vulnerabilities (e.g. risks of forks).

In addition to the efficiency gains driven by its disintermediation potential, asset tokenisation may bring benefits of increased *transparency* regarding transactional data and information around the issuer and the asset characteristics, through enhanced information recording and sharing.[3] The financial markets may benefit from the data integrity, immutability and security (no single point of failure, subject to consensus and governance vulnerabilities) as well as automatic auditability that are inherent to many blockchain-based systems. In addition, DLT-based security registries may provide increased transparency and a clear record of beneficial ownership with certainty at any point in time. The role of registrars/transfer agents may thus be rendered redundant and corporate/shareholder registries replaced by the decentralised ledger itself.

Increased transparency may also be achieved in terms of regulatory compliance and interactions with regulators: as programmed regulatory restrictions are automatically enforced, the regulator may be automatically notified through smart contracts when restrictions are modified or turned-off. Regulators may also have quasi-real-time information about specific on-chain events of interest to them.

It should be highlighted, however, that the quality of the data that is inputted into the blockchain is critical for the robustness of information recording and sharing. DLTs do not resolve the "garbage in, garbage out" conundrum and poor quality of data inputs (e.g. malicious or erroneous "oracles" feeding external data into the network) will result in a transparent, immutable, time-stamped repository of unsound or flawed outputs. In a tokenised world, it could be argued that there will be a need for regulated entities attesting to the accuracy of data before these are inputted onto the blockchain.

Tokenisation of assets could allow for *direct access* of investors in primary and secondary markets. ICOs were a prime example of tokens issued directly to investors on platforms/issuing venues facilitated by technology companies and without any middleman function in the traditional sense (OECD, 2019[4]). Secondary trading, however, continues to occur mostly at centralised exchanges, and pure decentralised exchanges are yet to dominate tokenised trading.

Investors who would have the possibility to hold *fractional ownership* of assets (or interest in funds) may enjoy the benefits from the wider use of assets tokenisation. Tokenisation of assets may allow for the slicing up of assets, dividing ownership into smaller claims than typically observed in stocks and bonds, in a way similar to structured products and securitisation. Investors, particularly retail, may therefore gain access to asset classes and risks that may have been otherwise beyond their capacity (e.g. participation in private equity funds) and participate in capital markets with lower minimum tickets or portfolio sizes.[4] Investors would thus potentially be able to better design or diversify their investment portfolio in certain asset classes with larger ticket sizes in their conventional form (e.g. real estate, gain exposure to a specific neighbourhood or diversify holdings internationally) or with new digital assets (e.g. intellectual property).

Fractional ownership may allow small and retail investors to benefit from a more *inclusive access* to somehow restricted asset classes, while enabling global pools of capital to reach parts of the financial markets previously reserved to large investors. Private placements of equity or debt of small and medium-sized companies (SMEs) are examples of security transactions that are traditionally restricted to large institutional investors and funds.

Increase in the participation of retail investors in previously restricted asset classes in a tokenised world would not mean that participation of retail investors in high-risk products should be completely unrestricted. Limitations to their participation and relevant thresholds to protect their interests can apply, as with the example of accreditation of investors under Regulation D in the United States or through the application of suitability requirements. Compliance of tokenised assets with the relevant (pre-existing) applicable regulatory framework will allow for such safeguards to be in place, therefore clarity around the applicable regulatory framework is of paramount importance for the issuers and participants in tokenised markets.

In addition to enhancing inclusiveness in markets that were previously restricted to larger or institutional investors, a potential proliferation of tokenisation of such securities may *enhance access to finance for SMEs* by potentially allowing any type of investor, including retail ones, to indirectly or directly fund SME projects. The flow of private financing from capital owners to small corporates could be facilitated, allowing for a more efficient allocation of capital within the economy and increasing inclusiveness not just for the investor side but also for seekers of capital unable to access capital markets otherwise.

The financing of SMEs and the real economy could potentially be facilitated not just through direct smaller-size investment and holding of fractional ownership in assets previously illiquid or completely unavailable to part of the investor base, but also through the *tokenisation of funds*. Investors may further diversify their risks by allocating capital in asset classes that traditionally lack liquidity (e.g. private equity and venture capital), indirectly promoting the use of such flows of capital from institutional investors to SMEs and start-ups, and enabling global pools of capital to finance their needs.

Importantly, a large part of the market argues that tokenisation of securities may benefit from a relatively clear regulatory and supervisory framework when compared to other crypto-assets, allowing for better regulatory compliance by its users. Although tokenisation has not benefited from regulatory arbitrage in the same way that the ICO market did over the past two years, the extent to which current regulation is sufficiently covering each and every aspect of tokenisation processes and practices is still debated. Potential for regulatory arbitrage may still be present in asset tokenisation markets, and possible gaps in regulation may still need to be examined.

Nevertheless, such “programmable” securities could potentially offer new possibilities of *automated compliance* with regulatory requirements. For example, in jurisdictions applying a limit to the number of investors allowed to participate in an offering, such limit may be programmed and built into the smart contract used for the distribution of tokenised securities, blocking any further investors from participating once the regulatory threshold applying has been reached.

Asset tokenisation and the trading of tokens representing assets in secondary markets may *increase or create the potential for liquidity* for those assets, provided there is sufficient volume of trading (or a market-

making function). This could be particularly important for assets with near-absent liquidity, such as some SME securities or Private Equity/Venture Capital (PE/VC) investment funds. At the same time, trading in secondary markets of tokenised assets that continue to be traded off-chain, risks creating a bifurcation of markets with negative consequences to liquidity conditions at conventional exchanges.

According to some, tokenised securities may benefit from lower "illiquidity premia"[5] which will allow investors to capture greater value from the underlying asset (Deloitte, 2018[8]). As investors expect higher yields from typically illiquid assets, these carry an illiquidity premium over and above the fair value of the asset, to reflect the higher risk of holding assets that cannot be easily sold over a longer period of time or in market downturns. Tokenised assets may carry *lower illiquidity premia* allowing for the asset to trade closer to its fair value. This, however, may be a difficult proposition to test, as liquidity/illiquidity premia are difficult to isolate, quantify and dissociate from systemic or market risk. According to some market participants, the benefit described above may be greater for the most illiquid asset classes (e.g. privately held SME equity, real estate, etc.), given that these carry the highest illiquidity premia.

A potential indirect benefit of asset tokenisation to market participants is related to potentially *faster clearing and settlement* driven by the near-immediate transfer of ownership on the blockchain and the continuous reconciliation of the ledger that is updated with every transaction. Increased efficiencies in clearing and settlement processes may perhaps be the biggest breakthrough of asset tokenisation with wider disruptive implications for financial markets and may result in reduced counterparty and operational risks in permissioned blockchains (FSB, 2019[2]). Uncertainty around settlement finality in public permissionless blockchains eliminates such potential benefit. At the same time, the ability to conduct "atomic swaps", i.e. the wallet-to-wallet exchange of two digital assets simultaneously in a single operation[6] across different blockchains without going through any centralised intermediary (e.g. exchange), may reduce significantly, if not eliminate, counterparty risk. However, these types of transactions are not widespread as the underlying technology is still quite nascent.[7]

The industry argues that issuing and transacting in a tokenised world promotes the creation of *new products and asset classes*. This is not necessarily accurate, as it is rather the form and not the substance of the asset classes that changes through tokenisation. Nevertheless, a tokenised environment may indeed create new and different incentives to participants, stemming from the nature of the underlying DLT. For example, the more applications/use-cases are built on top of the base protocol layer of a tokenisation platform, the more network effects can be realised and the more value can be derived from participation in the platform. Distribution of incentives is also different in a tokenised marketplace, with the different participants absorbing higher or lower rents from security transactions, when compared to traditional "off-chain" markets.

Challenges to a wider adoption of asset tokenisation

The adoption of asset tokenisation at a large scale would face a number of challenges related to the underlying technology itself. Scalability is still a technological challenge of DLT-enabled networks and is relevant to asset tokenisation given the significant throughput that would be required for the scale of global financial markets. Settlement finality, i.e. final and irrevocable settlement of payment instructions with deterministic finality, may still be a hurdle for some blockchains. Interoperability between different networks needs to be secured for connectivity between markets to be allowed. Other operational risks include network stability, exposure to cyber risk, risk of hacking and "51% attacks", but also business risks related to the migration to a DLT-enabled environment.

Governance issues, particularly relevant to fully decentralised ledgers, relate to the difficulty in identifying a sole owner or node accountable for the full network. The absence of a single accountable point is a problem that also arises when regulating DLT networks, or when responsibility for a failure in the network needs to be assigned. Network participants can perform "51% attacks" if the majority of the network decides to make changes that are not in line with the initial plan or can "fork" if they disagree with the

original protocol and decide to deviate and develop a separate network by adjusting the basic code (for permissionless DLTs).

Rapid advances in the field of digital technology raise forward-looking questions regarding technological robustness of market infrastructures based on DLT in the face of quantum threats to symmetrical cryptography[8] and even more so to asymmetrical cryptography[9]. The latter is, for example, useful for signing transactions on public blockchains. Further research is required on asymmetric postquantum cryptography for its safe use in tokenised markets.

A potentially unclear regulatory and legal status for selected tokenised assets is a risk to market participants, and can be addressed by clarity and interpretation of existing law and regulation by financial regulatory and supervisory authorities.

The legal status of smart contracts remains to be defined, as these are still not considered to be legal contracts in most jurisdictions. Until the clarification of whether contract law applies to smart contracts, enforceability and financial protection issues will persist. The auditability of the code of such smart contracts will require additional resources from market participants who will wish to confirm the basis on which such smart contracts are executed.

Questions arise also around data protection and privacy but also around storage of data and regulation applicable to the usage, sharing and storage of data. This is particularly pertinent in jurisdictions with data privacy regimes, such as the General Data Protection Regulation (GDPR) in Europe, requiring watertight consent management processes and effective data rights management systems to be in place, which can be somehow addressed in permissioned blockchains. Data erasure clauses, however, provide clients with the "right to be forgotten", which is the total antithesis of the immutability of the blockchain and will be harder to address for information that is written on the chain.[10] Nevertheless, it has been proven that privacy of transactions can be achieved in tokenised environments, where only relevant parties have visibility to transaction details (e.g. Monetary Authority of Singapore Project Ubin, Phase 2; EY's zero-knowledge proof (ZKP) private transaction protocol of Project Nightfall (Ernst and Young, 2019[9])).

Wider issues around identity and the management of digital identity at scale will also need to be addressed. Currently, there are no clear mechanisms in place to prevent, for example, "wash trading" and other market manipulation techniques. Without a unified approach to digital identity, participants can artificially affect the price of a digital asset through such techniques. As trading expands from within an exchange to across exchanges and across jurisdictions, that risk is expected to drastically increase. Such risks can be addressed by using strong anti-money laundering (AML)/know your customer (KYC) checks and the use of regulatory-compliant platforms.

Risks related to AML/combating the financing of terrorism (CFT) are prominent in DLT-based systems and are particularly high in tokenised markets that are based on public permissionless networks, especially when the protocol allows for anonymity of users. In 2019, the Financial Action Task Force (FATF) has issued important guidance on obligations of virtual asset activities and service providers (FATF, 2019[10]).

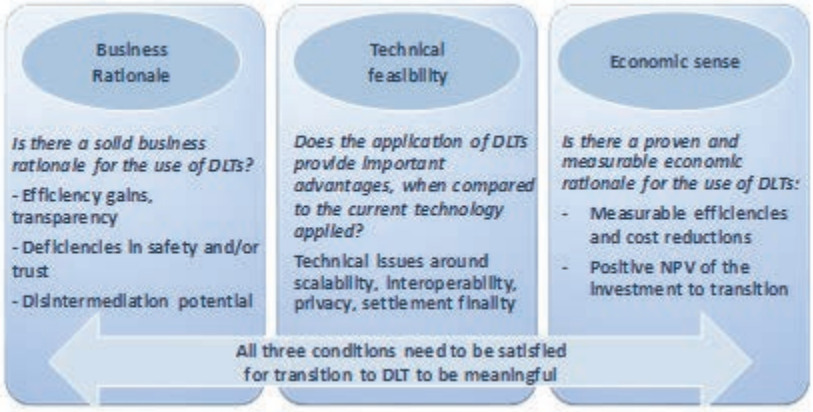
As private incentives established through the securities lifecycle are expected to be shifted around, fade or disappear in a tokenised environment, market participants do not equally share the motivation to transition to a blockchain-enabled market. The willingness and ability of the industry to agree on coordinated efforts to develop global or interoperable infrastructure solutions is not guaranteed. Most importantly, moving from legacy infrastructure to DLT-based networks requires significant investment from market participants, and is expected to materialise only once efficiency gains are proven and measurable for each asset type and part of the securities lifecycle.

In which markets does tokenisation make more sense? Conditions for a meaningful application

Tokenisation of assets could improve liquidity and tradability, as it may benefit from efficiency gains. Tokenisation could lower barriers to investment by enabling access to previously illiquid, unaffordable or insufficiently divisive assets. It may ease and simplify the flow of capital to start-ups and SMEs through the issuance of debt and equity in private companies where no trading infrastructure exists, and has the potential to indirectly enhance SME financing through the tokenisation of institutional SME funding (PE/VC funds).

As with all DLT-based applications, asset tokenisation would require a solid business rationale for the use of decentralisation and the blockchain (Figure 1.5). In other words, the use of DLTs in financial markets needs to be justified by efficiencies and related cost reductions; increases in safety, resilience and trust; reduction in complexity and disintermediation; or by the absence of existing trading infrastructure for the asset. Tokenisation of assets could therefore be more meaningful in those markets where there are efficiency gains to be reaped in terms of costs, speed, complexity of processes and with multiple layers of intermediation; or in markets with a deficiency of trust.

Figure 1.5. Conditions for a meaningful application of DLTs in financial markets



Source: (OECD, 2020[3]).

According to some market participants, tokenisation has the potential to provide a more efficient and less costly way to issue and administer securities particularly for niche small markets, such as SME or start-up equity and debt funding[11], thus potentially allowing smaller companies access to capital market financing (Reuters, 2019[11]). Enhanced transparency and availability of data could alleviate part of the information issue observed in SME markets, while disintermediation and automation could reduce costs and increase the efficiency of issuing, trading and administrating SME securities, which usually involve multiple layers of intermediation and relatively high complexity (e.g. documentation). The potential for increased liquidity is crucial for SME markets, which traditionally face lower liquidity than markets for larger corporates.

The efficiency gains to be realised by the adoption of asset tokenisation for public equities in developed economies requires a weighing of the cost and ease advantages against the fact that such markets enjoy high levels of trust by their participants and are supported by fast, safe and efficient processes with small net incremental efficiency gains achievable through such transition. However, market views differ over the potential of tokenisation to serve niche markets; some market participants argue that large players active in mature markets are more technology-ready and have the know-how and capacity required to invest in the adoption of tokenisation practices faster than small niche markets for SMEs.

At the same time, it could be argued that some of the potential benefits of asset tokenisation could only be achieved if the network reaches sufficient scale. Sufficient scale would help to ensure the full realisation of benefits such as increased liquidity. This could mean that under such a scenario, asset tokenisation would end up being more of a complement, rather than a replacement, of current conventional markets for the same assets, at least at the initial stage of development of that market, for certain processes or parts of the security lifecycle. This would still allow market participants to test the capabilities of DLTs and enjoy some of its benefits.

A potential transition of financial markets and products to a tokenised environment enabled by DLTs is not expected to happen in the near-term even by the most prominent advocates of the blockchain technology. The shift to DLT-based markets could more easily be envisaged to be deployed in a gradual manner, prioritising those processes that have the most potential for efficiency gains first. Tokenised markets may flourish as a complement to current conventional markets for selected processes along the security lifecycle, such as post-trade. Ultimately, legacy and DLT-enabled systems could end up converging into a hybrid version of interfaces with conventional infrastructure elements combined with automation and DLT-based applications in areas such as clearing and settlement, where efficiency gains are high enough to justify the (gradual) transition to a decentralised infrastructure.

How can asset tokenisation disrupt the securities markets?

A potential future proliferation in the use of asset tokenisation in financial markets can have implications on liquidity, but it can also affect trading, asset pricing, clearing and settlement of securities, and even monetary policy transmission.

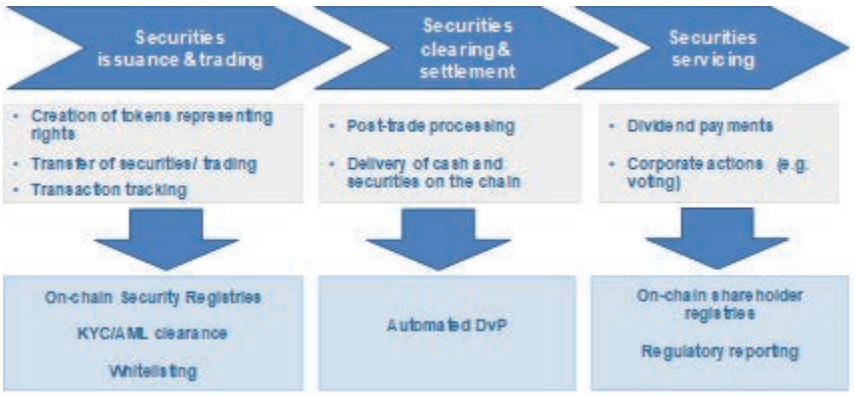
When looking at the potential disruptions in the markets from such a phenomenon, a differentiation needs to be made between the following two structures in the securities context:

(i) tokenisation of securities that also exist off-the-chain, e.g. securities traded off-chain, with some part or the entirety of securities being tokenised and transferred on-chain; and

(ii) issuance of securities in tokenised form directly on-chain and native to the blockchain, i.e. without issuing securities in the "conventional" form.[12] [13]

The implications of a potential expansion in the use of tokenised assets are widespread and would affect financial markets in a number of ways, affecting trading, pricing, liquidity, as well as clearing and settlement of securities (Figure 1.6).

Figure 1.6. Areas in securities markets with DLT use-cases and potential

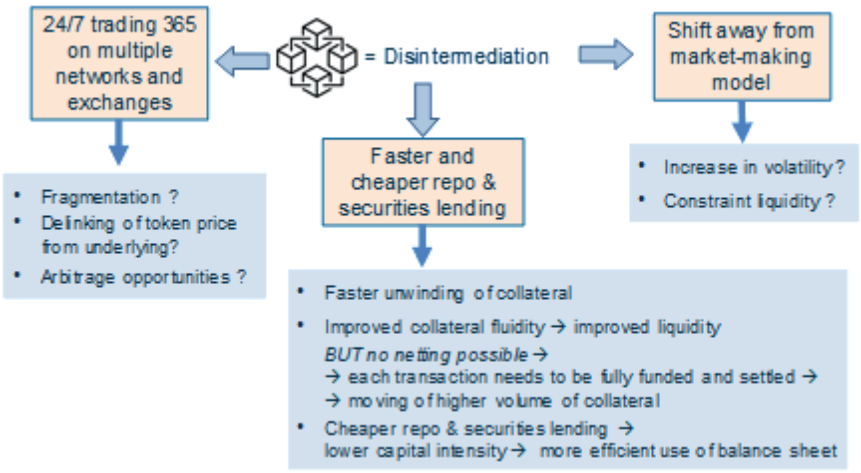


Source: (OECD, 2020[3]).

Trading, pricing and liquidity

A potential proliferation of tokenisation in the financial markets would have implications and potential disruptive effect on processes and participants alike. Efficiency gains in tokenisation stem to a large extent from its potential for disintermediation. Such disintermediation could affect trading by disrupting the market-making model, which could in turn affect volatility and liquidity of related markets, especially in times of stress (Figure 1.7).

Figure 1.7. Potential implications of tokenisation for trading and pricing

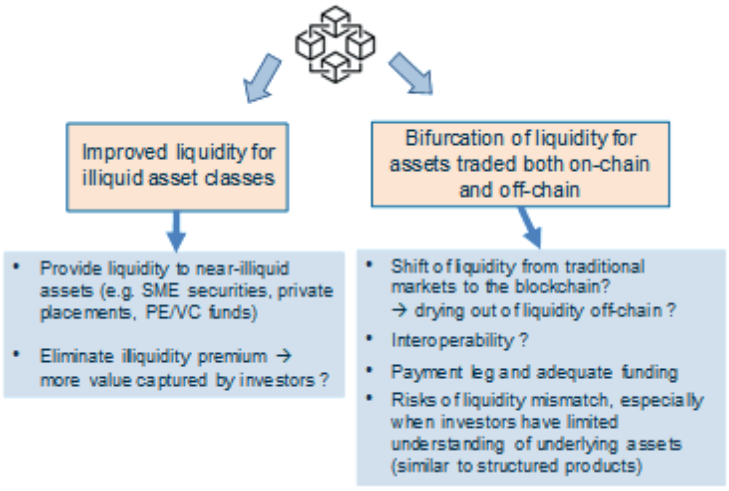


In terms of pricing of the assets, tokenisation enhances transparency and has therefore the potential to reduce information asymmetries and improve the price discovery mechanism. At the same time, trading of tokenised assets risks becoming fragmented if the asset trades on non-interoperable networks and exchanges on- and off-the chain.

A potential take-off in tokenisation activity would also affect repo activity for the funding of positions, as well as on securities lending activities used as part of trading strategies. The shift of the above activities "on-chain" would allow for direct and faster unwinding of collateral, easier mobilisation of collateral across security pools, more efficient use of balance sheet and lower capital intensity associated with such activities.

When it comes to liquidity, tokenisation can be a double-edged sword with positive effect on near-illiquid assets (e.g. participation in the capital of private SMEs) but potential risks of bifurcation of liquidity between on-chain and off-chain markets for the same asset (Figure 1.8). The latter may result from a shift in liquidity from conventional markets on to the blockchain, drying up liquidity in the off-chain markets and giving rise to risks of arbitrage. These issues are not too dissimilar to the challenges of managing dual-listings (e.g. American Depository Receipts (ADRs) and Global Depository Receipts (GDRs) vs. ordinaries) in off-chain markets.

Figure 1.8. Potential implications of tokenisation for liquidity



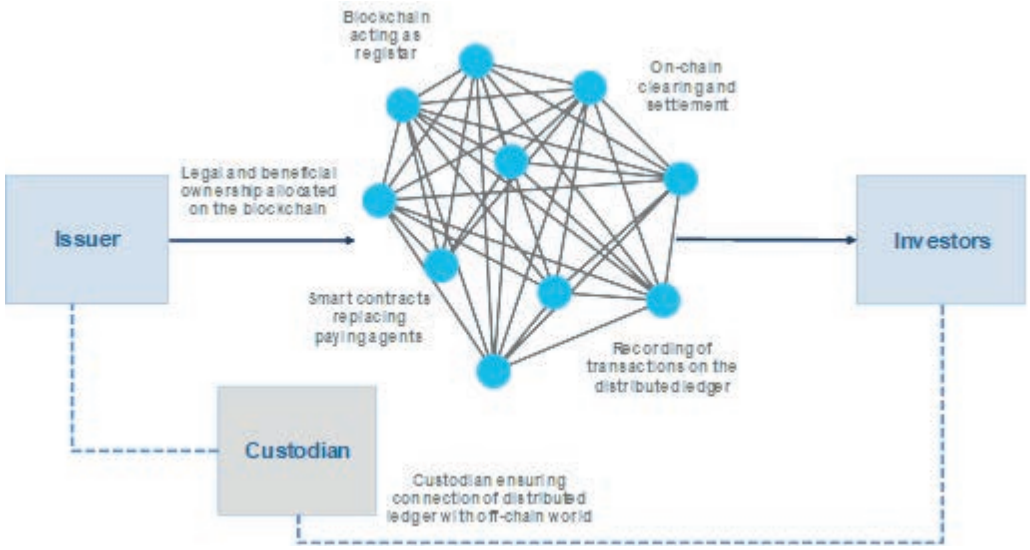
Clearing and settlement

The use of DLT can expedite and condense trade clearing and settlement to nearly real-time, reducing counterparty risks and freeing up collateral, producing capital efficiencies for participants in the trade. The post-trade multi-step process is simplified and the back-office administrative burden is lowered significantly (Figure 1.9). Experimental application of DLTs on clearing and settlement has, however, produced mixed results and hurdles in the development of the technology will need to be overcome for the application to arrive at the stage where it can provide better performance than systems currently in use.

Importantly, a tokenised form of currency or stable coins may be required for the payment leg of security settlement on DLT networks. A potential proliferation of tokenised markets raises the question of whether and how national central banks would be willing to facilitate the tokenisation of central bank money for use in tokenised markets, or whether such function will be instead performed by stable coins.

Tokenisation will ultimately depend on the existence of a trusted and credible central authority that will guarantee the connection of the off-chain world with the blockchain (e.g. existence and custody of unique assets backing the tokens issued).

Figure 1.9. Simplified scheme of corresponding tokenised security issuance



Notes: The above structure assumes that the technology allows the investor to retain beneficial ownership for tokens that are held by a custodian. In terms of technology, this would translate in a separate wallet address for the exercising of voting or other rights than the wallet address that holds the assets in custody. Such technology is in the early stages of its development.
Source: (OECD, 2020[3]).

High-level policy considerations

Tokenised markets should comply with regulatory requirements that promote financial consumer and investor protection, market integrity and competition, and seek to guard against build-up of systemic risks. Tokenised assets can be seen as cryptography-enabled dematerialised securities based on a DLT-enabled network, instead of electronic book-entries in securities registries of central securities depositories, therefore merely replacing one digital technology with another, raising no issues in jurisdictions with a technology neutral approach to regulation. Nevertheless, it can sometimes be difficult to know with certainty whether tokenisation falls within the regulatory perimeter or is fully captured by the perimeter, especially given the novel nature of some new business models and processes involved in tokenised markets. Potential gaps in the regulatory treatment of tokenisation may give rise to regulatory arbitrage opportunities, similar to the ones witnessed in the ICO market. This is less of an issue in jurisdictions where a technologically neutral approach applies to financial regulation.

To date, it is not completely clear whether tokenised assets, tokenisation processes, the markets in which they trade and the processes involved are fully compliant with the existing regulatory and supervisory framework covering the corresponding asset markets, particularly for assets native to the blockchain.[14] Given the inherent global nature of decentralised networks enabled by DLTs, such gaps would need to be examined both at national and cross-jurisdictional basis. In addition, the absence of a central point of accountability due to the decentralised nature of the network may be an impediment to the implementation of regulatory action when such mechanisms are used.

At the same time, tokenised assets that fall within the legal and regulatory perimeters of existing frameworks (policy frameworks and regulatory regimes) may not be fully and correctly understood by market participants. Regulatory or legal ambiguity around asset tokenisation can create uncertainties and risks for participants in tokenisation markets and undermine the smooth functioning of such marketplaces, with potential indirect impact on the conventional, off-chain markets (traditional assets and financial market infrastructure (FMIs)) for such assets.[15] Legal and regulatory ambiguity is also slowing down the adoption

rate of such technologies as participants are uncertain of the conditions under which they can participate in such markets and/or engage investors.

Greater clarity around the regulatory and supervisory frameworks applied to tokenised assets and markets will be a stepping stone to their safe development and use. Existing regulation may need to apply to new actors (e.g. trusted third party guaranteeing the accuracy of information at the onboarding of the asset on-chain and safeguarding the asset) and/or new requirements may need to be added (e.g. covering the interoperability between DLTs or the interaction or gateways linking the on-chain and off-chain environments). New risks that may arise for the application of DLT technologies (e.g. associated operational risks, risks related to digital identities) will also need to be appropriately supervised.

At the national level, different institutions regulating and supervising virtual assets should aim for a coordinated approach covering all different facets of such activity (e.g. payments, investments, taxes, accounting, AML/CFT compliance, law enforcement and crime prevention).

Cross-border transactions of tokenised assets require international cooperation to limit regulatory arbitrage and for the smooth operation of tokenised markets. International coordination is warranted when it comes to a more harmonised legal treatment of tokenised assets so as to avoid regulatory arbitrage. An appropriate balance needs to be struck between managing emerging risks and allowing space for innovation to flourish. The potential development of standards or principles that would apply to DLT-enabled networks operating in the financial markets (and beyond) could facilitate coordination at global level and promote a level playing field for participants performing the same activity.

Wider use of tokenised securities raises potential financial consumer protection and market conduct issues, the handling of which will be essential to safeguard investors' interests and ensure a fair and orderly market for tokenised assets. Recourse and redress in case of damage due to a technical issue, theft or non-existent real asset backing the tokenisation is only one example of such investor risk involved.[16] Market integrity issues can arise stemming from the immaturity of the market, the potential lack of monitoring and controlling mechanisms, combined with a lack of information around tokenisation. Risks to market integrity can damage market confidence and raise the possibility of consumer and investor loss.

Financial education efforts would be indispensable for the protection of investors in tokenised markets, especially given the potential for increased participation of retail investors in such markets. Tokenised markets will require appropriate understanding of technological aspects, over and above standard financial knowledge, for the informed participation of investors in such markets. Indicatively, tokenised assets are typically secured by the investor’s private key; loss of the private key results in loss of the entire investment.[17] The assessment of the suitability of tokenised assets for each individual consumer and/or investor is another example of a consideration in such markets, taking into account the individual needs, circumstances and/or risk tolerance levels of each participant in tokenised markets.

References

Allen & Overy (2017), *Press Release: Nivaura executes world’s first automated cryptocurrency bond issuance supported by Allen & Overy*, http://www.allenovery.com/news/en-gb/articles/Pages/Nivaura-executes-worlds-first-automated-cryptocurrency-bond-issuance-supported-by-Allen-Overy.aspx. [6]

Bank for International Settlements (2017), “Distributed ledger technology in payment, clearing and settlement: An analytical framework”, *Committee on Payments and Market Infrastructures*, https://www.bis.org/cpmi/publ/d157.pdf. [14]

Bank of International Settlements and Swiss National Bank (2019), *Press Release: SNB and BIS sign operational agreement on BIS Innovation Hub Centre in Switzerland*, https://www.bis.org/press/p191008.htm. [13]

Capital Markets and Technology Association (2018), *Blueprint for the tokenization of shares of Swiss corporations using the distributed ledger technology*, http://www.cmta.ch/wp-content/uploads/CMTA-Blueprint-for-the-tokenization-of-shares-of-Swiss-corporations-1.pdf. [15]

Daimler (2017), *Press Release: Daimler and LBBW successfully utilize blockchain technology for launch of corporate Schuldschein*, https://media.daimler.com/marsMediaSite/en/instance/ko/Daimler-and-LBBW-successfully-utilize-blockchain-technology-for-launch-of-corporate-Schuldschein.xhtml?oid=22744703. [7]

Delaware State Senate (2017), *Senate Bill No. 69, Act to amend title 8 of the Delaware code relating to the General Corporation Law*, https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69. [5]

Deloitte (2018), "The tokenization of assets is disrupting the financial industry. Are you ready?", *Inside Magazine* Issue 19, November, https://www2.deloitte.com/lu/en/pages/technology/articles/tokenization-assets-disrupting-financial-industry.html. [8]

Ermokhin, I. and A. Levashenko (2019), *Welcome to the tokenised world*, https://oecd-russia.org/en/analytics/welcome-to-tokenized-world.html. [16]

Ernst and Young (2019), *Press Release: EY releases zero-knowledge proof blockchain transaction technology to the public domain to advance blockchain privacy standards*, https://www.ey.com/en_gl/news/2019/04/ey-releases-zero-knowledge-proof-blockchain-transaction-technology-to-the-public-domain-to-advance-blockchain-privacy-standards. [9]

European Central Bank (2016), "Distributed ledger technologies in securities post-trading", *ECB Occasional Paper* 172, https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf. [18]

European Central Bank and Bank of Japan (2018), *BOJ/ECB joint research project on distributed ledger technology*, https://www.boj.or.jp/en/announcements/release_2018/data/rel180327a2.pdf. [17]

FATF (2019), *Public Statement on Virtual Assets and Related Providers*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html. [10]

Financial Conduct Authority (2019), "Guidance on Cryptoassets, Feedback and Final Guidance to CP 19/3", *Policy Statement* PS 19/22, https://www.fca.org.uk/publication/policy/ps19-22.pdf. [20]

Financial Conduct Authority (2019), *The impact and effectiveness of Innovate*, https://www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf. [19]

Financial Conduct Authority (2017), *Regulatory Sandbox lessons learned report*, https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf. [21]

FSB (2019), *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, https://www.fsb.org/2019/06/decentralised-financial-technologies-report-on-financial-stability-regulatory-and-governance-implications/. [2]

Henderson, A., J. Thornborough and J. Burnie (2019), "Issuing Equity Tokens on the Blockchain and Legal Reimagining", *Butterworths Journal of International Banking and Financial Law*. [22]

Hileman, G. and M. Rauchs (2017), *Global Blockchain Benchmarking Study*, http://dx.doi.org/10.2139/ssrn.3040224. [1]

HM Treasury, Financial Conduct Authority and Bank of England (2018), *Cryptoassets Taskforce, Final Report*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf. [23]

Kostika, E. and N. Laopodis (2019), "Dynamic linkages among cryptocurrencies, exchange rates and global equity markets", *Studies in Economics and Finance*, http://dx.doi.org/10.1108/SEF-01-2019-0032. [24]

Monetary Authority of Singapore and Deloitte (2017), *The future is here: Project Ubin, SGD on Distributed Ledger*, https://www2.deloitte.com/sg/en/pages/financial-services/articles/project-ubin-sgd-on-distributed-ledger.html. [25]

Nivaura (2017), *Overview of debt issuance, presentation by Dr. Avtar Sehra*, http://www.swissmlf.ch/wp-content/uploads/2017/08/Nivaura-Overview-20170706-Short.pdf. [26]

OECD (2020), "The Tokenisation of Assets and Potential Implications for Financial Markets", *OECD Blockchain Policy Series*, http://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf. [3]

OECD (2019), *Initial Coin Offerings for SME financing*, http://www.oecd.org/finance/ICOs-for-SME-Financing.pdf. [4]

Poskriakov,, F., M. Chiriaeva and C. Cavin (2019), "Cryptocurrency compliance and risks: A European KYC/AML perspective", in *Blockchain & Cryptocurrency Regulation 2019, Global Legal Insights, 1st edition*, https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf. [27]

Reuters (2019), *Press Release: London Stock Exchange invests in start-up behind world's first cryptocurrency bond*, https://www.reuters.com/article/lseg-fintech/london-stock-exchange-invests-in-start-up-behind-worlds-first-cryptocurrency-bond-idUSL3N20L4U6. [11]

Silverman, J. (2015), *NTRU and Lattice-Based Crypto: Past, Present, and Future*, http://archive.dimacs.rutgers.edu/Workshops/Post-Quantum/Slides/Silverman.pdf. [12]

SIX (2019), *The SDX trading platform*, https://www.sixdx.com/en/home/offering/services.html. [28]

Notes

[1] Some of the main differences lie in the structuring, as bundling is not necessarily the norm in tokenisation; the resulting securities being ring-fenced by originators in securitisation, which is not the case in tokenisation; and the fact that in securitisation there can be credit enhancement while in tokenisation the security's/token's credit quality can never be higher than that of the underlying asset.

[2] This is, to a large extent, linked to the recognition of the blockchain as a valid representation of ownership of the asset (instead of a proxy). The digital ledger would need to be recognised as evidence of ownership for equities to be able to be issued natively on DLTs and recognised as such.

[3] Increased transparency may not be desirable by large institutional investors and for the execution of block trades.

[4] The sale of risky assets to retail investors should, in all cases, be accompanied by consumer protection safeguards adapted to tokenised assets.

[5] Liquidity and illiquidity premium used interchangeably to describe the compensation investors seek for the risk of loss relative to an investment's fair value if an investment needs to be converted to cash quickly.

[6] Technically two transactions which are linked (two bilateral transfers on different chains which are confirmed by both sides within a certain time period, using hash technology).

[7] It should be noted that atomic swaps can only happen when both assets are locked-on in the position of the buy and sell-side prior to the execution of the trade. It should also be noted that the reduction of counterparty risk does not necessarily translate into total reduction in transaction risk, as new risks emerge with the application of DLTs (e.g. operational, security/hacking and cyber risks).

[8] Threat of Grover's quantum algorithm (Silverman, 2015[12]).

[9] Threat from Shor's algorithm (Silverman, 2015[12]).

[10] A practical solution to privacy issues involves the use of a combination of on-chain/off-chain mechanisms augmented by zero-knowledge proofs. For example, a third party identity provider or claim 'attester' can provide binary yes/no responses to the ledger without disclosing the detailed information.

[11] Examples include private placements of non-listed securities; participation in the capital of private limited liability companies; small-sized SME bonds; as well as private equity/ venture capital funds.

[12] The second structure may or may not be considered as tokenisation, given the absence of a real-word asset to back the token issued directly on the blockchain. However, in the absence of a common classification, we have included both structures under the tokenisation umbrella for the purposes of this note. Further clarification as to the classification of such structures will be required in the future.

[13] It should be noted that, *from a purely legal perspective*, tokens representing securities have a "real world" part to them, as there is always a claim/debt relationship between the issuer and holder of the security, which corresponds to a related contractual and legal framework.

[14] For tokenised assets which are issued on the back of pre-existing regulated assets, the representation of the existing asset on the blockchain should not change its regulatory status. Even in these cases, the use of DLTs may affect the way in which regulation applies to the asset, the processes or the market.

[15] To some extent, the absence of common definitions or harmonised terminology of the different categories of digital assets further inhibits the assessment of whether such assets fall within the boundaries of the regulatory perimeter for each activity.

[16] Protocols developed by the industry try to address the issue of lack of recourse and redress mechanisms: for example, a pre-defined 'approved authority' can be allowed to move tokens from one wallet to another without having the private key of either wallet. Such mechanisms could resolve issues that arise in case of death of a tokenholder or loss of private key.

[17] Unless the key is held by a specialised custodian, or unless the protocol used addresses this concern. For example, under the ERC1400 protocol, an investor can directly contact the issuer of the security, provide their identity and have the asset transferred back to their wallet using a "forced transfer mechanism".

2 Open banking

This chapter first presents initiatives to foster open banking in selected jurisdictions. It then describes benefits and selected challenges associated with the implied de-monopolisation of customer data, including in particular potential market structural effects. It also discusses selected regulatory considerations and identifies some open issues.[1]

Introduction

Open banking is an initiative aiming to increase competition in the provision of banking services, so that customers benefit from better or cheaper services. To date, open banking initiatives focus on retail payment services, although initiatives will focus on other services as well.

At the outset, it should be noted that there exists no single internationally agreed definition of "open banking".[2] That said, **implicit in the different discussions under the header of open banking is the view that greater competition in banking services needs to be fostered by allowing entry of new service providers**. The desired outcome is that the new entrants could suppress rents of incumbents, while offering consumers more innovative, better-tailored, easier-to-use, and perhaps cheaper financial services.

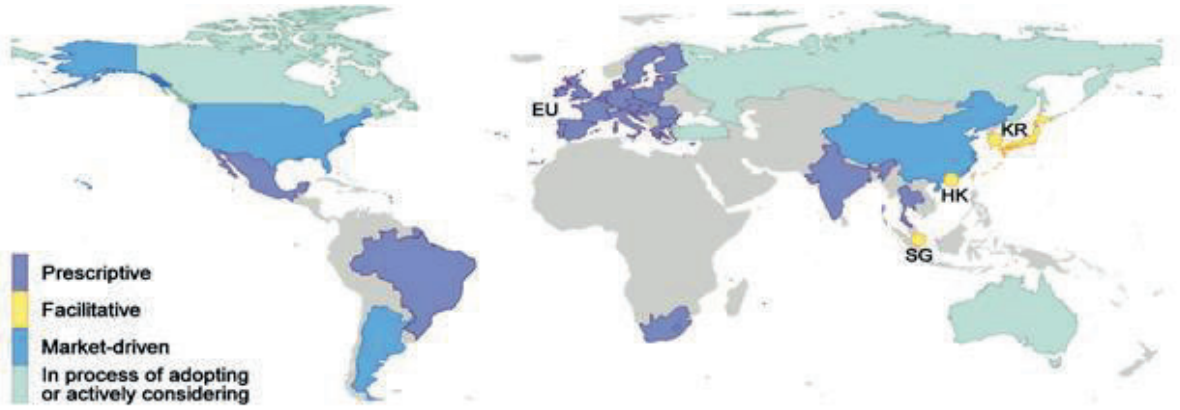
Open banking initiatives require banks to provide authorised third party providers with access to customers' transactional data, with customer consent. Such efforts have so far focused on payment services, but are not necessarily restricted to them. To what extent sharing is mandated also differs across jurisdictions. For the purposes of the present chapter, "open banking" is defined, following FSB (2019[1]), as *referring to a system in which financial institutions' data can be shared for users and third-party developers through application programming interfaces*.

Section 2 of this chapter observes that the extent and nature of regulatory initiatives to foster open banking differ across jurisdictions. It also explains some basic concepts such as that of application programming interfaces (APIs). Section 3 describes how the sharing of customer data could lead to the de-monopolisation of such data and highlights some aspects of the use of digital data in the development of financial services. Section 4 discusses potential market structural effects of open banking and singles out some open issues for special attention, while section 5 discusses selected regulatory considerations and open issues. Section 6 concludes.

Approaches to open banking

The extent and nature of regulatory initiatives to foster open banking differ across jurisdictions. A stylised characterisation of developments in different jurisdictions is provided in Figure 2.1, highlighting that authorities have taken a range of actions related to open banking in their respective jurisdictions (Basel Committee on Banking Supervision, 2019[2]). Some jurisdictions require banks to share customer-permissioned data and require third parties to register with a particular regulatory or supervisory authority. Other jurisdictions have issued guidance and recommended standards, and published open API standards and technical specifications (Box 2.1). Remaining jurisdictions follow a market-driven approach and currently have no explicit rules or guidance that either require or prohibit the sharing of customer-permissioned data by banks with third parties.

Figure 2.1. Examples of global open-banking developments



Note: Four stylised approaches are distinguished. "Prescriptive": requires data sharing. "Facilitative": encourages data sharing. "Market-driven": no explicit rule/guidance requiring data sharing. "In process of adopting or actively considering": in process of adopting or actively considering adopting. EU (European Union), HK (Hong Kong, China), KR (Korea), SG (Singapore).
Source: (Basel Committee on Banking Supervision, 2019[2]) and OECD Secretariat updates for Brazil.

Box 2.1. Application programming interface (API)

APIs are technology-enabled protocols that enable a computer system or source of data to interact with, or be used by, other software; they allow applications to share data and functionality. The intent of common and open standards for APIs goes a bit further. Specifically, they are intended to enable (smaller) developers to create products more easily and efficiently. However, it is not always clear exactly where the line on access is being drawn. In principle, an API can be open or restricted to specific participants. In an open API, any third party that meets certain standards can gain access and build applications for use by financial consumers. An API can however also be restricted to specific (business) partners. New linkages between various entities and networks could improve choice, but may also create additional vulnerabilities. Conceptually, opening up information via APIs multiplies entry points, which might be vulnerable to data breaches, manipulation or other operational risks. That said, APIs are already being widely used in other industries. For example, Google Maps exists because of APIs, as well as many other real-time services. APIs are tools that are not intrinsically dangerous although it is important to ensure that controls are appropriately implemented.

APIs also face a number of challenges. To begin with, building and maintaining APIs is costly and time-consuming, especially if such efforts are undertaken on a bilateral basis with multiple entities involved altogether. Costs tend to be higher in jurisdictions where there is no commonly accepted API standard and the relative costs are economically more meaningful for smaller entities, including smaller incumbent banks.

Many open banking efforts focus on the area of payment services. In a large number of jurisdictions, including the United Kingdom, Australia, and European Union countries, regulatory initiatives typically mandate that banks must grant third parties access to their customers' payment transactions data, if the latter so request, as well as the ability for third parties to initiate payments on customers' behalf.

Public authorities in different jurisdictions differ in their view as to how far efforts should ultimately go in terms of which, if any, other types of sectors or financial services should be targeted. For example, the European PSD2 (Box 2.2) focuses specifically on payment initiation and the sharing of bank account information, although it is conceivable that the latter will have implications that go beyond payment services

and include other types of financial services, such as investment advice. In Hong Kong, China, open banking initiatives focus squarely on (maintaining) the competitiveness of the banking sector (Box 2.3). By contrast, Australia and the United Kingdom are considering extending the principles of open banking initiatives to enhance competition outside the banking sector (for example in other sectors such as energy or telecommunications).

Box 2.2. European Payment Services Directive

A prime example of open banking regulation is the revised Payment Services Directive (PSD2) of the European Union. PSD2, which places the payment service function at the core of recent "open banking" initiatives. It requires banks to grant competitors access to bank customer data, if the customer so requests, as well as the ability for third parties to initiate payments on customers' behalf. In particular, bank account holders can request, free of charge, that banks share their financial data in digital form to authorised third parties. In addition, account holders can authorise third-party providers to initiate payments from their bank account. Consistent with the new General Data Protection Regulation (GDPR), the account holder remains the owner of the personal data. PSD2 entered into force on 13 January 2018. The explicit motivation behind it is to increase competition and innovation in payment services. The approach taken essentially consists of subdividing the payments function into three linked but separable aspects: the entity of customer account, the account information, and payment initiation. As to the first, to the extent that an account is enabled for online banking, customers can request the bank providing the account to grant a third party access to the respective account, share account information with the third party and allow the latter to initiate payments. The bank is required to make available open technical interfaces that allow easy digital access to bank customer accounts, and it cannot charge a fee for these services. Third parties, including other banks, will thus be enabled to build financial services on top of customers' banking data. The provision of richer and more detailed information that might be more convenient to assess should help consumers to compare products and facilitate switching between service providers.

Strong customer authentication is foreseen. Customers have to provide several independent features to prove their identity when logging in. These include information that only the customers should know (e.g. a password) and that identifies them uniquely (e.g. biometric information such as a fingerprint or face recognition), via a mobile device that only the customers would be expected to possess (e.g. their tablet or smartphone). In addition, when the customer initiates an electronic payment through a third party, the bank needs to request the customer, through a separate communication channel (e.g. a text message), to verify that transaction and confirm it, so as to authorise it.

To limit the risks of account holders giving third parties access to their accounts, the latter need to be licensed[3] by the financial supervisory authority and provide an electronic certificate for identification to the bank. Pass-porting rules allow that a license in one European Economic Area (EEA) member state is sufficient to operate in the entire EEA. Also, the customer needs to log into the third-party service provider using strong authentication and authorise the payment. In addition, a legal protection for the customer consists of the specification that the bank is liable for losses relating to wrong execution or fraud when using the third-party service provider, although the bank can claim compensation from the latter.

Box 2.3. Open banking in Hong Kong, China

In Hong Kong, China, an open banking initiative aims broadly at maintaining the overall competitiveness of the banking sector rather than addressing any specific identified weakness. The initiative included the publication of a framework on how to build open APIs. In addition, a guideline was issued in 2018 by the Hong Kong Monetary Authority (HKMA) that sets out the principles, which the HKMA will take into account in deciding whether to authorize "virtual banks" applying to conduct banking business in Hong Kong, China.[4] In 2019, the HKMA granted the first of altogether eight virtual banking licences, as part of its so-called Smart Banking Initiatives meant to facilitate financial innovation, enhanced customer experience and financial inclusion.

The HKMA expects to be able to conduct a comprehensive assessment of the results of these various initiatives about one year after the first virtual bank has launched its service (which thus would be before the end of 2019). The experience is particularly relevant as large non-financial firms with a strong focus on technology-use stand behind some of them. The role of large technology firms in financial services has received heightened attention since the announcement in June 2019 by Facebook of its Libra project, even if other large technology firms had been active in financial services for some time now including but not restricted to Asia.

The HKMA granted licenses to Ant SME Services (Hong Kong, China) Limited, a subsidiary of ANT Financial and an operator of Alipay, Infinium Limited, Insight Fintech HK Limited and Ping An OneConnect Company Limited, Welab Digital Limited, and Livi VB Limited, SC Digital Solutions Limited and ZhongAn Virtual Finance Limited. Ping An OneConnect Company Limited is part of Ping An Group, the world's largest insurer. Tencent, who is operating WeChat Pay HK in Hong Kong, China, is a major investor in Infinium Limited. Insight Fintech HK Limited is jointly established by Xiaomi Corporation, the world's fourth-largest smartphone producer, and AMTD Group.

Several regulatory open banking initiatives foresee that bank account holders can request, free of charge, that banks transmit their financial data in digital form to third party providers. Moreover, account holders can authorise third-party providers to initiate payments from their bank account. Some proposals (e.g. UK's Open Banking) require banks to make available open-source APIs that allow easy digital access to their customer accounts, while others (e.g. the PSD2) only require that the data be shared. Brazil approved an open banking model that is particularly comprehensive in terms of the scope of shared data and services,[5] including the sharing of financial customer's data on deposit accounts, credit cards, credit operations, investment, insurance and some types of (open) pension funds, as well as the services of payment initiation and loan proposals' forwarding (Box 2.4).

Box 2.4. Open banking in Brazil

The Central Bank of Brazil (BCB) defines open banking as "the sharing of data, products and services by financial institutions and other licensed institutions, at the customers' discretion as far as their own data is concerned, through the opening and integration of platforms and infrastructures of information systems, in a safe, agile and convenient manner." The Brazilian open banking model shares the same basic principle that motivated the enactment of the country's General Data Protection Law (LGPD; Law No. 13,709, of 14 August 2018), which is that consumers own their personal data. Customers must give express consent prior to that data being shared with another party. Moreover, in order to avoid consumer discrimination and to set a boundary on what type of data could actually be shared, sensitive personal data, related to ethnical, racial, religious, politic opinion, health, sexual life or sexual orientation, genetic or biometric data, as well as credit scores or ratings, credentials and other information used with the objective of authenticating the customers and transactional data about products and services that are not contracted with nor distributed by the data transmitter institution do not fall under the scope of open banking in Brazil. As regards the "right for individuals to have their personal data to be forgotten", it is noted that open banking regulation in Brazil only deals with the data sharing process, while the processes associated with how data must be handled by the recipient institutions is addressed in the light of the aforementioned LGPD, which will come into force in May 2021, and the Civil Framework of Internet (Law No. 12,965, of 23 April 2014), which is the law that regulates the use of the Internet in Brazil. Both the LGPD and the Civil Framework for Internet ensure that consumers have the right to request for their data to be deleted. It foresees that the owner (individual to whom the data belongs) can, at any time, request that the data controller (company or organization that, for its purposes, stores and uses that data) deletes this information from its systems. Moreover, the LGPD also establishes that the data controllers must eliminate or anonymize all data after it serves the specific purposes that motivated its collection.

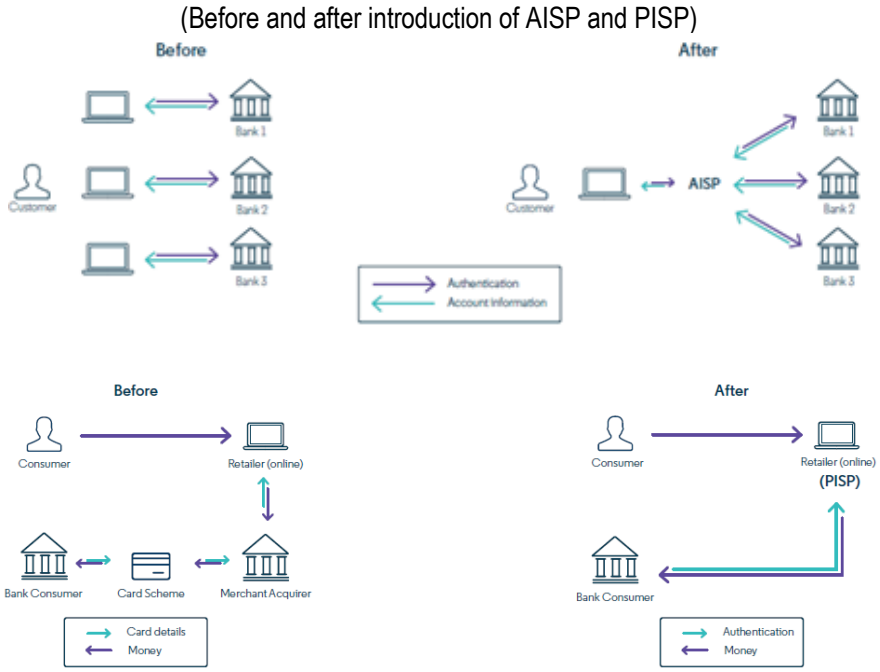
In the United States (Box 2.5), APIs have been used for a long time already, including to enable personal financial management software and to connect developers to payments networks such as Visa and MasterCard, but these connections were used mainly to share information, and not to initiate transactions. By contrast, a key principle of PSD2 is that upon the account holder's consent, a third-party provider must be granted access to initiate payments on the account holder's behalf. The authorised Third-Party Provider (TPP) could be (another) bank, a digital bank, a payments or a technology company.

Box 2.5. Open banking initiatives in the United States

In the United States, open banking initiatives are driven by the private sector. A United States Treasury report (2018[3]) covers "nonbank financial, fintech, and innovation" and considers ways of how best to embrace digitisation, data, and technology. Among other things, it focuses on consumer financial data, observing that digitisation has given rise to a new sector of nonbank financial institutions focused on products and services utilising data aggregation. Data aggregation involves compiling data from one or more sources and standardising it into a summary form. At present, there are two primary methods through which data aggregators gain access to consumer financial data: APIs and "screen-scraping", that is the collection of screen display data from one application and translation of that data so that another application can display it. The US Treasury report notes that the advantages of using APIs as opposed to screen-scraping for data aggregation are recognised, but that current APIs have their limitations, and that further efforts are needed to advance standardisation. The report also notes that given the differences in the environment, open-banking initiatives such as that taken in the United Kingdom are not readily applicable in the United States, but that US regulatory authorities should be able to learn from experiences made in the United Kingdom.

TPPs can take several forms, including Account Information Service Provider (AISP) or Payment Initiation Service Provider (PISP). AISPs allow the customer to see all of its account information from different bank accounts in one place online. By aggregating customers' banking data, AISPs can then provide customers with insights about their spending, or suggest better-priced services. PISPs allow customers to make payments directly from their bank account rather than using its debit or credit card. A PISP requires explicit consent from the customer (also referred to as the Payment Services User or PSU) before the service can be provided. Figure 2.2 provides stylised descriptions of the possibly changing links between customers, banks and other financial services providers.

Figure 2.2. Stylised depiction of changing interconnections



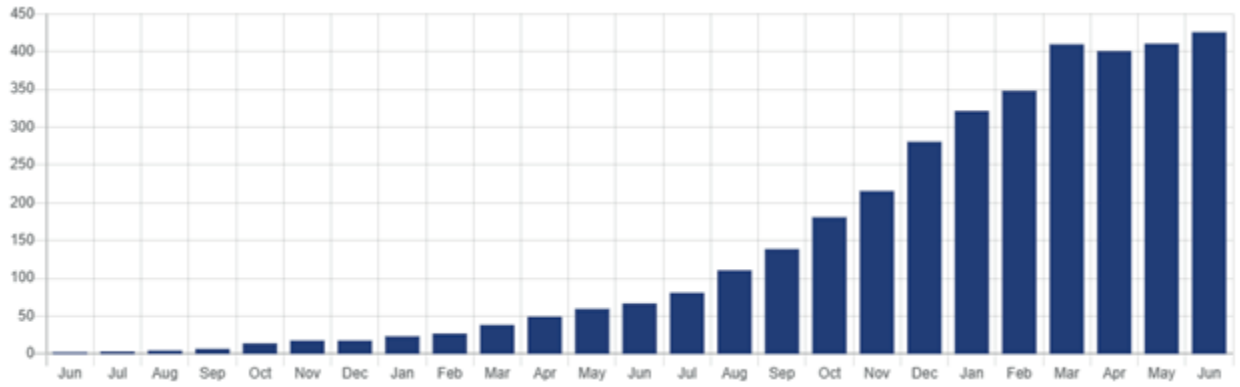
Note: AISP stands for Account Information Service Provider and PISP for Payment Initiation Service Provider.
Source: (Evry, 2018[4]).

Another difference among the regulatory initiatives taken to promote open banking in different jurisdictions relates to how standardisation of APIs might be achieved. Such standardisation is essential to the smooth implementation of the initiatives and for limiting information technology investment costs, while facilitating interoperability and allowing greater reach and efficiency. There are questions however as to whether technical standardisation across different institutions and national markets will be achieved. At the same time, taking a non-standardised approach could in principle generate a faster pace of financial innovation.

PSD2 has left the issue of standardisation to private sector initiatives. However, in the United Kingdom, the Competition and Markets Authority (CMA) tasked the nine largest domestic banks to "adopt and maintain common API standards through which they will share data with other providers and third parties." In this context, an Open Banking Implementation Entity (OBIE) was founded in late 2016,[6] which delivered several API standards (one for payment, one for data aggregation, etc.) in early 2018. The declared aim is to create standards, and ensure that banks implement the standard consistently and that third parties can adopt the outcomes and build on them their own propositions as effectively as possible. A remarkable observation is that unlike standard bodies elsewhere, OBIE considers not only technical standards but also consumer experience. In the United Kingdom, the uptake of Open Banking remains low but the quality and performance of the open banking APIs has been improving. OBIE has been reporting an increase in the number of successful API calls (Figure 2.3) and a decrease in the API average response times (Figure 2.4).

Figure 2.3. Successful API calls, United Kingdom (June 2018 to June 2020)

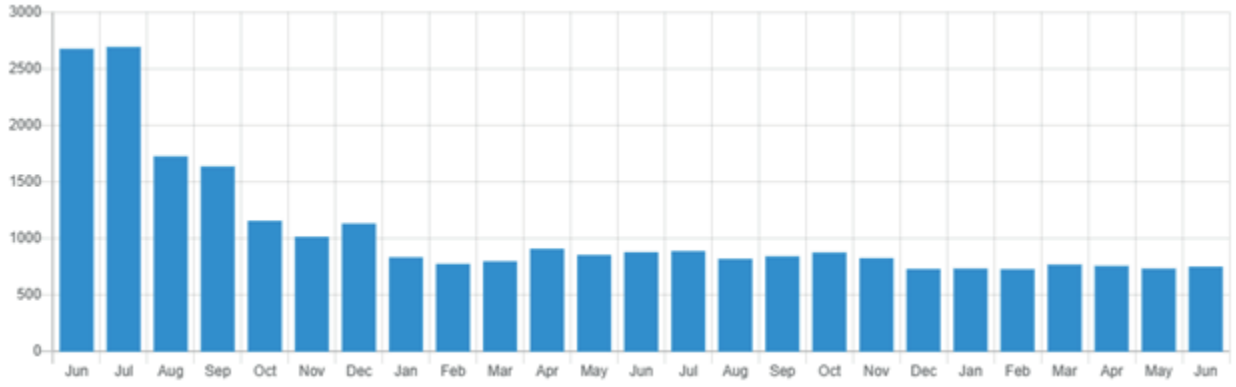
Number of successful calls made by TPP using account providers' Open Banking APIs



Note: TTP denotes third party providers. Successful API calls are based on data submitted by account servicing payment service providers (ASPSPs) to Open Banking in the United Kingdom. Data until July 2018 includes data from eight providers. August 2018 onwards includes data from 9 providers and 16 brands in total. In June 2019, the number of brands increased to 17. Since July 2019, there are 18 brands. ASPSPs are made up of the following banks, building societies and sub brands: Allied Irish Bank, Bank of Ireland, Bank of Scotland, Barclays, Danske, First Direct, First Trust Bank, Halifax, HSBC, Lloyds Bank, Marks & Spencer, MBNA, Nationwide, NatWest, Santander, The Royal Bank of Scotland, Santander and Ulster Bank.
Source: https://www.openbanking.org.uk/providers/account-providers/api-performance/.

Figure 2.4. Average API call response times, United Kingdom (June 2018 to April 2020)

Average response time for API calls made using account providers' Open Banking APIs



Note: See note to previous figure.
Source: https://www.openbanking.org.uk/providers/account-providers/api-performance/

In Australia, data standardisation under the Consumer Data Rights legislation, which includes an Open Banking component, will be set by a data standards body involving a governmental research organisation.[7] Australia's four major banks had been tasked with implementing an open banking standard by July 2019 and all other banks need to comply with these standards by July 2020. In Japan, banks have been encouraged to open up their APIs by May 2020.

To what extent sharing is mandated differs across jurisdictions. As noted in BCBS (2019[2]), mandated sharing can range from providing third parties with both "read" and "write" access to data (e.g. United Kingdom) to only providing "read-only" (e.g. Australia). For example, in the United Kingdom, there are two types of Open Banking APIs that the largest nine banks are mandated to implement and support: account aggregation APIs (allowing users to see a consolidated view of their banking accounts held with different institutions) and payment initiation APIs (allowing third party providers to initiate payments on behalf, and with the consent, of users).

One could describe *account aggregation* APIs as "read-only" because they can only display values, while *payment initiation* APIs are "read-write", as they can also change the underlying values. As shown in Figure 2.2, Account Information Service Provider (AISP) are authorised to retrieve account data provided by banks and financial institutions, while Payment Initiation Service Provider (PISP) are authorised to initiate payments into or out of a user's account. The latter function could rise additional challenges for banks compared to the former because "read-write" permissions also enable funds to automatically move between accounts. If multiple users choose to move their funds from the same banks, at the same time, liquidity issues could arise. In fact, by enabling funds to move around more seamlessly, in principle, deposits could become "flightier".

Facilitating switching by de-monopolising ownership of data: Benefits and selected challenges

A fundamental implication of open banking developments is putting customers in charge of their financial data, by requiring banks to share this data with authorised TPPs (note that banks are also able to act as AISP or PISP) if customers request it. This sharing of data could lead to the de-monopolisation of customer data.

A potential benefit is reducing the asymmetric information problem,[8] thus facilitating switching between financial services providers. Alternative financial services providers can find it difficult to offer better terms to the extent that they have incomplete information about potential new customers. By allowing customers to share information, thus limiting the asymmetric information problem, alternative financial services providers will be in a better position to assess risks as a result of which they may offer better terms than the bank of the existing relation.

APIs are instrumental in this context and tend to lower switching costs and increase contestability as they help consumers to compare products and services offered by financial services providers, while also helping the latter to assess the track records of customers. APIs provide the support for the increased unbundling of financial services from incumbent banks. By allowing the sharing of payments-related data, new financial services providers get access to customers and might offer similar services at lower costs, especially to the extent that they are unencumbered by legacy non-performing asset problems and high bank capital charges. They might benefit from open banking initiatives by being able to reach more customers at potentially lower cost. This could lead to a reduction in the fees for payment-related services. Greater switching and contestability seems also to incentivise incumbent banks to offer better terms to existing customers to maintain the relationship or to attract new customers.

Open banking initiatives allow customers to open up their own (payments, and in some cases also other) data history to third parties.[9] That data history has value, as it can reduce the asymmetric information problem, and new technology could be used for gaining richer insights from customer data. For example, the data can be an input into credit risk assessment, e.g. to compute credit scores, and price risk more accurately. By sharing data more widely beyond the perimeter of the customer bank, and allowing it to be aggregated and analysed, through big data analysis tools including artificial intelligence, credit risk assessments are likely to become more effective (see also Box 2.6).

As a result, credit scores might better capture actual affordability, and the latter might become more closely aligned with actual lending. This outcome, in turn, could foster financial inclusion, and some open banking initiatives are explicitly aimed at this outcome. Such an outcome is not guaranteed, however. In principle, more individualised and accurate credit risk assessment might also lead to the more effective exclusion of specific risks that are considered too high.

Box 2.6. Examples of links between consumer data sharing and financial inclusion

One essential element of financial inclusion is access to instruments that allow for borrowing. As regards the latter, opening up access to consumer data can help (i) determine the prospective borrowers' eligibility for finance in the event that they do not have, or are unable to prove, their credit history. For example, applications such as *Mojo Mortgages* combines open banking data with scoring methods to facilitate calculation of what customers can afford in terms of payment, while *Canopy* uses the history of consumer rent payments to facilitate improving their credit score. Access to consumer data can also ii) improve and speed up the lending decision process and iii) facilitate credit risk pricing that more accurately reflects actual risk profiles. Moreover, increased access to consumer data through open banking can iv) facilitate the risk management capacity of consumers. For example, applications are available in this regard and, for example, help consumers with lower wealth or incomes to smooth their income or wealth volatility and strengthen resilience to financial shocks. An example are automatic saving sweepers that calculate, based on the consumers historical data, what the consumer can save and then automatically transfer funds to dedicated savings accounts, e.g. to constitute some buffers for adverse financial shock or to finance upcoming purchases. Effectively, otherwise more volatile income streams are smoothened as a result of the use of such instruments. This observation is noteworthy, as it is clear that greater financial inclusion is desirable, but also requires consumers to acquire additional skills and abilities. In this regard, appropriately designed applications can assist in the management of the new and different risks that might be associated with more widespread access to financial products and services stemming from increased financial inclusion.

Considered as a production factor, one key characteristics of data is that it is non-rival: A customer's transaction history, payment record, medical record etc. can be used by any number of firms simultaneously and over and over again without being depleted. This characteristic implies that the potential economic gains from data usage can be particularly large, which is why some authors have argued that policy makers should not see privacy protection as the sole goal in answering questions such as the ones raised above (Jones and Tonetti, 2018[5]). At the same time, the need for protection of data ownership has been highlighted as part of the interactions between public sector officials and Facebook representatives following the company's announcement of its project Libra.

The use of digital data for the development of financial services is likely to become more important over time. As a result, difficult questions regarding the balance between the economic value and exploitation of personal data on the one hand, and privacy protection on the other have to be answered.[10] Who should ultimately own the data and what restrictions should apply to its use (see also Box 2.7)? Should the data be available on an immutable ledger forever or should there be a right for individuals to have their personal data to be forgotten if they so request? Yet other questions relate to the capacity of investors or financial consumers to evaluate and compare different types of services (Box 2.8). Addressing these various questions requires one to undertake a careful evaluation of efficiency, consumer protection and privacy considerations in the use of data as a production factor.

Box 2.7. Trade-off between efficiency and privacy considerations regarding data usage

Many firms, including technology companies with established presence in the market for digital services (BigTechs), specialize in collecting, processing and re-selling personal data to other firms that operate in various markets, taking advantage of advances in computing and communications technologies to store and process personal information. As a result of these developments, privacy is effectively reduced, while social mechanisms to prevent misuse are only being developed. In this context, a fundamental question is whether and how property rights should be defined over the use of personal data (Dosis and Sand-Zantman, 2019[6]).

Responses to this question across jurisdictions differ, not least as privacy is understood differently across individuals and jurisdictions. In this regard, on a fundamental level, Acquisti, Taylor and Wagman (2016[7]) distinguish i) the protection of someone's personal space and their right to be left alone ("seclusion"); ii) the control over and safeguard of personal information, which might involve the data subject getting paid for its data ("property"); and iii) an aspect of dignity and human freedom ("autonomy"). For individuals whose primary concern is seclusion, protection of their property will not suffice. For example, an individual who cares about seclusion will consider the receipt of any e-mail spam as a critical privacy violation, while one who cares about property may be satisfied to receive payment or discounts in exchange for receiving spam. Autonomy is an issue if people find their behaviour is constrained by their concerns that their behaviour is being tracked. While different, the various interpretations of privacy share the observation that they pertain to the boundaries between private on the one hand and shared or, in fact, public, on the other. In fact, the economics of privacy concerns the trade-offs associated with the balancing of public and private spheres between individuals, organizations, and governments. In this regard, much attention focuses on the informational dimension, that is on the trade-off arising from protecting or sharing of personal data.

Many jurisdictions with open banking initiatives also updated or plan to update their data protection and/or privacy laws (Basel Committee on Banking Supervision, 2019[2]). For example, the European General Data Protection Regulation (GDPR) stipulates the principle that privacy is a basic human right, which is why the creation of explicit markets for rights over data is not allowed. That said, to circumvent the issue of ownership, firms specialising in data collection and processing, as well as regulators of those and other firms, tend to avoid direct references to ownership but instead focus on the potential controls of a data subject or the limitations of a data controller. In fact, in Europe, data privacy laws are based on the principle that both the customer owns their data and has the right to control it. Somewhat different from the GDPR, other legal frameworks view banks, and sometimes third parties, as the data owner. That said, they might nonetheless limit their rights to control the use of such data to the boundaries of the consent provided by the customer. Many jurisdictions' consent rules also place restrictions on downstreaming data to fourth parties, and on reselling customer data for purposes beyond the customer's initial consent (Basel Committee on Banking Supervision, 2019[2]). Thus, consumer consent to the usage of their data is a widely accepted principle. That said, identifying what is "personal data" is challenging. For example, the distinction between the "personal data" and "non-personal data" is rather unclear and, for example, "non-personal data" is excluded from the scope of the GDPR. Furthermore, anonymized datasets can potentially be de-anonymized, blurring, even more, the frontier between personal and non-personal data (Dosis and Sand-Zantman, 2019[6]).

Tensions might exist between economic efficiency and privacy considerations. On the one hand, the sharing of customer data by banks with Third-Party Providers (TPP) allows the latter to build applications and services that are potentially faster, more convenient and cheaper. The cost of processing and storing data continues to decline and data usage is non-rival as production factor. Data could be used over and over at little cost. Admittedly, consumer consent is a precondition for data

usage, but for a consumer to make informed decisions about its privacy can be complicated as the consumer often does not understand when data is being collected, for what purpose and with what ultimate consequence. Initially, the data subject may know something the data holder does not know, but disclosing its data can cause a reversal of informational asymmetry. Disclosing information might generate some immediate benefits, for example in terms of greater convenience of using services, but the ultimate costs in terms of reduction of privacy are less clear. In this context, an important aspect of open banking frameworks are provisions related to whether TPP can share and/or resell data to "fourth parties", whether they can use the data for purposes beyond customer's original consent (e.g. by including inferred data generated by algorithms or forecasts) and whether banks or third parties could be remunerated for sharing data. In fact, nearly all BCBS jurisdictions restrict third parties from reselling or using data for purposes outside of the scope of the consumer's initial consent, although third parties could provide data to fourth parties as long as this is specified in contractual arrangements (Basel Committee on Banking Supervision, 2019[2]).

The scope of customer data accessible by authorized TTPs varies depending on the specific jurisdiction's implementation and legislation. For instance, in the EU open access is limited to payment account data excluding other kind of data (e.g. on credit cards), while in the United States the so-called consumer financial data aggregation services include a wider set of data. Brazil foresees a particularly wide scope for data sharing in terms of the types of financial services concerned, including deposit accounts, credit cards, credit operations, investments, etc. To the extent that TPP are entities that do not have contractual relationships with banks, oversight and monitoring by banks is challenging and/or bank supervisors may have limited or no direct oversight of these third parties (Basel Committee on Banking Supervision, 2019[2]), making it difficult to monitor adhesion by TPP to data usage standards. Bank supervisors expect banks to have bilateral contracts before sharing data in jurisdictions that do not require third parties to be authorised or licensed.

One additional issue is whether regulation should aim at establishing a level playing field and what a level playing field means when different activities may entail different levels of risk.[11] In this context, one controversial issue continues to be that of so-called reciprocity, by which banking sector representatives mean that there might be an asymmetry in the requirements for data sharing across entities from different sectors, including banking sector on one side and the information technology sector on the other. PSD2, the argument goes, has created a particularly demanding regime of data access from banks by obliging them to provide payment data to non-banks, without allowing the former to charge for it. By contrast, similar requirements for (large) information technology to make their own core customer data shareable with third parties including banks does not exist. Note however that many public initiatives to encourage greater data sharing might have focused initially on specific financial services, but are not meant to be limited to these.

Another concern expressed by representatives from incumbent banks is that relatively smaller entities that become part of the supply or value chain as data aggregators or intermediaries could have less well developed (cyber and other) risk management systems in place. That said, it could also be argued that the opposite argument applies, namely that the new firms are particularly technology savvy and as such use state-of-the-art technology as opposed to the much older one used by incumbent banks. Furthermore, the additional and new interconnection points created by APIs could generate additional vulnerabilities. In fact, personally identifiable data are increasingly being collected and shared between various entities and/or stored in different locations, with common credentials used across different platforms. As a result, concerns regarding cyber-attacks, data theft and fraud might become more relevant. Whether such and other operational risks applying to new financial services providers such as Fintechs are smaller or larger than the same risks from incumbents is not clear *a priori*.

Some of the largest reported data breaches in terms of accounts affected have involved incumbent financial institutions.[12] Moreover, concerns of incumbents regarding new entrants are less justified where the Fintech entities are regulated and required to have adequate systems in place. It is also worth noting

that APIs remove the need for screen-scraping (PSD2 even explicitly bans it), which is a practice used by third-party providers to access user account information by requesting (and sometimes storing) customers' banking login details in order to collect screen display data from one application and translating it so that another application can display it. APIs help increase the safety of the personal data customers choose to share by removing the need for TPPs to login on behalf of customers and they substantially reduce the type of operations TPPs can conduct on behalf of customers. Instead, APIs offer a safe and secure environment in which data can be shared allowing users to have oversight and transparency of the data they share with TPPs (as well as allowing for customers to revoke access to their data at any time). Reputational risk might also be lowered by reducing the sensitivity of the data unauthorised parties might be able to get access to.

Given the inherent risks in sharing data and creating new linkages between entities, it is critical to develop processes and governance mechanisms that accompany the development of new technical and data connections. APIs are not new but open banking is likely to increase the speed and volume of data sharing. A key required feature for this new infrastructure will be to embed privacy into its design from the outset. Such an approach involves giving customers clear and easy-to-understand information as well as control over how, when and with whom their personal information will be used and shared.

There is also need for protection of data ownership and a clear liability structure to accompany the transformation process. In fact, open banking initiatives recognise that the opening up of access for third parties to bank customer data raises the question as to who bears responsibility in case of breaches of privacy laws and/or fraud. For example, according to PSD2, in principle, if financial consumers notice a payment that they did not authorise, they are entitled to make a claim against the bank, even if the payment has been initiated through a third-party provider. If the third-party was at fault, the bank can recover funds from the latter.

Box 2.8. Issues related to the capacity of consumer to evaluate products and services

Consumer funds safeguarding measures

Financial innovation, facilitated among other things by open banking, also raises consumer protection issues when it comes to the safety of consumer funds. For example, even if not strictly a consequence of open banking initiatives, innovative products and services such as online money market funds (such as e.g. *Yu'e Bao* in China) or electronic money accounts (such as those offered e.g. by *TransferWise* in Europe) are not covered by deposit insurance from the jurisdictions in which financial products are offered. To the extent that consumers are aware of this situation, the absence of the deposit insurance could expose the financial services providers to a more pronounced risk of runs.

Yet, it cannot be excluded that consumers might also be unaware of this lack of protection and might even assume the existence of implicit guarantees. Such perceptions would be distortive and, to the extent that the service providers are sufficiently large and/or owing funds to unsophisticated retail customers, might under some circumstances even induce public authorities to vindicate such expectations ex post in case of the entities experiencing financial distress. The recent example of the political decision in one jurisdiction to partially refund retail investors of small banks, rather than fully bailing in *all* subordinated debt holders, is a reminder of the difficulties in bailing in households even in situations where such bail-in is a declared policy goal. Such difficulty seems to arise in particular to the extent households might not have fully appreciated (or even be misinformed about) the risks associated with the financial instruments they had been offered by financial services providers.

There are various instruments in place to protect funds when they are not covered by deposit insurance. For example, to protect customer funds held by an e-money issuer, there are functionally equivalent mechanisms to deposit insurance available to protect customers in case of failure. Beyond risk-based

prudential regulation and supervision, these include fund safeguarding measures such as ring-fencing and segregation. Segregation requirements involve keeping funds separately, including from the e-money issuer's own funds. Ring-fencing provides an additional layer of protection by requiring funds to be kept in a trust or custodial account and segregated from other assets of the trustee or custodian managing the account on behalf of e-money customers. Despite such safeguards, e-money customers remain exposed to a non-zero risk of losing money. Against this background, the question has been raised to what extent and how deposit insurance might apply to e-money, which is particularly relevant for some emerging economies where e-money accounts are more prevalent than bank accounts (Izaguirre, Dias and Kerse, 2019[8]). As a general rule, third parties in open banking do not hold customer funds in the same way as banks do, so that the issue of e-money fund protection is different from that of protection of balances in accounts at deposit-taking banks that face strong prudential regulation and supervision.

Addressing limits to consumer financial literacy

Beyond the specific issue of safety of funds or deposits, the relationship between financial consumers and their banks is changing in more fundamental ways. Responsibility for initiating some transactions is being shifted away from banks and towards their customers and the providers of apps that are being used by the customers. A positive outcome would be the availability and use of apps that facilitate good financial management, for example, by aiding debt avoidance, automating saving, facilitating the identification of personal product matches and even automating regular switching between financial services providers. These services can be time-saving and financially beneficial.

There are, however, questions about how consumers can evaluate and compare different services and apps (especially when the underlying algorithms are not revealed), as well as – more fundamentally – to what extent they are capable of using the new opportunities to their own benefit. Obviously, consumers need to have a minimum level of digital and financial literacy to be able to take advantage of these services.

To facilitate the design of adequate consumer protection policies, high-level principles were developed by the G20/OECD Task Force on Financial Consumer Protection as a response to a G20 Finance Ministers and Central Bank Governors call in February 2011. Following the endorsement of the Principles by G20 Leaders (in 2011) and OECD Governments (in 2012), the Task Force engaged in the development of effective approaches to implement the Principles in the current digital environment. The Principles are also expected to be reviewed and revised in the coming two years to reflect market and regulatory evolution.

Potential market structural effects of open banking

Further unbundling of the economic functions provided by incumbent banks

Open banking needs to be seen as part of the broader wave of financial innovation based on the use of digital technologies and big data. Finance has a long history of making use of technological advances, and thus the combination of the two is not new. What is new however is the rapid pace at which new digital initiatives in a wide range of financial services have developed during the past decade, with recent policy initiatives such as open banking perhaps having accelerated that pace.

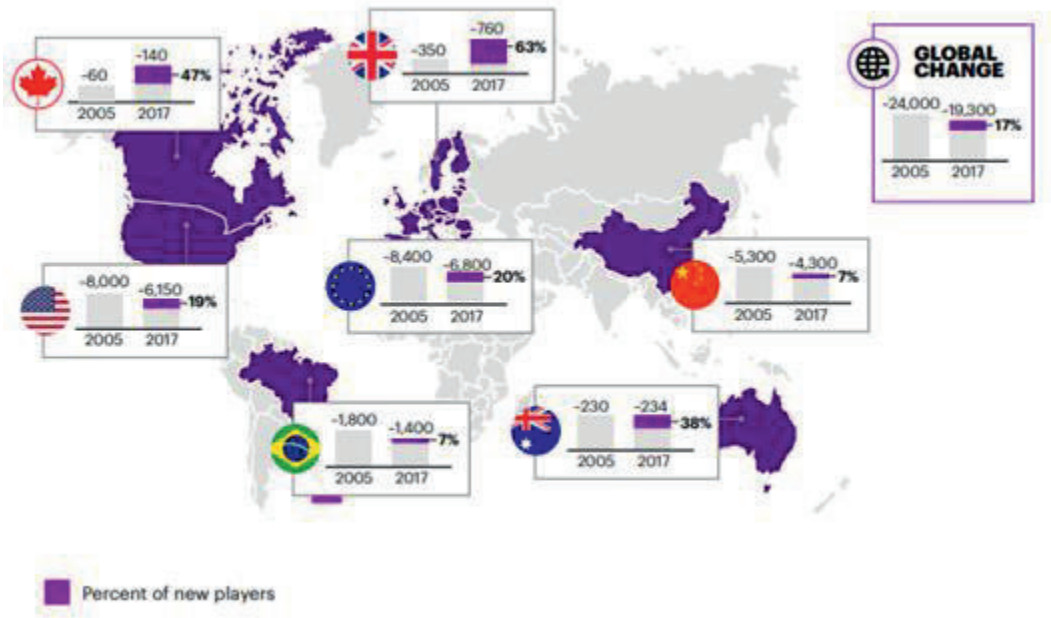
For about a decade, the confluence of disenchantment with the performance of incumbent banks, the regulatory response to the global financial crisis and the evolution of information technologies have provided a powerful mix to facilitate Fintech initiatives to challenge established banks' and other financial institutions' pivotal positions in providing various economic functions.

Much of the current structural transition is driven and accompanied by technological advances, including distributed ledger technology and artificial intelligence, which promise to make more efficient use of data in providing financial services. At the same time, demographic developments and changes in consumer expectations have meant that there is greater demand for the provision of more convenient, individually-tailored and, perhaps, cheaper financial services. Especially the development of smartphones and their widespread proliferation have facilitated the unbundling of many of the activities traditionally performed by banks.

Many of the economic functions traditionally performed by incumbent banks are being unbundled by Fintech initiatives (Lumpkin and Schich, 2020[9]). This development has been reflected in new entrants providing payment services (Figure 2.5) and absorbing some of the revenues from incumbent banks. Also, valuations have further risen for so-called Fintech unicorns (Figure 2.6), that is for companies with a private market valuation exceeding one billion USD, to more than USD 200 billion at end-2019, compared to less than USD 150 billion at the beginning of the year (CBInsights, 2019[10]).

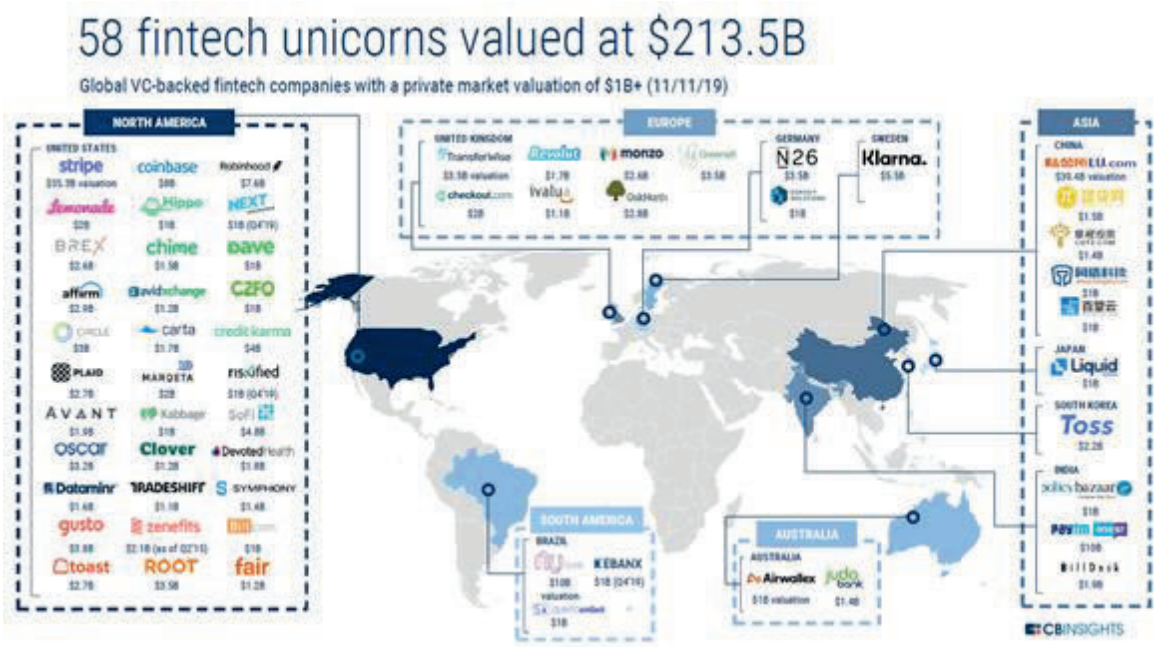
Open banking facilitates the unbundling of payment services from the overall bundle of economic services traditionally provided by banks, in particular regarding payments.[13] To the extent that more economic functions traditionally performed by banks are also provided by other entities (Box 2.9), incumbent banks tend to become more easily *substitutable* in an economic sense. To what extent they also become less special in the sense of meriting the full backing by the financial safety net provisions is another issue discussed separately (see e.g. (Lumpkin and Schich, 2020[9]) and (Schich, 2019[11])).

Figure 2.5. Market penetration of new entrants



Note: Percentage in terms of total number of entities with banking and payment license.
Source: (Accenture, 2018[12]).

Figure 2.6. Rising market valuations of new entrants



Note: "Unicorns" is the term used for companies with market valuation exceeding one billion USD.
Source: (CBInsights, 2019[13]).

Box 2.9. Limits to how far banks' economic function can be unbundled

There might be limits to how far the unbundling of the economic functions performed by incumbent banks can go, however. Banks continue to differ from other financial intermediaries in that they provide a very specific mix of three core economic functions (Lumpkin and Schich, 2020[9]). They include that banks offer transaction accounts withdrawable on demand (first economic function) and that they provide liquidity to other banks and the economy at large (second economic function). Incidentally, performance of that second economic function effectively implies that banks engage in maturity transformation, given the first economic function that they perform. Note in this context that lending as such is not one of the three core functions; other entities provide that function. The third core economic function that they perform is to act as conduits for the payment system and monetary policy transmission, although it is also conceivable to consider the payments and monetary-policy-transmission function as two separate economic functions.

In fact, while the payments function is being challenged through open banking initiatives, the monetary-policy-transmissions function is not, at least not to the same extent. To perform the latter function, given the current monetary system, banks need to be able to undertake maturity transformation, so as to allow the availability of money to be flexible, going well beyond stocks of central bank money, when demand for money is strong. This system is considered efficient by central banks. Without any fundamental changes to that system, it is difficult to see how the latter core economic function could possibly be performed by Fintech initiatives.

The strategic response of banks to unbundling and revenue pressures

Other things equal, the result of increased competition and contestability in retail financial services will likely be that incumbent bank profits in retail payments could come further under pressures, especially as retail payments used to be an important source of revenues (Petralia et al., 2019[14]). Banks in turn might react to these pressures – which are further amplified by the effects on bank asset quality and profits from the fallout of the Covid-19 pandemics -- by cutting costs and/or changing their business models in an attempt to offset the effects of lower profits (or raise profits from new sources) or by limiting effective competition.

Incumbent banks may try to limit expansion of new entrants e.g. by using new bundling or tying strategies, although such strategies are difficult to maintain when the products or services are sufficiently independent (Vives, 2019[15]). This situation seems to describe payment-related services, which seem to be sufficiently independent from other services such as lending etc. However, where the incumbent uses its market power to limit entry, such practises might be anti-competitive. In this context, an interesting observation is that a number of competition agencies have adjusted their merger notification thresholds in order to allow them to investigate cases in which there are concerns that incumbents might purchase smaller start-ups in order to limit potential competition. In fact, a common strategy is for incumbent banks to partner with new entrants, acquire them or invest in them (Lumpkin and Schich, 2020[9]).[14]

Identifying new sources of revenues in the current environment of low interest rates and flat yield curves appears difficult and not all incumbent banks will be able to recuperate lost revenues through the creation of revenues elsewhere. In this regard, there seems to be some regional differences. Put simply, incumbent banks in Europe and Japan have reportedly been using technologies initially with a sharp focus on reducing costs. By contrast, banks in China and other emerging markets have been using them to a greater extent already to create additional revenue streams, as part of which they tend to foster financial inclusion, which tends to be more limited than in many mature markets (S&P Global, 2019[16]).

Part of the specialised Fintech press continues to pit new digital banking initiatives against incumbent banks, suggesting that the competitive pressure from the former implies the inevitable exit from the market of some of them at least.[15] In response, some incumbent banks may decide to take on more risk in other areas in an attempt to "*gamble for redemption*", and materialisation of risks might turn out to threaten solvency. To the extent that effective resolution mechanisms are available to allow an orderly exit of some incumbents from the market, such an outcome would not be of much policy concern. Clearly, such a consideration applies not only to incumbent banks, but also to new entries (see Box 2.10). The possibility of a messy exit of either incumbent banks or new entries would be a concern, however. In fact, in this context it is worth recalling that there are some uncertainties about how smoothly the newly available resolution tools can be applied to large incumbent banks in actual practise.

Incumbent banks might also respond to competitive pressures by changing their own business model and corporate structures, perhaps resulting in a smaller footprint and less complexity. For example, according to CBInsights (2019[17]): "With virtually every core function of traditional investment banking under siege, banks are rushing to launch products, restructure, and sell off unprofitable units. For many banks, downsizing or otherwise modifying their original growth ambitions will be the natural culmination of a decade of change and turbulence." In fact, if indeed incumbent banks were getting "smaller and leaner", this development would in principle help make entities more resolvable, thus facilitating any orderly exit. Empirical evidence in favour of significant progress in this regard does not yet appear to be overwhelming, however.

Nonetheless, to the extent that new financial services providers, including Fintech and Bigtech, fill in and provide similar financial services instead, incumbent banks become more easily substitutable. Thus, other things equal, they should be able to exit more smoothly the market in case of financial distress, which is desirable as it would tend to limit the too-big-to-fail (TBTF) problem that tends to distort competition and

risk-taking incentives. The TBTF issue explains the prevalence of implicit guarantees for the debt of at least some banks, which in turn explains in part why excess rents might have been earned by incumbent banks. In fact, such rents can be considerable, attracting more funds into the banking sector than might be merited by considerations of financing real economic activity alone (Denk, Schich and Cournède, 2015[18]). Open banking initiatives tend to limit such rents, although it is not so clear yet whether and to what extent such rents earned by incumbent banks have yet been compressed.

Box 2.10. The need to focus on (potential) exit when considering entry

The crucial role of exit for an efficiently functioning financial system has been acknowledged, especially given the experience with the global financial crisis where arguably smoothly functioning exit mechanisms for large, interconnected and complex financial intermediaries had been unavailable. In fact, regulatory authorities are considering the issue of (credible plans for potential) exit when considering the issue of entry into financial services provision. For example, the Hong Kong Monetary Authority has defined a new category of financial services provider referred to as "virtual banks". To obtain such a license and being able to offer the specified financial services in Hong Kong, China, entities must fulfil a number of requirements, including the specification of an "exit plan" (paragraph 20 of (Hong Kong Monetary Authority, 2018[19])). "As virtual banking is a new business model in Hong Kong, China, the Monetary Authority will require a virtual bank applicant to provide an exit plan in case its business model turns out to be unsuccessful. The purpose of the exit plan is to ensure that a virtual bank, should it become necessary, can unwind its business operations, in an orderly manner without causing disruption to the customers and the financial system. In general, an exit plan should cover matters including the circumstances under which the plan will be triggered, the authority to trigger the plan, the channels to be used to repay depositors and the source of funding for making the payments." Altogether eight new licenses were extended to entities that met these conditions (Box 2.3). Of course, only time will tell how effective resolution will be in practise. In any case, it is clear that in order to be able to reap the benefits of open banking initiatives, it is vital to ensure that new entries into the financial services sector can also smoothly exit if they fail.

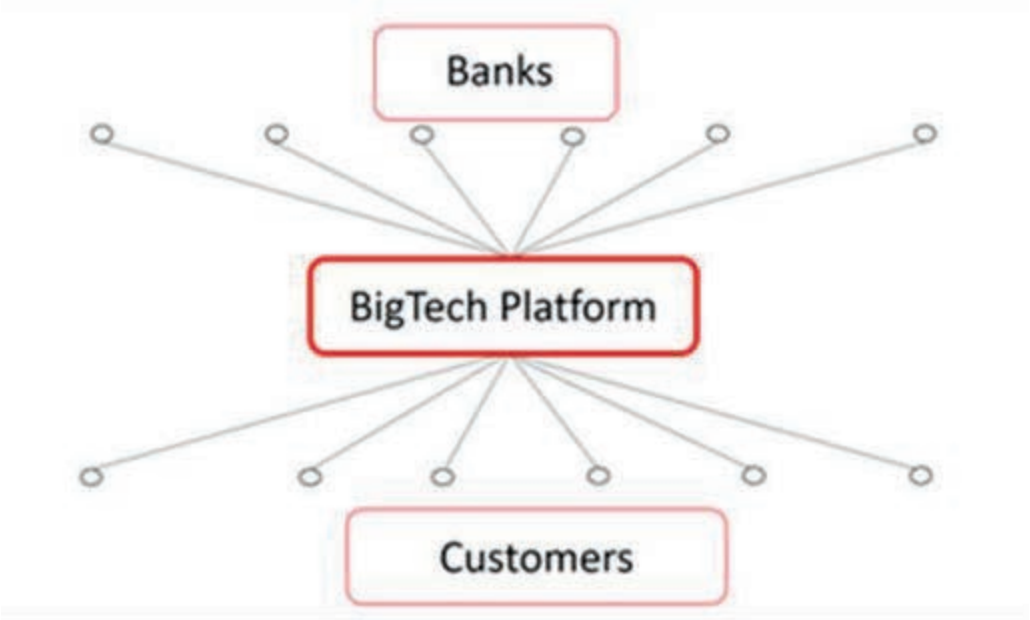
Open banking to act as catalyst for Bigtech growth in financial services?

Open banking implies giving access to the existing payments infrastructure and data to third parties. These third parties could be other banks, Fintech firms or Bigtech. To the extent that the latter make use of open APIs, and given Bigtech firms' well-developed capacity to collect and exploit large amounts of data, they might become formidable challengers in payment and perhaps other financial services (Box 2.11). As a result, increased competition or contestability is likely to lead to lower prices for financial services, at least initially.

It cannot be excluded that open banking initiatives could function as a catalyst for faster growth of Bigtechs to the extent that the latter can take advantage of the opening up of access to payments data of bank customers. The latter have established networks and accumulated big data from mostly non-financial activities (for example, Amazon on sales of merchants and Apple on payments through its ApplePay) and have already gained a foothold in financial services in some jurisdictions, particularly in retail payments. BIS (2019[20]) draws attention to the characteristics of the business model of Bigtech firms, referred to as "DNA" (data analytics, network externalities and interwoven activities), which allows them to scale fast. For example, Google Pay has absorbed almost a third of total Unified Payments Interface transactions in India. Open APIs allow third parties to obtain parts of customer bank data and even initiate transactions. For example, provided consumers agree to do so, their Amazon purchases could be paid directly from their bank accounts. With open banking, Bigtech firms can use banks to some extent as an invisible back office for their financial services, thus changing traditional banking relationships.

While initially a welcome source of contestability of markets and competition for established financial institutions, it cannot be ruled out that Bigtechs are becoming a large share at the detriment of competitors in some market segments, resulting in an increased concentration in those segments. For example, in China, just two firms account for 94% of the overall mobile payments market, which might raise efficiency concerns over the longer term. In particular, to the extent that a Bigtech platform manages to monopolise the interface with customers (Figure 2.7), the short-term beneficial effects for competition in financial services could be overturned by adverse competition effects in the long run (Vives, 2019[15]), as well as giving rise to financial stability concerns (Annex 2.A).

Figure 2.7. Bigtech monopolising customer interface



Source: (Vives, 2019[15]).

To ensure that new entries gain scale for the appropriate economic reasons requires at a minimum a joined-up approach of competition and financial-stability authorities. BIS (2019[20]) warns that if a Bigtech has established a captive ecosystem, potential competitors might have little scope to build rival platforms. In principle, dominant platforms can raise entry barriers and exploit their market power and network externalities to increase user switching costs to exclude potential competitors. However, it is not yet clear that financial services involve the same strong network effects that are found in digital platforms, nor that market power in those digital platforms can be easily used to exclude rivals to their own financial services.[16] While there is no strong evidence of Bigtechs hindering potential competitors' provision of financial services on their platforms so far, some practises of Bigtechs have been considered anticompetitive. For example, Google was fined in March 2019 following a finding by the European Commission that the company had discriminated successfully in their central platform in favour of their own (vertical) affiliates or to protect the dominance of its own search engine and operating system.

Box 2.11. Bigtech in financial services

One development consists of large non-financial firms, such as technology, telecommunications, and e-commerce firms, becoming increasingly active in providing financial services, often starting with payment services. Such firms are often referred to as "Bigtechs" to highlight that they are technology companies with established presence in the market for digital services. Bigtechs have been offering financial services for some time now and thus provided some (welcome) competition to incumbent financial services providers in several niche financial services areas.

In fact, the core of financial services can be said to be information processing, which is why banks have used technology and data throughout their existence. That said, a subtle difference in the approaches to the use of technology and data could be identified between banks on the one hand and Bigtech firms on the other as part of the most recent episode of heightened interactions between finance and technology (Arner, Barberis and Buckley, 2017[21]). Banks start from their relationship with customers and subsequently supplement their risk analysis by using, in addition to the data collected as part of these relationship, more broadly derived data. By contrast, Bigtech firms start with their data and relationship with a large number of customers in a non-financial-services environment, collect large amounts of data from those relationships and then move on to use the data and insights for activities related to financial services.

Traditionally, banks may have had the most accurate and detailed digitalised information about their financial services customers, which also meant that they were best placed to analyse the information and data so as to price financial services for these customers. This information advantage might not continue to hold, however. Bigtech firms collect and aggregate information about users' activities through their software use and internet search activities (e.g. Microsoft and Google), about usage behaviour and location through hardware (e.g. Apple), about social preferences through social media activities (e.g. Facebook), about consumer demand, payment history and merchant sales through e-commerce (e.g. Amazon), and on mobile activities through telecommunications services providers. The data provided by each of these sources typically covers a large proportion of the population of the reference market segment and is often very comprehensive in terms of the data points that can -- and are -- being collected with respect to any given individual. Moreover, by matching and combining data from these different sources, even more comprehensive databases can be created.

Bigtech firms typically have established large customer networks in non-financial services, including social media, and they attempt to capitalise in providing financial services on the economies of scale and scope offered by technology, which includes but is not restricted to network effects. For example, Bigtech firms could use proprietary customer data generated through social media to tailor offerings of financial services and products to individual customers' preferences. Moreover, given their often strong financial positions and the potential to cross-subsidise from non-financial services, Bigtech firms could operate in financial services with lower margins and prices than both incumbent competitors or smaller Fintech firms.

Bigtechs can compete with incumbent banks either by becoming banks themselves or as multi-sided platforms (marketplaces) focusing on the most profitable banking activities. So far, Bigtech firms have mostly stopped short of becoming or acquiring banks, although Bigtech firms have been behind some of the virtual banking licenses granted by the HKMA since 2018 (Box 2.3).

Selected considerations, open issues and recent developments

Considerations regarding the monitoring of the structural implications of open banking

It is too early to attempt to draw definite conclusions regarding the effectiveness of open banking initiatives, not least because regulatory changes have only recently taken place and the effects of such initiatives are difficult to isolate from other developments including in particular technological advances. A recent survey on open banking by the BCBS (2019[2]) concludes that open banking is still at early stage in many jurisdictions and that "approximately half of the [BCBS] Committee members have not observed significant open banking developments in their jurisdictions."

This outcome is commonly attributed to the weak demand as a result of limited awareness of consumers of the options available to them. It can however also not be excluded that at least some consumers are aware of the options but concerned about sharing their data. The fundamental idea of open banking is to allow customers to share information, thus allowing alternative financial services providers to be in a better position to assess risks as a result of which they may offer better terms than the bank of the existing relation. Obviously, consumers may not want to share their data, as they may be concerned pricing and availability of services available to them might become even less favourable. Yet another explanation for the relatively weak demand on the part of consumers for the new options created by open banking might be a lack of trust in newcomers. To the extent that certification processes scrutinize third party's protocols and that third parties' capabilities are periodically assessed, additional confidence is however generated. Also, public authorities might also need to invest further in developing materials and information targeted both at consumers and perhaps also at Fintechs that may not have the same level of resources to devote to the issue as incumbent banks or Bigtechs.

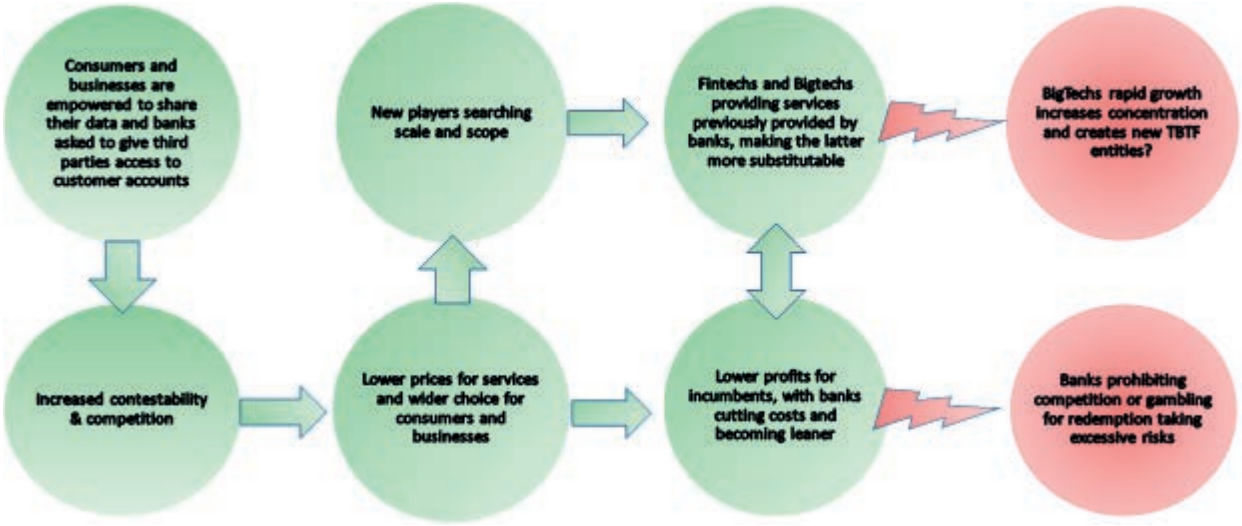
The framework for data exchanges continues to evolve, which also explains why it is too early to arrive at definitive conclusions. For example, in the European Union, banks had to be compliant with PSD2 by September 2019, although the initial Regulatory Technical Standards (RTS) for PSD2 published in November 2017 do not provide specifics about technology. It instead aims to be "technology and business-model neutral" so as not to stifle innovation, although the European Banking Authority (EBA) develops related standards. Some private initiatives to develop standards for open access have been created although it is noted that such different initiatives may lead to the risk of a fragmented market for open access and perhaps imply an altogether slower progress in the implementation of innovative solutions. Moreover, the framework for data exchanges is likely to evolve as the ongoing debate on the issue of so-called reciprocity evolves (see also section 3).

The outcome of the various developments depends on the regulatory policy actions. Tensions can arise where institution-specific regulation interferes with the dynamics created by the financial system's attempt to provide specific economic functions in a more efficient way. Regulating according to activities may foster innovation and the current policy consensus seems to be that innovative activities should not be blocked as long as they are not obviously mainly motivated by regulatory arbitrage. Micro-prudential regulators should maximise efficiency gains through Fintech and Bigtech further entering financial services while minimising the potential for these new firms to be seen as benefitting from bypassing costs and constraints of regulation. The difficulty with this approach is however that the demarcation line between different activities is not easy to draw and seems to evolve over time and sometimes very fast; as a result, a too narrow focus on activities is problematic, as it is not activities but entities that fail and might even generate systemic risks.

As a preliminary concluding observation, open banking initiatives have been successful in bringing about structural changes in the banking sector, fostering competition through the sharing of data. This, in turn, helps to improve the quality of products and services and lower their production costs. That said, as discussed in section 4, the opening up is not without risks, including in relation to strategic responses of incumbents and potential risks created by new market participants. In this context, it is worth mentioning

that the Covid-19 fallout in terms of adverse effects on bank asset quality and profitability adds to the somewhat more gradual pressure arising from open banking initiatives for bank profitability. Taking a more long-term view of the structural changes set in motion by open banking, Figure 2.8 provides a stylised summary view of different scenarios regarding medium to long-term effects on market structures and selected risks. This stylised framework could guide future monitoring of open banking developments.

Figure 2.8. Stylised summary of potential longer term structural effects of open banking



Notes: The stylised description above focuses on longer term structural financial system effects; it thus does not explicitly focus on issues of consumer protection as such. In fact, while a key aspect of open banking is an enhanced ability of the consumer to make use of her data, it cannot be excluded that consumers are not making the best use of this possibility, and this situation could raise financial consumer protection issues (see Box 2.8).
Source: OECD Secretariat assessment.

Covid-19 as catalyst for decisive change from cash to digital payments?

The Covid-19 pandemics further complicate the assessment of the effects of open banking. Among other things, the pandemics and related containment measures have implications for digital payments as opposed to the usage of physical cash. The Covid-19 pandemics and the containment measures taken to limit its spread represent a massive adverse external shock, affecting both economic supply and demand. A distinctive characteristic of the present episode, as compared to previous epidemic episodes, is that the spread of the virus has hit most major economic areas and not just a few geographical areas. While the initial economic effects of the epidemics might have consisted more of a supply shock (with domestic and global supply-chains affected), subsequent containment measures have directly targeted social behaviour and thus adversely affected economic demand. This description holds for all economies with open banking initiatives.

Many of the confinement measures taken at the peak of the pandemics involve attempts that effectively limit physical contacts, often referred to as “social distancing” measures. This term might be somewhat misleading given that the attempt is not to limit social contacts per se. The purpose is to limit social contact involving physical closeness between people, e.g. as opposed to social contacts via telephone, video or social media communications. Reducing the extent of the former type of social contact, the spread of the virus causing the disease Covid-19 can be limited. In particular, the virus infects and replicates in people’s airways and transmits from person-to-person mainly via respiratory droplets, if in close physical contact. In addition, it may also be possible that a person gets infected by touching a surface or object that has the virus on it and then touching its mouth, nose, or eyes.

The pandemics and the policy response to it have implications for physical cash usage.[17] There already has been a global trend, with a few notable exceptions, towards increased use of digital payments and reduced cash usage for transactions, and this trend might be accelerated by recent developments. In fact, even if the precautionary holdings of cash increased, which is typical of periods of heightened economic uncertainty, the usage of cash for payments declined during the pandemics period (Shin, 2020[22]). Many of the Covid-19 containment measures discourage physical contact. Thus, to the extent that the purchase of goods and services involving physical encounters become fewer, the need for the use of physical cash to pay for gods and services also becomes less. Moreover, there are concerns that the hand-to-hand exchange of physical currency could help transmit the coronavirus, and such concerns might further discourage the use of cash. In China, authorities reportedly disinfected and even destroyed banknotes that may have circulated through high-risk areas such as hospitals and food markets. In the United States, the Federal Reserve reportedly initiated quarantine measures for physical US dollars from Asia.[18] It is not unreasonable to assume that physical currency can play a role in spreading the virus underlying Covid-19.[19]

Some shops reportedly refused to accept cash payments during the Covid-19 pandemics, demanding that customers pay by card only, and these developments contributed to a further decline in the use of physical cash.[20] Against this background, public authorities intensified efforts to ensure that people who rely largely on cash, and may not have a bank card, continue to be able to pay for essential goods and services during the Covid-19 pandemics. Limited availability of cash raises payment inclusion concerns (Access to Cash Review, 2019[23]). For example, in Sweden, where there has been a pronounced trend decline in cash use, the central bank issued already in May 2016 a press release warning of the risks of switching over too rapidly to a cashless society. Similarly, Liikanen (2016[24]) notes: "*But the payment system is a utility which must be accessible to everybody, not only the majority of people. It must be inclusive. So that raises the issue of how social groups with special needs can cope without the option of cash*."

In addition, against the background of the observation that households and firms make less and less use of money issued by central banks to pay for their purchases, central banks have investigated already for some time now whether they might need to provide a new type of money, such as central bank digital currency (see e.g. (Auer, Cornelli and Frost, 2020[25])). To the extent that the Covid-19 pandemics reinforces the trend decline in cash usage, it further entrenches that question on the agenda of central banks. It should be noted that central banks consider issuance of such instruments for several other reasons, including to address identified inefficiencies in cross-border retail payments (BIS Committee on Payments and Market Infrastructures, 2018[26]).

Changes in the behaviour of financial consumers during the Covid-19 pandemics might have effects that are relevant for open banking initiatives that last beyond the pandemics period. In fact, people continue newly formed habits of using less cash once they get accustomed to it. Thus, recent developments might turn out to be the catalyst that brings digital payments more fully into the mainstream.

Moreover, an important aspect of the recent Covid-19 episode is that, beyond payments and other financial services, both households and firms have increasingly relied on digital as opposed to physical services. Some of these services might be considered useful and perhaps essential even after the Covid-19 episode (consider the example of digital so-called 'zoom' or 'FaceTime' meetings). To the extent that these services continue to be provided in similar quality or costs by technology firms, which might be small or large, these firms might find it easier to provide also financial services to an existing customer base.

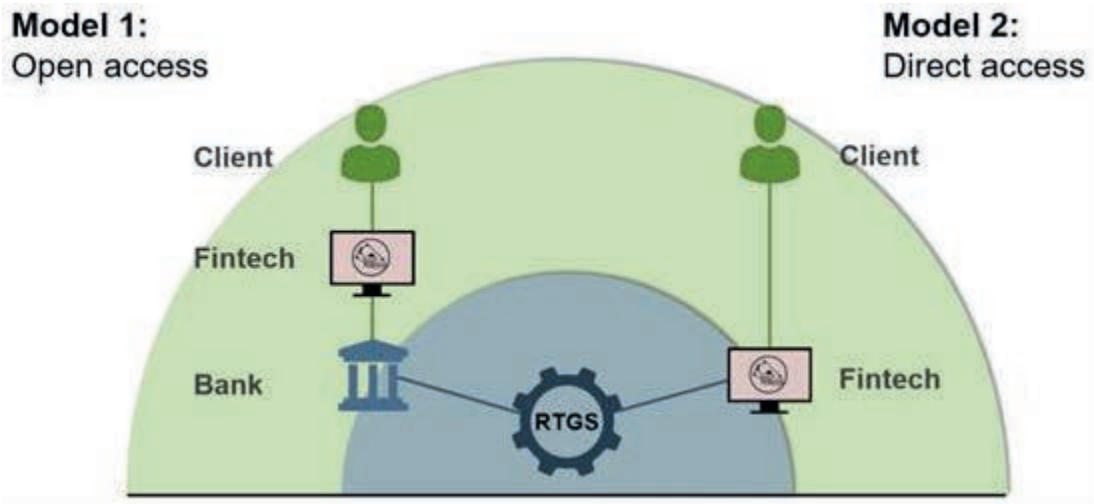
(Re-)defining the perimeter of access to the core payment infrastructure?

Open banking is a challenge for central banks, too. Central banks play an important role as the operator of the fundamental infrastructure of payments. That infrastructure allows different payment service providers to compete with each other and, to ensure a levelled playing field, they are required to meet various standards and data access requirements between them, such as open APIs. A challenge for central

banks, as the operator of the fundamental infrastructure of payments, is that they need to adapt the core payment infrastructure in such a way that the unbundling of financial services and in particular payment services generates efficiency gains, without creating new risks for monetary and financial stability (Maechler and Moser, 2019[27]). One specific open issue is to what extent new financial services providers should be given access to the core financial system infrastructure including central bank facilities.[21]

On a conceptual level, two stylised models for integrating new financial services providers into the two-tier payment system could be distinguished (Maechler and Moser, 2019[27]). The two-tier system is shown in simplified form in Figure 2.9. On the first level, via the real time gross settlement system (indicated by blue-shading), the central bank enables financial institutions to settle payments using secure systems and electronic central bank money. On the second level, (indicated by green-shading), financial institutions, typically banks, enable retail payments. The first model of integrating new participants such as Bigtech or Fintech firms (labelled as Fintech in the chart) consists of providing indirect access, via banks or other financial institutions; this model is referred to as "open access" in the chart. It essentially describes the approach taken by PSD2, which requires banks to open up access to data and payments infrastructure (Box 2.2). The second approach consists of granting new financial services providers direct access to the core payment systems; this model is referred to as "direct access" in the chart.

Figure 2.9. Two stylised approaches to integrating Fintech into payment systems



Source: (Maechler and Moser, 2019[27]).

In the United Kingdom, the Future of Finance Report by van Steenis (2019[28]) recommended that the Bank of England should (re-)consider the appropriate level of access to its balance sheet and payments infrastructure to ensure the public infrastructure supports efficiency and inclusiveness of payments (Bank of England, 2019[29]). There was a call for evidence designed to help the Bank of England to gather information to support a later consultation on whether, and if so how, the Bank might need to change its access criteria for its accounts and payments infrastructure to improve resilience, innovation and competition in payment services (Bank of England, 2019[30]).[22]

Historically, in the United Kingdom, only the largest banks had access to central bank reserves accounts. Since 2006, however, access to these accounts has expanded to include all banks and building societies, Prudential Regulation Authority-authorised broker-dealers and Central Counterparties (CCPs). As a result, access to accounts increased to 200 firms, as compared to just 17 firms before 2006. In 2017, the Bank took that process a stage further when it announced that non-bank Payment Service Providers (PSPs) would be eligible to apply for intraday settlement accounts at the Bank, which similarly had previously only

been available to a small number of systemically important firms. By 2020, six non-bank PSPs opened settlement accounts, with more in the pipeline to join.

Starting from 2019, the Swiss National Bank grants Fintech companies access to its real time gross settlement system, provided that they have a Fintech licence and are significant participants in the area of payments transactions. Thus, new financial services providers would have the same access as existing financial services providers to settlement in central bank money, which is superior to settlement in commercial bank money in terms of safety as it is irrevocable and unconditional. An important qualification is that the required Fintech license is granted by the Swiss Financial Market Supervisory Authority (FINMA) under the condition that the institution accepts public deposits not exceeding CHF 100 million, and that the deposits are not invested and not remunerated by interest payment.

One key question arising from granting access to central bank money to those new players is whether they should also qualify for central bank standing facilities that aim at supporting the smooth functioning of the payment system or whether they should even qualify to access central bank open market operations and emergency liquidity facilities. In principle, those new institutions do not engage in maturity transformation as banks do, thus they should not require access to emergency central bank credit. There might be a case for intraday liquidity or end-of-day liquidity facilities to avoid gridlocks in the system. That said, central banks have recognised (Bank for International Settlements Committee on Payment and Settlement Systems, 2003[31]) that one challenge is that the provision of central bank money accounts might be perceived as providing semi-automatic access to emergency liquidity from the central bank, that is that some provisions of the financial safety net are being made available. Central banks attempt to correct this misperception, but they may not be successful in this regard under all and every circumstances.

Concluding remarks

Contestability, competition, innovation and choice in retail financial services seem to have increased during recent years, which is consistent with the objectives of open banking initiatives. Open banking initiatives effectively facilitate the further unbundling of financial services previously provided by banks as bundles, and the offering of these services in different form by other entities. This development can result in the provision of better services. In particular, these services could become cheaper, and perhaps also better tailored to the individual customer and delivered in a more convenient way.

Open banking does not come without risks, however. The opening of an established payments infrastructure to (and the sharing of data with) new participants and the creation of new interlinkages through APIs could create new risks, including for consumers and their privacy. **To address these, it is crucial to develop processes and governance mechanisms that accompany the development of new technical and data connections, and facilitate consumers' understanding of the actual usage of their data**.

Open banking initiatives focus in most cases on digital payments. By opening up both access to payment infrastructures and to related data, switching of customer between different financial services providers is facilitated as the problem of asymmetric information, which notoriously limits switching, tends to be reduced.

To what extent open banking has been successful so far in achieving customer switching is however ultimately an empirical question, which is beyond the scope of the present chapter. It might simply be too early to venture any conclusive assessment. The starting positions differ across jurisdictions in terms of the structure of existing retail payments systems and there does not appear to be any widely agreed metrics to measure progress on open banking, not least because related initiatives have different designs, motivations and starting points. Also, the framework is evolving.

For example, the framework is evolving also as a result of new data privacy legislation, such as the European Union *General Data Protection Regulation*. Both open banking and data privacy laws have an important common element, which is that they imply that customers will have more control over their own data. Thus, one important challenge for financial services providers is to ensure customers understand how and why their data is being used, and how they can best benefit from that use, while being adequately protected.

In this regard, additional work analysing the issue of the economics of data generation and usage is needed, including on the specific issue of a potential lack of symmetry among market participants with regard to their disclosure obligation related to core data. Also, complementary analysis of the issue of the economic model of data is needed, and in particular the medium-term sustainability of a model in which banks might carry a disproportionate share of the initial data collection costs.

A widely shared view is that it might be too early to draw final conclusions on the results of open banking initiatives, as their implementation is very recent and the framework is evolving. In this regard, however, the recent Covid-19 pandemics might bring digital payments more fully into the mainstream, thus perhaps even acting as a catalyst for open banking initiatives.

Currently, consumer demand for data sharing with third parties might be limited as the open banking framework continues to evolve and awareness is not yet widely spread. **More needs to be done in terms of raising consumer awareness and monitoring the effects of open banking initiatives on consumer awareness of the greater choices offered to them, their actual use of them, and the implications for consumer switching between financial services providers**.

Unfortunately, there is no natural set of indicators to assess open banking progress, given the different motivations for, designs of, and starting positions behind such initiatives. Anecdotal evidence suggests that consumer choice has increased, which is desirable. Whether any economic rents in banking have declined is less clear.[23] More empirical work is needed to understand to what extent open banking initiatives have had already some significant effect on market structures, including on any rents that incumbent banks might have benefitted from. Admittedly, such work is complicated by currently subdued levels of bank profitability and emerging asset quality challenges.

Adapting central bank balance sheet access policies in principle might further benefit innovation and enable competition, which is desirable as long as monetary and financial stability is ensured. In fact, policy makers are considering the question to what extent access to central bank balance sheet and infrastructure may be given to a wider set of entities, including Fintech and Bigtech firms. One important consideration in this context should however be the question to what extent any changed policies has implications for perceived or actual access to the provisions of the financial safety net, which focuses on deposit-taking banks.

Open banking can facilitate the entry of non-bank financial services providers with regard to the provision of traditional banking services and is thus a welcome source of contestability of markets and competition for established financial institutions. **It cannot be ruled out however that new non-bank financial services providers are absorbing a large share at the detriment of competitors in some market segments so that the overall results in such segments is an increased concentration**. Such effects are a particular concern in industries with strong network effects, as is the case for payments. The network effects can generate a virtuous circle of greater user participation, reduced costs and more convenient services, but could ultimately also lead to increased concentration and pricing power, with consumers ending up being worse off.

Going forward, data is likely to continue to become more important as production factor. In this regard, open banking initiatives have highlighted the observation that competition, consumer protection and data privacy, as well as financial and monetary stability considerations need to be all taken into account as policy frameworks related to financial services are further adapted. This approach would allow one to reap

the efficiency and other benefits of wider proliferation of data in the economy without compromising other policy objectives.

References

Accenture (2018), *Star shifting: Rapid evolution required - Banks can grow by accelerating their move to digital*, https://www.accenture.com/_acnmedia/pdf-87/accenture-banking-rapid-evolution-required.pdf. [12]

Access to Cash Review (2019), *Final Report*, https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf. [23]

Acquisti, A., C. Taylor and L. Wagman (2016), "The Economics of Privacy", *Journal of Economic Literature*, Vol. 52/2, pp. 442-492, http://dx.doi.org/10.1257/jel.54.2.442. [7]

Arner, D., J. Barberis and R. Buckley (2017), "Fintech, regtech, and the reconceptualization of financial regulation", *Northwestern Journal of International Law & Business*, Vol. 37/3. [21]

Arner, D., J. Barberis and R. Buckley (2016), *150 years of fintech: An evolutionary analysis*, Australian Centre for Financial Studies. [35]

Arner, D., J. Barberis and R. Buckley (2016), "The evolution of fintech: A new post-crisis paradigm", *The Georgetown Journal of International Law*, Vol. 47, pp. 1271-1319. [32]

Auer, R., G. Cornelli and J. Frost (2020), "Taking stock: ongoing retail CBDC projects", *BIS Quarterly Review*, https://www.bis.org/publ/qtrpdf/r_qt2003z.htm. [25]

Bank for International Settlements Committee on Payment and Settlement Systems (2003), *The role of central bank money in payment systems*. [31]

Bank of England (2019), *Access to Bank of England payments infrastructure and balance sheet for payments firms – A call for evidence*. [30]

Bank of England (2019), *New economy, new finance, new Bank – The Bank of England's response to the van Steenis review of the Future of Finance*, https://www.bankofengland.co.uk/-/media/boe/files/report/2019/response-to-the-future-of-finance-report.pdf?la=en&hash=34D2FA7879CBF3A1296A0BE8DCFA5976E6E26CF0. [29]

Basel Committee on Banking Supervision (2019), *Report on open banking and application programming interfaces*, https://www.bis.org/press/p191119.htm. [2]

BIS (2019), *Big tech in finance: opportunities and risks*, https://www.bis.org/publ/arpdf/ar2019e3.htm. [20]

BIS Committee on Payments and Market Infrastructures (2018), *Cross Border Retail Payments*. [26]

CBInsights (2019), *2019 Fintech Trends to watch*, https://www.cbinsights.com/research/report/fintech-trends-2019/. [10]

CBInsights (2019), "Building the bank of the Future", *Research Briefing*, https://www.cbinsights.com/research/briefing/bank-future/. [37]

CBInsights (2019), *Global Fintech Report Q3 2019*. [13]

CBInsights (2019), *Killing the I-Bank: The disruption of investment banking*, https://www.cbinsights.com/research/report/disrupting-investment-banking/. [17]

CBInsights (2019), *The 7 industries Amazon could disrupt next*, https://www.cbinsights.com/research/report/amazon-disruption-industries/. [38]

Denk, O., S. Schich and B. Cournède (2015), "Why implicit bank debt guarantees matter: Some empirical evidence", *OECD Journal: Financial Market Trends*, Vol. 2014/2, http://www.oecd.org/daf/fin/financial-markets/Why-implicit-bank-debt-guarantees-matter-some-empirical-evidence.pdf. [18]

Dosis, A. and W. Sand-Zantman (2019), *The Ownership of Data*, http://dx.doi.org/10.2139/ssrn.3420680. [6]

European Banking Authority (EBA) (2019), "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2", *EBA Opinion* EBA-Op-2019-06, https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf. [39]

Evry (2018), *PSD2 – Strategic opportunities beyond compliance*, https://www.evry.com/en/campaigns/white-paper-psd2/. [4]

Frost, J. et al. (2019), "BigTech and the changing structure of financial intermediation", *BIS Working Papers* 779, https://www.bis.org/publ/work779.htm. [34]

FSB (2019), *FinTech and market structure in financial services: Market developments and potential financial stability implications*. [1]

Hong Kong Monetary Authority (2018), *Bank Ordinance - Guideline on Authorization of Virtual Banks*, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/guideline_eng_virtual_bank_20180608.pdf. [19]

Izaguirre, J., D. Dias and M. Kerse (2019), *Deposit insurance treatment of e-money – An analysis of policy choices*, Consultative Group to Assist the Poor (CGAP), https://www.cgap.org/research/publication/deposit-insurance-treatment-e-money-analysis-policy-choices. [8]

Jones, C. and C. Tonetti (2018), *Nonrivalry and the economics of data*, http://christophertonetti.com/files/papers/JonesTonetti_DataNonrivalry.pdf. [5]

Liikanen, E. (2016), *Cash and the central bank*, https://www.bis.org/review/r160616e.pdf. [24]

Lumpkin, S. and S. Schich (2020), "Banks, Digital Banking Initiatives and the Financial Safety Net: Theory and Analytical Framework", *Journal of Economic Science Research*, Vol. 3/1, https://ojs.bilpublishing.com/index.php/jesr/article/view/1113. [9]

Maechler, A. and T. Moser (2019), *The evolution of payment systems in the digital age: A central bank perspective*. [27]

Petralia, K. et al. (2019), "Banking disrupted? Financial intermediation in an era of transformational technology", *Geneva Reports on the World Economy* 22, https://cepr.org/content/geneva-report-22-banking-disrupted-financial-intermediation-era-transformational-technology. [14]

S&P Global (2019), *The future of banking: Will banks trip over tech disruption?*. [16]

Schich, S. (2019), "Do fintech and cryptocurrency initiatives make banks less special", *Business and Economic Research*, Vol. 9/4, http://www.macrothink.org/journal/index.php/ber/article/view/15720. [11]

Shin, H. (2020), *Central banks and the new world of payments*, https://www.bis.org/speeches/sp200630b.htm. [22]

U.S. Department of Treasury (2018), *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation", Report to President Donald J. Trump*. [3]

Van Leeuwen, B. (2018), *Fintech needs a voice to counter aggressive lobbying from banks*, https://medium.com/datadriveninvestor/fintech-needs-a-voice-to-counter-aggressive-lobbying-from-banks-fa8e1fe1510e. [36]

van Steenis, H. (2019), *Future of Finance - Review on the outlook for the UK financial system: What it means for the Bank of England*, https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report.pdf?la=en&hash=59CEFAEF01C71AA551E7182262E933A699E952FC. [28]

Vives, X. (2019), *Digital disruption in financial markets*. [15]

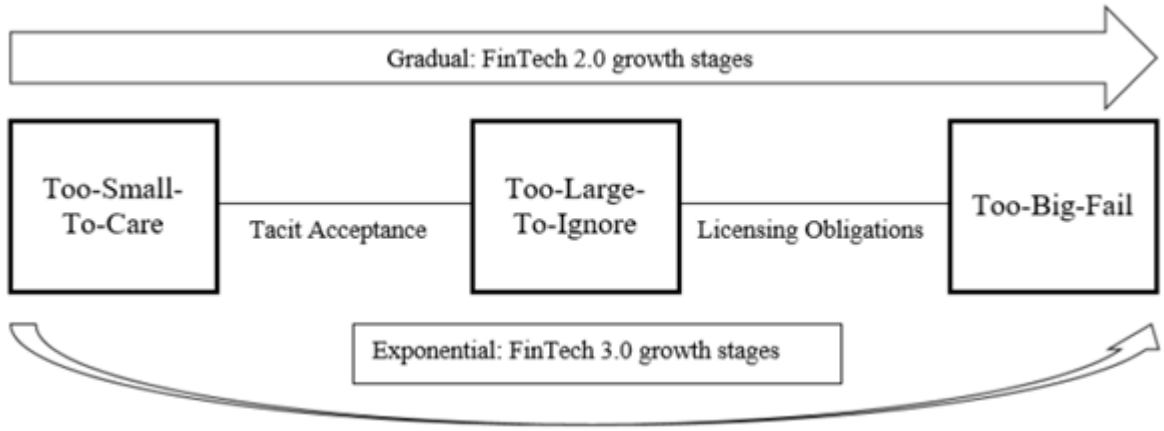
Zetsche, D. et al. (2017), "From FinTech to TechFin: The regulatory challenges of data-driven finance", *European Banking Institute Working Paper* 6. [33]

Annex 2.A. Potential financial stability risks from Bigtech

On a general level and not necessarily strictly related to open banking, the financial stability implications of Fintech, on the one hand, and Bigtech developments, on the other, in financial services might differ considerably (see also (Petralia et al., 2019[14])). As regards the former, the FSB (2019[1]) concludes that evidence for the existence of financial stability vulnerabilities related to Fintech developments are limited at the global level, although it also acknowledges that these developments require continued monitoring.

The potential for "risk blind spots" to arise in the context of Bigtech firms' activities in financial services has however been identified for some time now (Arner, Barberis and Buckley, 2016[32]). Bigtech firms might move fast from being a data broker, via the use of such databases for their own financial activities to becoming a large and diversified financial service provider themselves (Zetsche et al., 2017[33]). In this context, it is useful to remember that Bigtech firms often start with payments, especially to overcome the lack of trust between buyers and sellers on e-commerce platforms (BIS, 2019[20]), but then expand into the provision of a wider array of services, including credit (Frost et al., 2019[34]). Network effects and advanced data analysis techniques, potentially involving the merger of different datasets might facilitate fast growth in market shares. A stylised description of the idea of "risk blind spots" is shown in Annex Figure 2.A.1. It suggests that the somewhat more traditional Fintech growth ("FinTech 2.0 growth stages") can be described as linear, moving gradually from "too-small-to-care" to "too-large-to-ignore", and then potentially to "Too-Big-To-Fail", while the Bigtech ("Fintech 3.0 growth stages") might grow exponentially and thus move almost directly to "Too-Big-To-Fail". One specific issue is that to the extent that a Bigtech created or bought a bank that became systemically important, there will be a risk that the non-bank business contaminate the bank business, adding to the already present risks of adverse spill-overs within different types of banking activities. Such a situation would violate the prudential call for separation of banking from (non-financial) industry.

Annex Figure 2.A.1. Stylised description of "risk-blind-spots" in case of exponential Bigtech growth



Source: (Arner, Barberis and Buckley, 2016[35]).

Notes

[1] The author is particularly grateful for extensive and very helpful comments and specific drafting suggestions from Benjamin Müller, Irina Mnohoghitnei, Stephanie Payet, Chris Pike, and Ilaria Supino, as well as delegates of the OECD Committee on Financial Markets (CMF) and its Experts Group on Finance and Digitalisation. The author remains however solely responsible for any remaining errors.

[2] This observation is highlighted by the discussions in various fora, including an extra plenary OECD Financial Roundtable held by the CMF in October 2018 and a roundtable by the OECD Working Party No. 2 on Competition and Regulation on 4 June 2018. For example, in the exchange organised by the latter, a presentation from the United Kingdom discussed effects on competition and on customers, singling out both personal current accounts and SME lending for special attention. Another presentation from Portugal noted that "open banking" focused mostly on payment services and crowdfunding, but also discussed the potential for Insurtech and Robo-advice. Yet another presentation from the Netherlands placed a narrower focus on payment services.

[3] A list of all authorised third party providers in the European Union is available here: https://euclid.eba.europa.eu/register/pir/disclaimer?returnUrl=%2Fpir%2Fsearch.

[4] See Authorization of Virtual Banks -- A Guideline Issued by the Monetary Authority Under Section 16(10) of the Banking Ordinance, available at https://www.hkma.gov.hk/eng/key-information/guidelines-and-circulars/guidelines/20000505.shtml#1.

[5] "New regulation on open banking in Brazil", Banco Central do Brasil, 8 May 2020; https://www.bcb.gov.br/en/pressdetail/2330/nota.

[6] The Open Banking Implementation Entity (OBIE) is the company set up and governed by the Competition and Markets Authority in 2016 to deliver Open Banking; it is funded by the UK's nine largest banks and building societies.

[7] See https://www.csiro.au/en/News/News-releases/2018/Data61-appointed-to-Data-Standards-Body-role.

[8] The asymmetric information problem is a key impediment to customer switching bank accounts, as customers tend not to switch to a new bank unless they will be given better terms, and even then, customers tend to be reluctant to switch.

[9] Open banking initiatives imply that banks lose any monopoly power they might have had with regard to access to retail payments data. As a result, open banking initiatives tend to foster an ongoing process of decentralisation of decision-making, risk-taking, and record-keeping in the provision of financial services. The implications of this process especially for financial stability and policy requirements is discussed in FSB (2019[1]), to which the OECD has contributed.

[10] Privacy issues are also a concern in the context of the (growing) use of cloud services, that is of computing and data storage services on remote servers via the internet. Cloud services can offer economies of scale, operational efficiencies and better cost-effectiveness, but there are challenges in terms of data protection and security issues and risks from concentration on limited number of suppliers (e.g. large suppliers of cloud services can become a single point of failure when many institutions rely on them). The location of the suppliers of cloud services can matter and create additional challenges. For example, concerns have been expressed about one form of extraterritoriality whereby United States authorities can have access to private data stored or processed through US-based companies, while foreign banks might risk breaking their domestic country privacy laws if they used these US companies for data storage or processing functions.

[11] See OECD Working Party on Competition and Regulation roundtable on digital disruption in financial markets on 5 June 2019, at http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm.

[12] See e.g. "The top 10 FinServ data breaches", by Ellen Zhang, 8 May 2019, at https://digitalguardian.com/blog/top-10-finserv-data-breaches.

[13] For example, measured by transaction value, in Europe, the largest Fintech segments is by far digital payments, as compared to personal finance, alternative lending, and alternative financing, and this segment is expected to further grow fast by some analysts (see e.g. https://www.statista.com/outlook/295/102/fintech/europe?currency=eur).

[14] Representatives from incumbent banks often claim that an unfair advantage for Bigtech firms in their competition with established banks exists, as banks have to allow to share their customer data, while a similar requirement does not apply to Bigtech firms (lack of "reciprocity"). A Fintech company representative suggests that incumbent banks are however not prevented from building up their own technology expertise and digital platforms, so as to compete with Bigtechs on a whole range of digital services (Van Leeuwen, 2018[36]).

[15] For example, "*A.T. Kearney is predicting the demise of one in ten European banks over the next five years as more agile digital challengers embrace the changes wrought by Open Banking to increase their market reach*…" at https://www.openbankingexpo.com/news/one-in-ten-european-banks-to-fall-away/.

[16] Obviously, incumbent banks might also want to limit entry by Bigtech firms. For example, the Australian Competition and Consumer Commission issued in 2017 a determination denying authorisation to a group of Australian banks to collectively bargain with Apple and collectively boycott Apple Pay in Australia https://www.accc.gov.au/media-release/accc-denies-authorisation-for-banks-to-collectively-bargain-with-apple-and-boycott-apple-pay.

[17] The policy response to the Covid-19 pandemics consists of two distinct elements. First, driven by public health concerns, containment measures have aimed at flattening the amount (curve) of new infections sufficiently to allow the health system capacity to be sufficient to deal with all infected cases that need special treatment. These measures have tended to have adverse effects on economic supply and demand, however. Thus, second, to support confidence and cushion the effects on real activity of the pandemics and especially containment measures, a large range of support measures for financial and non-financial firms have been taken.

[18] See e.g. https://www.bloomberg.com/news/articles/2020-03-06/fed-puts-quarantine-on-repatriated-physical-cash-from-asia.

[19] Empirical studies have identified that the human influenza virus can remain infectious on banknotes for more than two weeks. That said, influenza viruses are different from coronaviruses. Also, the risk of infections passing through the touching of physical banknotes is not necessarily greater than that of touching other surfaces including physical credit cards.

[20] For example, in the United Kingdom, consumers' ATM and cash use fell significantly, by around 50%, over just a few days in March 2020, while digital payments were facilitated through increases in the limit for contactless payments.

[21] Yet another question is whether central banks, as the operator of the fundamental infrastructure of payments, should give retail customers access to claims on the central bank in electronic form. One route is to issue a central bank digital currency (CBDC) available to retail customers. Judged by speeches and reports coming from central banks, the balance of opinion towards either retail or wholesale CBDC seems to be leaning more favourably (Shin, 2020[22]). CBDC are another way in which central banks can play the role of the operator of the payment infrastructure and some versions of it could imply important changes to the structure of the current monetary and banking system. The role of banks and effects of open banking initiatives might change substantially.

[22] This call is distinct from the Bank of England's programme to deliver the next generation of its Real Time Gross Settlement (RTGS) service. The Bank of England also continues to explore the topic of a CBDC.

[23] Such rents can be considerable, attracting more funds into the banking sector than might be merited by considerations of financing real economic activity alone and resulting in wage premiums paid in the financial as compared to other sectors (see e.g. (Denk, Schich and Cournède, 2015[18])).

3 The impact of big data and artificial intelligence (AI) in the insurance sector

This chapter examines both the benefits and risks big data and artificial intelligence (AI) can bring to the insurance industry. In particular, it describes how the OECD Recommendation on Artificial Intelligence and the European Commission's Independent High-Level Expert Group on Artificial Intelligence's (AI HLEG) Ethics Guidelines for Trustworthy AI should be considered in the context of the insurance sector. The chapter then presents areas related to big data and AI in the insurance sector where policy makers may consider taking action going forward.

Introduction

The advance of technology and innovation in processes has enabled the global economy to benefit in terms of improved productivity and other economic benefits. In 2016, the information industries contributed to around 6% of total value added and 3.7% of employment across OECD countries (OECD, 2019[1]). In addition, the level of labour productivity in information industries of OECD countries is about 65% higher than that of other industries in the business sector (OECD, 2019[1]).

In addition, digitalisation has the potential to transform the way we work, enabling more diverse groups of people to gain employment, as well as engaging technology where automation can be introduced in processes (Manyika, 2017[2]). It is estimated that 60% of all occupations have at least 30% of activities that are technically automatable (Manyika, 2017[2]).

These predictions are in line with developments in the insurance sector, although funding deals in insurance start-ups (venture capital funding, VCs) (8% of all fintech funding) is far surpassed by investment in lending (19%), wealth and asset management (30%) and payment VCs (23%) (Accenture, 2019[3]). Nevertheless, the number of activities related to InsurTech is high and has the potential of improving insurance business processes and business models (OECD, 2017[4]).

The OECD's Insurance and Private Pensions Committee (IPPC) has been actively engaged in discussing the impact of technological development and innovation in the insurance sector. The OECD has also been a leader in policy discussions related to cyber risk insurance (OECD, 2017[5]), and a report on InsurTech was published in 2017 (OECD, 2017[4]).

While there are a number of technologies that are being developed and employed to improve the experience and business of insurance in general, the potential that artificial intelligence (AI) and big data may play in insurance production is strong. There is much interest expressed from both the industry and regulators in how technology can benefit the insurance sector, especially given the potential of improving the customer experience.

Insurance is based on the idea of pooling risks, and underwriting is most often based on past loss experiences and/or risk modelling. The prospect of having more data leads to the possibility of greater data analytics and, in particular, improving predictive analytics, enabling pricing that is better suited to expected risk, and is more granular or adjusted to policyholder behaviour.

However, this is too simplistic a way of understanding how data contributes to insurance, as there are a variety of questions and implications that arise when considering potential scenarios that could occur with the arrival of big data. One of the first and principal questions is what big data means in the insurance context. There is also the question of whether pricing would, in fact, be more accurate in terms of risk and whether this would lead to an overall better production of insurance products.

Further, big data has implications for AI. AI is developed by using machine learning, which inputs data for the algorithm to learn responses. Big data is a valuable source of data for machine learning, but the extent of their potential contribution is uncertain, given that big data often involves unstructured free text.

The benefit of AI has been demonstrated in its application of many business processes, in particular in forms such as chatbots, optical character recognition, sentiment analysis (EIOPA, 2019[6]) and social media algorithms, and these could easily be applied for insurance purposes.

The potential for greater AI application in the insurance sector is high; however, while this could have a positive impact in terms of profitability and hence solvency, there remain aspects of AI that raise questions in areas such as data collection and pre-processing, privacy and ethical issues, and how insurance regulators should approach this.

There are also regulatory issues as well as wider considerations such as data protection and privacy. In this context, the UK's Financial Conduct Authority (FCA) published a Feedback Statement in 2016, which

lists many of the issues involved in big data for general insurance. The US's National Association of Insurance Commissioners (NAIC) has established a working group on big data, and the NAIC and the European Insurance and Occupational Pensions Authority (EIOPA) have jointly been discussing issues of big data (EIOPA and NAIC, 2018[7]) and published a paper on the European insurance market. It is also important to recognise the potential social and ethical questions on using big data, and to that extent EIOPA established a Consultative Expert Group on Digital Ethics in Insurance in late 2019.[1].

This chapter has been developed to bring better understanding to what big data and AI are, as well as what impacts they might have on the insurance sector. It will conclude with potential policy actions countries may consider to ensure that they are prepared and proactive in light of these developments. As the OECD's IPPC undertakes surveillance of market developments, including on technological developments, it will continue to monitor related developments so timely policy recommendations can be made for policymakers.

Big data

What constitutes big data

Big data is increasingly ubiquitous, with big data often being cited as a source for better understanding politics, economy, society, etc. However, it is not always clear what is meant by big data, so understanding what big data is, especially given that insurance could potentially use big data as a source of its data analytics, is important.

One of the common definitions of big data is to view it in the 3Vs (Laney, 2001[8]) or the three challenges in data management: volume, variety and velocity (Chen, Chiang and Storey, 2012[9]), which are all "high" in the case of big data.

High volume is the size of the data, which for big data could be reported in multiple terabytes (which is 1 000 gigabytes and would fit as much as 1 500 CDs or 220 DVDs) or petabytes (1 million gigabytes).

High variety is when there is structural heterogeneity in the dataset. Structured data, which constitutes only 10%-15% of all existing data, refers to the tabular data found in spreadsheets or relational databases. Text, images, audio, and video are examples of unstructured data, which sometimes lack the structural organisation required by machines to be used for analysis and makes up about 80% or more of all enterprise data. Spanning a continuum between fully structured and unstructured data, the format of semi-structured data does not conform to strict standards. Extensible Markup Language (XML), a textual language for exchanging data on the Web, is a typical example of semi-structured data. XML documents contain user-defined data tags, which make them machine-readable. Semi-structured data constitutes around 5%-10% of data (Gandomi and Haider, 2015[10]; Taylor, 2018[11]).

Velocity refers to the rate at which data is generated and the speed at which it should be analysed and acted upon. The proliferation of digital devices such as smartphones and sensors has led to an unprecedented rate of data being produced (Gandomi and Haider, 2015[10]). This in turns requires greater speed at which data needs to be filtered.

The FCA carried out a feedback statement in 2016 outlining what big data means. Big data is referred to as (FCA, 2016[12]):

- using new or expanded datasets and data, including from unconventional sources such as social media;
- adopting the technologies required to generate, collect and store these new forms of data;
- using advanced data processing techniques;
- sophisticated analytical techniques such as predictive analytics; and

- applying this data knowledge in business decisions and activities.

Thus, it is not limited to the type of data, but also includes the data processing and analytic aspect of big data. On the other hand, the FCA report identifies the main sources of big data that insurers may be using as (FCA, 2016[12]):

- Proprietary data (e.g. data from connected companies such as personal data of products purchased or loyalty cards);
- Data acquired from third parties (e.g. aggregated search engine data such as credit checks, license details, claims discount databases, price comparison website quote);
- Social media data (e.g. consumer-specific data taken from Facebook or Twitter); and
- Connected devices data (e.g. telematics devices such as could be used in motor, home or health telematics).

Proprietary data and data acquired, as well as connected device data, would likely be structured data, including data from the Internet of Things (IoT). Social media data would likely be unstructured, which could make it costly to make it useable for big data analytics purposes. Both structured and unstructured data could include audio and visual data, which could assist in instances of disasters.

AI is closely related to big data, but distinct. Big data refers primarily to the information data that is collected, while AI is the process of machine learning that uses data or big data to achieve the learning process of the algorithms. AI is a specific process, which may or may not use big data, while big data is the data that could be inputted for a variety of processes in the insurance value chain.

How and where insurance may be affected by big data

Big data is anticipated to affect insurance in a number of ways. The most widely anticipated is data analytics, although what this specifically means is not always clear from the coverage of this topic. The second is underwriting and pricing, with different views on how big data could affect them. Distributions and sales are more obvious avenues given the way big data might enable better targeting and understanding of consumer behaviour. Claims handling and complaints could be streamlined using big data, and marketing could be more targeted with big data.

Data analytics is the science of drawing insights from raw information sources. Data analytics is a broad term that encompasses many diverse types of data analysis. Essentially any type of information can be subjected to data analytic techniques to get insight that can be used to improve understanding and processes. Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms.

There are four types of data analytics (Investopia, 2018[13]):

- Descriptive analytics: what happened over a given period of time (analysis of past data);
- Diagnostic analytics: why something happened, which involves more diverse data inputs and some hypothesising;
- Predictive analytics: what is likely going to happen in the near future;
- Prescriptive analytics: suggesting a course of action going forward.

Based on data analytic tools, insurers can take advantage of big data to apply diagnostic and predictive analytics to predict the behaviour of potential policyholders and take action based on the outcomes.

It should be mentioned that without expert input, big data analytics could be subject to spurious correlation and caution needs to be taken in interpreting data. Spurious correlations occur when two random variables track each other closely on a graph, leading one to suspect correlations. This may lead to assumptions that one of the variables is linked to the movement of the other variable.[2] However, this does not always

confirm causation between the variables, and only through expert analysis can causation be well established.

In the insurance industry, firms have primarily relied on traditional generalised linear models (GLMs) to assess and price risks.[3] This is a statistical technique used to estimate the relationships between the probability of making a claim and different risk factors.

However, some firms have started to use other analytical techniques as well to create inputs to GLM. For example, decision tree analytics or non-linear techniques, such as machine learning techniques, are being used (FCA, 2016[12]).

The International Association of Insurance Supervisors (IAIS) is looking across the insurance product lifecycle, and thinking on a number of cases when big data is being deployed (IAIS, 2020[14]).

Big data is being employed in **product development**, for example, through the use of telematics (see Box 3.1). While the most widely known and actually applied use case is auto telematics, there are a number of potential ways in which telematics may become more integrated into insurance products going forward.

Box 3.1. Telematics insurance

While the most widely known form of telematics insurance is for automobile insurance, there are a variety of telematics insurance which are being deployed or have a strong potential of being applied.

Motor insurance related data have been abundantly accumulated in insurance companies, as it is one of the largest lines in most countries. Telematics motor insurance is when a device (blackbox) is fitted into motor vehicles or by using an app on a smartphone, and used to track driving. For example, the Italian Insurance Association estimates that blackboxes have been installed in over 2 million cars in Italy to support the provision of blackbox insurance, "telematics car insurance" or Usage Based Insurance (UBI), and is one of the largest markets for telematics car insurance. Blackbox devices track speed, braking, acceleration, cornering and the time of the day a journey is made via satellite technology. The data is transmitted to the insurer by GPS, which enables the insurer to estimate the likelihood of a claim being made. Such programmes benefit young drivers that do not have a track record to influence their premiums, for example.

There are a number of *home devices*, such as Hive, which is a home security product, or Nest, which is a thermostat which have the potential to link to insurance. These products are controlled through an application on your smartphone to manage how your security or energy use is regulated in your home. While premium discounts are offered to more traditional security measures for property insurance, such as deadbolts, burglar alarm, or fire alarm, there are few examples of home telematics being applied for insurance. Allianz and Deutsche Telekom have formed a partnership in which digitally connected homes automatically alert Allianz's emergency hotline if there is a problem, such as a burst pipe (Allianz SE, 2014[15]). However, the objective does not appear to automatically lead to premium discounts, for example.

Personal devices such as Fitbit and Apple watch permit device operators to collect individual activity data as well as health related data. These devices collect a wide range of lifestyle data, such as heart rates, exercise information, and GPS, which are data that could lead to better predictive and diagnostic analytics. Fitbit recently released a new tracker, Inspire, which is available only to corporate employees and health insurance members. In addition, Fitbit is a named covered fitness benefit in 42 Medicare Advantage plans across 27 US states, while it is working with insurance firms like United Health (Russell, 2019[16]). The logical step for those affiliated insurers would be to better link the data with insurance.

Vitality offers life and health insurance in the United Kingdom, and offers premium discounts based on the activity points that can be earned via use of Apple watches and demonstrated activity levels. Vitality activity points can also contribute to individual savings accounts (ISAs), which allows individuals to hold cash, shares, and unit trusts free of tax on dividends (Vitality, 2019[17]).

In addition, some companies are starting to offer premium discounts on pet insurance for pets that use a Fitbit like device, PitPat. Regularly exercising dogs can receive a cash reward of up to GBP 100 a year (Howlett, 2019[18]).

Marketing, both direct and indirect, is the other area in which big data could be effectively used to target consumers. Search engine optimisation is increasingly being employed, by improving the visibility of a website or a webpage in a search result, and which itself is a result of processing and analysing large datasets.

Aggregated search engine data is being used to analyse potential groups of consumers who may have a specific insurance need. By understanding what a consumer is searching for, more tailored marketing can be carried out. For marketing in particular, social media data is a potential source of data.

In terms of **distribution and sales**, the increasing popularity of price comparison sites have changed how consumers search for insurance products. Firms can use a variety of data sources to verify consumer information during the sales process. Most insurers predict that big data should make it easier for consumers to obtain quotes.

Connected devices and social media are likely to assist with **claims verification** process, which is being improved through digitalisation. Social media can also be used to detect **fraudulent claimants**. For example, social connections can be analysed to identify suspected fraud rings.

Pricing and risk classification

In insurance, it is sometimes useful to distinguish between "costing" (the calculation of the technical premium) and "pricing" (the actual commercial decision to offer a policy at a certain premium level). Insurance rates must be based on predictions rather than actual costs. Most rates (costs) are determined by statistical analysis of past losses based on specific variables of the insured. Variables that yield the best forecasts are the criteria by which premiums are set. However, in some cases, historical analysis does not provide sufficient statistical justification for setting a rate, such as for earthquake insurance. In these cases, catastrophe modelling is sometimes used (thisMatter, n.d.[19]).

The advent of big data has given rise to the possibility that risk-based pricing is increasingly applied given that more data could improve the predictability of policyholder behaviour or incidents. However, given the competitive landscape of insurance, insurers may not wish to distinguish between similar risk level policyholders but based on risk sensitivity or propensity to switch (FCA, 2016[12]).

Insurance sets prices by groups of people who have similar risk profiles, whether, for example, by gender[4] or age for auto insurance, which is call risk classification. Big data provides new sources of information for understanding policyholders, fine-tuning the risk classification.

There are benefits and draw backs that may arise from risk classification being further broken down. The benefits to greater risk classification is pricing based on risk, allowing insurers to combat adverse selection by marketing to low risks. Potential policyholders that are low risk may not want to pay for a price that reflects the wider population of the risk pool. Pricing based on risk may be far fairer to low risk policyholders as low risk policyholders would usually subsidise a high risk policyholder in a risk pool. Pricing based on risk provides a signal to the policyholder about their riskiness. On the other hand, a signal of a higher price may encourage a change of behaviour (Swedloff, 2014[20]).

Nevertheless, there are risks to greater risk classification. It may be socially beneficial that insurers succeed in bringing new, low risk entities or individuals into the overall risk pool. However, if this leads to the exclusion or difficulty of obtaining a quote for a high risk policyholder, this could result in sub-optimal market outcomes.

While insurance can be viewed as spreading risks through a population, risk classification could undermine this risk spreading, since some policyholders may be burdened or locked out of insurance as a result. It is particularly troubling when a risk classification is based on a suspect category. There may be constitutional, legal or regulatory concerns of discriminating groups based on ethnicity, race, gender, etc. too[5] (Swedloff, 2014[20]).

If the policyholder has no control over the characteristic to which risk classification is based on, such as genetics, it could be viewed as unfair. Even if the characteristic does accurately reflect a risk, it may not be socially acceptable for this classification to take place (Swedloff, 2014[20]), although it could become a relevant consideration for policyholders in taking preventative care, for example.

Returning to the spurious correlation mentioned above, while risk classification is based on correlation and not causation, there must be a strong causal backbone for the correlation to be considered. Moreover, risk classification is imperfect and expensive, creating incentives to take advantage of correlations found as much as possible.

Finally, risk classification may require insurers inquiring about otherwise irrelevant information, such as credit score, genetic information and sexual orientation, raising privacy concerns. If policyholders' refusal to respond to such queries were to affect pricing or offering of a policy, this could raise concerns over the merit of risk classification (Swedloff, 2014[20]).

Regulatory considerations of the use of big data in insurance

While there are significant benefits from using big data in the production and business of insurance, there may be certain social costs in doing so. While not directly from big data, the example of New Zealand's earthquake insurance is a case in which more granular data has led to the exclusion of some cities from being insured as discussed in Box 3.2.

Box 3.2. Risk-based pricing in New Zealand's property insurance

New Zealand experienced a 7.1 magnitude earthquake (EQ) in Canterbury in September 2010, and then the Christchurch earthquake in February 2011, which had a magnitude of 6.2. Christchurch's central city and infrastructure was badly affected with liquefaction affecting some areas as a result of the 2010 EQ, making the damage wide spread and deadly.

New Zealand's Earthquake Commission (EQC) provides government-backed natural disaster insurance for residential properties, covering perils that are a result of EQs. It is an automatic extension to property insurance, and cover building, content and land. It is estimated to have paid around NZD 11 billion (USD 7.3 billion) by the time it settled its claims (RMS, 2018[21]).

The losses have exposed significant shortfalls in the country's insurance market, in terms of deficiencies in data and gaps in portfolio management. Since then, policy terms have been tightened, restrictions have been introduced on coverage, and efforts made to improve databases. A cap will be introduced on government-backed residential cover from NZD 100 000 to NZD 150 000. While an increase, it is well below the average house price in New Zealand, which was NZD 669 565 with a rebuild cost of NZD 350 000 in December 2017 (RMS, 2018[21]).

However, in March 2018, Tower Insurance announced a move to risk-based pricing for home insurance, which has resulted in 300% price hikes for some Wellington properties (Stepanova, 2018[22]). This was possible as a result of the increasing quality and granularity of underwriting and claims data, and in particular the advance in liquefaction module, leading to the development of a high-definition EQ model. The model is built upon a variable resolution grid, which is set at a far more localised level (RMS, 2018[21]).

Following this, a number of other insurers, including IAG, the largest property insurer, followed on with their transition to risk-based pricing, with IAG's chief risk officer predicting that there will soon be an end to low risk parts of the country subsidising the higher risk places (Tibshraeny, 2018[23]).

This has resulted in IAG refusing to take on any new property contents business in the Wellington area although IAG did not to take on risk-based pricing in the end (NZ, 2019[24]).

The EQC removed contents coverage at the end of 2018, given submissions from the private insurance market that this could be privately provided.

Besides the FCA's work on big data, the NAIC has established a Big Data (EX) Working Group which discusses how to improve the understanding of predictive models (NAIC, Big Data Working Group, 2018[25]).

In addition, the EU-U.S. Insurance Project hosted a dialogue on big data in October 2018 (EIOPA and NAIC, 2018[7]). The working group on big data is currently focussed on better understanding the types of big data, how this is being used for underwriting, and how supervisors are addressing their data needs to appropriately monitor insurance markets.

The main concerns that have been raised by these groups appears to be **privacy and data protection** concerns. This stems primarily from the fact that much of big data is often linked with personal information. The NAIC's model law of 2000, the Privacy of Consumer Financial and Health Information Model Regulation, requires insurers to (1) notify consumers about their privacy policies; (2) give consumers the opportunity to prohibit the sharing of their protected financial information with non-affiliated third parties; and (3) obtain affirmative consent from consumers before sharing the protected health information with any other parties, affiliates and non-affiliates.

In the EU context, the European Supervisory Authorities (EIOPA, EBA and ESMA) conducted a joint cross-sectoral review on the use of big data and published a report with key findings in February 2018 (European Supervisory Authorities, 2018[26]). The EIOPA also set up a multi-disciplinary InsurTech Task Force and a thematic review was published in April 2019 (EIOPA, 2019[6]) on the use of big data specifically by insurance undertakings and intermediaries. One of the objectives of the thematic review was to gather empirical evidence on the impact of big data across the insurance value chain (EIOPA, 2018[27]). As a follow up to the thematic review, the InsurTech Task Force is currently developing a common understanding on machine learning algorithms and their implications from a supervisory standpoint to promote supervisory convergence in this area. Furthermore, through the Consultative Expert Group on Digital Ethics in Insurance, EIOPA is developing a set of principles on digital responsibilities. The principles will address the use of new business models, technologies and data sources in insurance from the perspective of fairness and considering ethical considerations.

In the EU, the General Data Protection Regulation (GDPR) requires increased transparency from EU firms (i.e. not only insurance undertakings) and creates new rights for consumers, additional records, application of enhanced security measures, compliance checks and impact assessments (Box 3.3). The GDPR recognises the overarching principle of fair treatment of consumers when it comes to processing personal data, and enables consumers to demand the removal of their data from insurers' databases (commonly known as "right to be forgotten").

Box 3.3. EU General Data Protection Regulation (GDPR)

The EU Parliament and the European Council agreed on the General Data Protection Regulation (GDPR) in December 2015. It is applicable to firms that process personal data from those residing in the EU, irrespective of whether their services are free or fee-based, whether the firm is based in the EU or not. It is an update to the Data Protection Directive, which came into force in 1995.

Under the GDPR, fines can be up to EUR 20 million or 4% of global annual turnover, whichever is the higher, if the action of the firm leads to a loss of information or a data breach. It took effect in member states from May 2018.

GDPR requires private information to be erased without undue delay when the data is no longer required in relation to the purpose for which it was collected. The data user must also restrict use of data when the data quality has been contested by the data subject. The firm must maintain an accurate record of the data subject's agreement for their data to be used for primary and any secondary purposes, without which the firm may not have the right or ability to use the data.

Depending on how and where insurers process their data, this could have implications on how new technologies could be introduced.

In Germany, the supervisor (BaFin) published its circular concerning supervisory requirements for IT in the insurance sector (*Versicherungaufsichtliche Anforderungen an die IT* – VAIT). VAIT primarily targets senior management, and clarifies what BaFin expects from insurance undertakings with regard to the management and control of IT operations, including the required access rights management. In addition, VAIT lays down requirements for IT project management and application development, which also encompasses end-user computing in business units.

The other main concern refers to **competition**. On the consumer side, while big data creates the potential for greater information being available and more customised insurance products, a source of big data could unfairly advantage any one insurer that has been able to take advantage of big data (FCA, 2016[12]). Given that some of the biggest firms are technology firms like Google, Amazon, Facebook and Apple, there is a tendency for digital technology to result in oligopolistic outcomes due to the network externalities (Keller

et al., 2018[28]; European Union et al., 2019[29]), and the insurance entity with the best access to the appropriate data could benefit the most.

Artificial intelligence (AI)

Improvement in artificial intelligence (AI) is impacting many facets of life, even if the way in which AI is applied often times is not obvious. While the advent of AI has many positive aspects, media coverage of incidents like Facebook data harvesting and questions on the extent to which robots may take over jobs have led to some scaremongering of AI. In this context, it is important to contemplate and understand how AI is changing insurance business operations, and what regulatory and ethical questions need to be discussed given the developments in AI technology.

What is AI and how is it being applied

The field of AI research was developed in the 1950s (Anyoha, 2017[30]), although there have been a number of cycles and it has experienced what is generally called "AI winter" with disappointments in the technology to deliver on its promise and funding cuts to its research after this period. The technology has been experiencing a renaissance in the last 20 years, as a result of growth in computing power and memory capacity, developments in cloud computing and distributed and parallel processing, availability of large databases, and improvements in theoretical understanding (Kessler, 2018[31]). The potential impact of AI is estimated to drive global GDP up to USD 15.7 trillion by 2030 (PwC, 2018[32]), and 85% of customer interactions could be managed without a human by 2020 (Deloitte Digital, 2017[33]).

AI encompasses all intelligent agents (computer systems) that have the capacity to learn, adapt and operate in dynamic and uncertain environments (Miailhe, 2018[34]). To achieve this, smart systems use advanced algorithms that learn with every additional data record and continually adjust and enhance their predictions (Hehner et al., 2017[35]). Machines mimic cognitive functions associated with human minds, such as learning, perceiving, problem solving and reasoning to achieve this (Balasubramanian, Libarikian and Mcelhaney, 2018[36]).

Machine learning is one of the main ways in which AI is being applied, with algorithms that can learn from examples and can improve their performance with more data over time (PwC, 2018[32]). Deep machine learning is a branch of machine learning which relies on complex statistical models and algorithms with multiple layers of parallel processing that loosely model the way the biological brain works. Neural networks "learn" to perform tasks by considering examples, generally without being programmed with any task-specific rules. Deep machine learning requires powerful computers and huge amounts of data to enable the self-learning to take place and hence why it has been able to develop more in the last 20 years. Defence and security have been an important part of these developments, which has accelerated with the need for general cyber and terrorism defences to be deployed (Miailhe, 2018[34]).

The difference between machine learning and deep machine learning can become significant when considering what goes into AI for any given output. Machine learning involves decision trees and Bayesian networks (a type of probabilistic graphical models) thus making the process of decision making more transparent and any biases easier to detect. On the other hand, deep machine learning is based on neural networks or genetic algorithms (a search heuristic inspired by the theory of natural evolution reflecting the process of natural selection) produced by directed evolution (a method used in protein engineering that mimics the process of natural selection to evolve proteins or nucleic acids towards a user-defined goal). This makes it nearly impossible to understand why or how the algorithm is reaching certain decisions (Bostrom and Yudkowsky, 2018[37]).

When AI or machine learning is being applied for business purposes, such as online retail and recommender systems, the outcome would be to show products, social media posts and search results,

which would require accuracy of data, but may not necessarily lead to considerations of an ethical nature or on its criticality. When an AI decision has a large stake, such as a financial decision, a diagnostic medical decision, or a critical safety decision of an autonomous vehicle, the decision making process of the algorithm becomes important and the fact that it is a black box causes concerns on the potential assumptions that are made by the algorithm (PwC, 2018[32]). Even with recommender systems, there is potential for algorithms to push inappropriate images and products, and push dangerous social circumstances[6] (Fisher and Taub, 2019[38]). There is also the risk of so called "filter bubbles", where previous search results will already filter the outcome of a search.

The best known example of machine learning is google search, which can be posed questions instead of simple search terms, as well as Amazon and Facebook sites, which make recommendations and ads based on browsing history and past purchases in the case of Amazon. Siri and Window's Cortana are examples of deep machine learning applications, which will learn to understand the nuances and semantics of language to closely resemble real-life conversations. Another example is AI being used to root out exam cheats and reduce costs by including plagiarism detectors, and randomly changing numerical variables for mathematic questions (Jack, 2018[39]).

Box 3.4. Work on AI in the OECD

The OECD has been developing three main avenues of work related to AI:

1. Analytical work in a report called 'AI in society'. The report describes economic and social applications and impacts of AI technologies and their policy implications with an overview of i) the technical landscape; ii) the economic landscape; iii) applications (including financial services); iv) public policy considerations; and; v) the policy landscape.
2. Scoping principles to foster trust in and adoption of AI with an AI Group of experts at the OECD (AIGO). AIGO brings together experts nominated by national delegations, businesses, civil society, trade unions and technical community advisory committees, and experts invited by the Secretariat.
3. The OECD AI Policy Observatory provides data and multi-disciplinary analysis on AI, working with committees across the OECD and a wide spectrum of external actors.

Work by the OECD in relation to AI can be found here.

International guidelines on AI and ethical considerations

A number of international organisations and fora have been discussing and producing guidelines related to the ethical application of AI, and it is important to understand their framework to be able to consider how it could be approached in the context of insurance.

The OECD Council adopted the Recommendation on Artificial Intelligence in May 2019. It was the first inter-governmental standard on AI, and will be followed up by the development of practical guidance for its implementation. The OECD Recommendation was also the basis for the G20 adopted human-centred AI Principles.[7] The OECD AI Principles aims to promote AI that is innovative and trustworthy and that respects human rights and democratic values (see Box 3.5). The OECD Recommendation contextualises the world that surrounds AI, and tries to ensure that AI is developed in a conscious and inclusive manner.

Box 3.5. OECD Recommendation on AI

The OECD Recommendation identifies five complementary values-based principles for the responsible stewardship of trustworthy AI:

- AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
- AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Consistent with these value-based principles, the OECD provides five recommendations to governments:

- Facilitate public and private investment in research & development to spur innovation in trustworthy AI.
- Foster accessible AI ecosystems with digital infrastructure and technologies and mechanisms to share data and knowledge.
- Ensure a policy environment that will open the way to deployment of trustworthy AI systems.
- Empower people with the skills for AI and support workers for a fair transition.
- Co-operate across borders and sectors to progress on responsible stewardship of trustworthy AI.

The other guideline comes from the European Commission's Independent High-Level Expert Group on Artificial Intelligence (AI HLEG). The AI HLEG adopted Ethics Guidelines for Trustworthy AI in April 2019 (High-Level Expert Group on Artificial Intelligence, 2019[40]). The assessment list included in the Guidelines is undergoing a pilot phase. The AI HLEG's Guidelines are more focussed on ethics related issues, and due to this is more specific on the nature of AI and how it should be developed (Box 3.6). It is in fact derived from four ethical principles, which are rooted in fundamental rights: respect for human autonomy, prevention of harm, fairness and explicability (High-Level Expert Group on Artificial Intelligence, 2019[40]).

Box 3.6. Ethics Guidelines for Trustworthy AI: High-Level Expert Group on Artificial Intelligence (AI HLEG)

The Guidelines put forward a set of 7 key requirements that AI systems should meet in order to be deemed trustworthy:

- Human agency and oversight: AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.
- Technical Robustness and safety: AI systems need to be resilient and secure. They need to be safe, ensuring a fall back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented.
- Privacy and data governance: besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data.
- Transparency: the data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and must be informed of the system's capabilities and limitations.
- Diversity, non-discrimination and fairness: Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.
- Societal and environmental well-being: AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.
- Accountability: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes, plays a key role therein, especially in critical applications. Moreover, adequate and accessible redress should be ensured.

There are some common themes between the guidelines, which is worth highlighting. Both guidelines are human-centric, emphasising the need for AI to be beneficial to people. In addition, the need for security and transparency of AI are echoed in both guidelines.

An important element that is included in both guidelines is that human intervention or agency and oversight should be made possible to ensure that AI contributes to a fair and just society (OECD) and empowers people (AI HLEG). This is a critical component of ensuring that AI is applied in a way that can remedy unfair bias or can be made accountable in certain circumstances.

As the AI HLEG proposes a more comprehensive set of principles, there are additional elements that go beyond that of the OECD Recommendation. In particular, they raise the need for traceability, as well as to have adequate data governance, which includes privacy and data protection. The AI HLEG also raises the potential of marginalisation of vulnerable groups, with the need to foster diversity, so that AI is accessible to all.

When considering these in the context of insurance, it is clear that all themes should be adapted in a manner that encourages inclusive growth, while maintaining safeguards that will ensure AI is operated for the benefit of people and any externalities are swiftly addressed. The OECD Recommendation is geared towards governments, which would be an important factor for insurance regulators and supervisors to take into account while being subjected to the wider policy framework that is developing related to AI.

A number of supervisors have established regulatory sandboxes and innovation hubs to spur innovation in the financial sector by establishing platforms to enable experiments with their technology and relaxing some of the regulatory requirements within the platform.[8] The UK Financial Conduct Authority (FCA)'s Innovation Hub is one of the first applying the "regulatory sandbox" approach. Singapore's Monetary Authority of Singapore (MAS) has also adopted the regulatory sandbox approach. Australia's Securities and Investment Commission (ASIC) has established an Innovation Hub to mitigate risks by engaging early with innovators and helping new entrants understand the regulatory requirements. The Hong Kong Monetary Authority and Canada's Ontario Securities Commission have also launched similar platforms. These platforms are all designed to assist new market entries that would encourage greater competition and innovation in the market, ultimately benefiting consumers.

The regulatory sandbox approach intentionally creates a space for insurance technology to be experimented in a different regulatory regime from the regular regulatory requirements. This supports better understanding of when technologies are deemed successful and scalable, and how they will be graduated into the regular regulatory framework if this is the case. Another possible approach in that regard are Innovation Hubs, which do not create different/parallel regulatory regimes. Going forward, this will be important in ensuring that a level playing field is applied at the appropriate stage.

A relevant development that is taking place between the MAS, the FCA and the ASIC are bilateral cooperation agreements between the authorities that allow them to make referrals on innovative businesses seeking to enter each other's market. This would assist in enabling innovators to transfer their business models on a cross-border basis, assisting with the businesses to scale when the opportunity arises. This responds to the OECD AI Recommendation in having better international cooperation to progress on responsible stewardship of trustworthy AI. This is also relevant with regards to data transfer, as data is a key component of the insurance sector and cross-border cooperation to enable this, where appropriate, should be discussed.

The more important aspect is how could insurance regulators and supervisors appropriately monitor and take necessary action when inappropriate decision making by AI has been detected. This is in fact an economy wide issue, which governments are struggling to respond to. There are principally two ways in which the two international guidelines foresee government intervention: explainability/traceability/auditability, and human intervention.

As the OECD Recommendation is subject to development of implementation guidelines, the AI HLEG Guidelines provide some context on human intervention. Human oversight is intended to ensure that AI does not undermine human autonomy or causes other adverse effects. It refers to oversight in the form of governance mechanisms such as human-in-the loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) approaches[9] (High-Level Expert Group on Artificial Intelligence, 2019[40]). Practically speaking and given the need for traceability, it seems that a combination of HOTL and HIC would be important in any circumstances in which AI is being developed.

The need to have a HIC approach in particular is implied in the AI HLEG report, in terms of fallback plans and general safety, including AI systems switching from a statistical to rule-based procedure, or asking for a human operator before continuing their action in certain circumstances.

Another relevant issue, however, as raised in the OECD Recommendation, is the need for policies that build human capacity in AI. The skill shortage related to AI development is a wide ranging problem, with some research suggesting that while 95% of US and UK organisations consider AI to be a business priority,

51% acknowledge they do not have the right mix of skills within their organisation to execute this (snapLogic, 2019[41]). The French financial sector supervisor, *Autorité de contrôle prudentiel et de résolution* (ACPR), published a report in 2018 which includes a glossary of AI jobs[10] (Fliche and Yang, 2018[42]). This list is long and presents the challenges of any supervisor, or company for that matter, trying to monitor their AI activities.

At this stage of adoption of big data and AI in the insurance sector, which is still relatively early, a basic governance structure that can tract and manage AI does seem important and is suggested in the ACPR report too (Fliche and Yang, 2018[42]). This could ensure a level of responsibility within an insurance entity that is using the technology, as well as providing the supervisor with a way to address any supervisory concerns. It should be expected that as soon as any potential bias or unintended consequences from AI are detected, which could also be indirect and affecting individuals and groups, a human intervention be made to examine and rectify the situation to ensure fairness of the process.

However, the way in which AI works could make it almost impossible to make this determination unless there is a consultation process with supervisors at the HOLT or design stage, or data analysis of AI outcomes is made. Article 22 of the European Union's General Data Protection Regulation (GDPR) requires that when automated decision-making is used for profiling an individual, the data subject can object to an automated decision (Proust, 2015[43]). The data controller must then implement "suitable measures" to safeguard the rights of individuals, and permit human intervention and importantly to obtain information on the basis by which the automated decision was made. This has been widely referred as the GDPR's "right to explanation" and the European Commission has prioritised support in developing explainable AI (European Commission, 2018[44]).

However, practically speaking, it is unclear what explainable AI would require and how regulators might be able to get the necessary expertise or information to make this requirement viable. Discussions with experts in the OECD's Insurance and Private Pensions Committee did not provide any clarity on the issue, whether in a specific insurance context or a more general context, although this requires further consideration among regulators.

Thus, insurance regulators and supervisors should keep abreast of developments related to AI in the insurance sector either planned or being undertaken, and learn from developments in other sectors. In addition, and depending on the level of market development and size of entities, insurance regulators and supervisors may wish to develop basic governance requirements as a first step to ensuring that a minimal level of understanding and responsibility of AI is *in situ* in the insurance entity, as well as providing supervisors a way to monitor developments.

Ways in which AI can/is being applied in the insurance sector

When there is an article on how AI can be taking over workforces, insurance, and in particular claims handling, is the prime example that is always provided (Wright, 2019[45]). While there have been a number of insurance entities attempting to harness AI to their processes, the level of adoption has not been as straight forward as has been suggested.

In the insurance sector, there are a number of ways in which AI could be adopted to improve the efficiency of transactions and business processes (Box 3.7). Some examples that have been previously examined by the OECD include robo-advice (OECD, 2017[4]). Robo-advice is being developed for investment management and, in particular, to provide quotes with automated advice and offerings calculated through algorithms. Automated advice could assist pockets of population that do not have access to financial advice to gain input in a more cost-efficient way than a human advisor.

While price comparison and distribution sites are becoming wide spread, much effort is being made to develop sites that provide financial guidance, which is tailored to the policyholder's income and needs, with greater automation through algorithms for products with investment and/or long-term saving components.

This could assist in narrowing the protection gap of the lower income population, as the cost of such services is lower. For example, robo-advice has the ability of developing a financial plan addressing multiple goals, including retirement, protection needs, estate planning and health/long-term care coverage. Robo-advice allows privacy, which some may feel more comfortable with given the sensitivity in discussing money matters.

Insurance start-ups such as Lemonade and PolicyGenius use AI to support their policy offerings. AI can simplify and tailor policy offerings to match the needs and financial situation of the policyholder. A number of start-ups are integrating AI to their processes, and their success will affect how the wider insurance sector introduces AI into its businesses as well.

An area that is considered to be well suited for AI adoption is claims management, as AI processes can speed up claims payment significantly (Hehner et al., 2017[35]). However, there are also concerns that the rapidity can compromise the optional payment, as well as potentially being open to fraudulent claims (Ralph, 2019[46]), although EIOPA's thematic review, in fact, identified fraud detection to currently be the most common case use of big data analytics (EIOPA, 2019[6]). While companies like Claim Technology have been providing machine learning systems for claims handling, it appears that the experience has not been uniform. While Zurich, for example, has benefited from machine learning automation for human resource management, it is not clear whether current machine learning would be able to handle complex analytical and sorting work, such as assessment of insurance claims for car crashes or burglaries (Wright, 2019[45]). Humans had to override the computer's decision too often in the past.

However, the scope in which AI can be deployed in insurance is significant, and how conventional insurers, as opposed to start-ups, are applying AI in their processes will provide important input into this development.

Box 3.7. Impact of AI on insurance business models

AI application in the insurance sector has the potential to improve the efficiency of processing data and making decisions in terms of both contracting and claims processing, as the more obvious areas. Situations where there is interaction with consumers, and where transaction costs are particularly high, are particular areas in which efficiency gains could be made.

However, AI could also be introduced into the internal systems of insurers to harness data that is being collected to support the data analytic process.

Life insurance that includes an investment component could leverage AI to support the investment decision of policyholders.

Non-life insurance, such as parametric insurance, takes advantage of pre-determined criteria to trigger claim payments, which AI could process in an automated fashion, and is particularly suitable to AI processing. This could reduce premium level and benefit less developed insurance markets where parametric insurance is being widely deployed.

Considerations for policy and regulation in AI

The underlying algorithm of AI is not transparent in most cases, especially in deep machine learning, and biases could be built in, both unintentionally and intentionally, potentially leading to inappropriate advice/output. The understanding of how this impacts policyholders' behaviour but also insurers' solvency and reputation, and how regulation should address this is unclear, but is an area that requires greater discussion.

Given the potential for AI to become ubiquitous in the insurance sector, it is imperative that while encouraging innovation, regulators and supervisors invests in better understanding the underlying technology. Innovation Hubs or regulatory sandboxes are part of this process for determining the appropriate regulatory approach, especially when there are cross-border cooperation arrangements. But as conventional insurance companies introduce new technology into their internal processes, it will become increasingly important to hold dialogues with insurers to be able to understand the data that is being used, and potential impacts that could be built into the AI.

Regulators will also need to monitor whether AI outcomes are leading to inappropriate pricing and/or marketing, in particular related to retail policyholder protection. Generally speaking, the transaction cost of a retail policy offering is higher than a commercial policy offering. This provides an incentive for insurers to seek ways to reduce the transaction cost with retail policyholders, and applying AI to such processes would seem an ideal way to do so.

Digital security and data protection would also become a consideration, as AI could request data via an open internet connection or a database, which could allow for the system to be hacked, requiring approaches to prevent such security incidents and developing contingency measures for when such an incident occurs.

AI also raises ethical questions, as election hacking has well demonstrated. While ethical questions are applicable for any AI, some questions may be more relevant for the insurance sector. As we have witnessed from video games and click-bate headlines, humans are already starting to behave in certain ways in response to machine generated contents as the reward centre of the brain reacts positively to such contents (Bossmann, 2016[47]). The long-term implications of having mainly machines interacting to conclude a transaction could lead to customers reacting in unexpected ways, assuming that they are interacting with a human customer service agent.

Ethical questions are complex as machines take on cognitive work with social dimension for duties that were previously performed by humans. International guidelines by the OECD and the AI HLEG are key starting points for thinking of how to approach ethical issues of AI. There are a number of elements that AI may need to strive to achieve, to ensure that it is ethical. This includes being predictable to those that govern the system, robust against manipulation, and finding the person responsible for getting things done (Bostrom and Yudkowsky, 2018[37]). These may also be some of the elements that policymakers should consider whether they are necessary in a regulatory context, for AI to be integrated into systems of the insurance sector.

In relation to this, some have explored the idea of “explainable AI” which encourages the notion that AI also needs to be able to respond to questions on “why” it has reached certain decisions. AI is often not trusted to reach the appropriate decision given its tendency to enhance any biases that may be learned (PwC, 2018[32]). Such approaches could support the development of AI that is more widely acceptable in society.

In Germany, the Federal Financial Supervisory Authority (BaFin) established a new division in 2016 to identify and assess innovations in financial technology and their impact on the financial market. In 2018, BaFin published the report “Big data meets artificial intelligence – Challenges and implications for the supervision and regulation of financial services” (BaFin, 2018[48]). Based on potential market scenarios, the report outlined various implications of big data and artificial intelligence for the supervision of financial services.

In France, the *Autorité de contrôle prudentiel et de résolution* (ACPR) launched a Task Force on Artificial Intelligence in April 2018 to investigate challenges that AI poses to the financial sector. They are gathering information from insurers, banks and fintech companies to better understand how AI is being applied, risks and opportunities from AI, and regulatory impediments for adopting AI in the financial sector.

In the United States, the NAIC has launched a State Ahead Initiative to develop a new data platform and business intelligence framework to allow more self-service analytics and facilitate more sophisticated predictive analytics and AI projects to support market, solvency and macro prudential surveillance needs of state supervisors. As State Ahead matures through 2020, the NAIC will experiment with an AI solvency tool to complement these tools. In 2019, the NAIC discussed the use of AI-models by insurers, including governance, data quality and how to reduce the opacity of complex ('blackbox') models.

As a first step, regulators should discuss the possibility of having a governance requirement related to the management of AI in an insurance entity, which may be useful for a corporate to consider as the focus of AI increases, and to have a handle on ethical aspects. Regulators and supervisors should look to gain a better understanding of AI developments so that any skill gap within the supervisor can be identified and filled as the need arises.

In the future, there may come a point when supervisory analysis may become necessary to ensure that AI is not resulting in bias or discriminatory outcomes. Transparency of AI would support this to a certain extent, but there could come a point when greater accountability of outcomes will become necessary. Supervisors could actively monitor complaints data, for example, in the meantime, which could indicate if there is a continuous trend.

Concluding policy and regulatory considerations

Big data and AI will continue to be areas in which many businesses will pay much attention, especially as they become increasingly integrated into business processes. While the insurance sector may be in relatively early stages of adopting big data and AI, the potential for it to impact every step of insurance production as well as business models of insurance is high, and it should serve to improve individuals' and society's well-being and welfare.

The benefits that can be gained from use of big data and AI could potentially be wide ranging and high. Thus, it is important that opportunities are available to develop potential innovations that can be brought to insurance production, and **regulatory sandboxes and innovation hubs** could facilitate such developments. At the same time, there are risks to the technology as well as potential unintended consequences. A balanced but vigilant approach is necessary to ensure that the maximum benefits can be reaped for all stakeholders.

Being conscious of the potential social costs of using big data and AI, including privacy and ethical concerns, and being proactive when issues are arising is a key role that policymakers should play in ensuring that consumer protection and fairness in the market can be achieved. While in most cases regulation may be technology neutral and not necessitate the development of specific regulation, there are particular areas in which good cooperation with other governmental agencies will be key to having a better understanding of how to ensure that broader regulation is being appropriately applied, as well as how it should be interpreted and applied in the insurance sector.

Privacy and data protection requirements are, generally, an issue for the general data protection agency to prescribe, but given the nature of insurance, if the insurance sector is taking advantage of big data, it could become necessary to ascertain the means in which databases are acquired, and the appropriateness of the data being used for its analytics. There are already some instances of insurance supervisors imposing additional requirements, and the advent of big data and AI could become such an occasion too.

Technology has the tendency of exacerbating existing **market structures**, and companies using big data and AI could accelerate this process. The access some firms have to particular big data or AI technology should be monitored to ensure that it does not result in an oligopolistic market structure. Digitalisation has encouraged some regulators to look into different norms and principles to establish consumer welfare

(European Union et al., 2019[29]). This could be an important consideration for insurance regulators too and consumer welfare should in any case be carefully monitored.

Risk classification can lead to potential exclusion from an insurance policy or could hamper affordability, and big data can accelerate this process. Understanding and drawing lines on what types of big data can be used will become an important part of how insurance regulation ensures reasonable and appropriate use of big data.

A lot can be learned from the recommendations on AI of the OECD and the AI HLEG for the insurance sector. While broader guidance and requirements could be implemented at the national level for AI applications in general, insurance regulators could take steps to better monitor AI developments by requiring a **governance structure** that manages this in insurance entities. This will be particularly important for insurance regulators, so they might be able to request human intervention when unintended consequences or bias is detected from AI decision making. Regulators may need to analyse whether AI is resulting in unwarranted biases or discriminatory practices.

Given the GDPR's wide reach, a better understanding of how to make **AI explainable** is needed. It will be imperative to keep abreast of developments in relation to this aspect of AI for insurance regulators too, as the criteria on what constitutes an explainable AI could emerge, in addition to what actions can be taken when any inappropriate decision making is detected from AI.

There is a lack of skills related to AI both in the regulatory/supervisory side, as well as in the industry. This is not limited to the insurance sector, as the **skill shortage** is a challenge to all industries.

Greater **international cooperation on technological developments** and **facilitation and cooperation on cross-border activities** would also be an important consideration, regardless of whether there is a regulatory sandbox/innovation hub or not. This could be particularly important for **data transfers** that may be happening and being able to ensure that data is being collected and used in an appropriate manner.

References

Accenture (2019), *Global Fintech Investments Surged in 2018 with Investments in China Taking the Lead, Accenture Analysis Finds; UK Gains Sharply Despite Brexit Doubts | Accenture Newsroom*, Accenture New Release, https://newsroom.accenture.com/news/global-fintech-investments-surged-in-2018-with-investments-in-china-taking-the-lead-accenture-analysis-finds-uk-gains-sharply-despite-brexit-doubts.htm (accessed on 18 June 2019). [3]

Allianz SE (2014), *Allianz and Deutsche Telekom enter into a digital alliance*, https://www.allianz.com/en/press/news/financials/stakes_investments/news-2014-06-06.html (accessed on 18 March 2019). [15]

Anyoha, R. (2017), *The History of Artificial Intelligence*, Harvard Science in the News, http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ (accessed on 23 August 2018). [30]

BaFin (2018), *Big Data meets artificial intelligence– Challenges and implications for the supervision and regulation of financial services*, https://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html (accessed on 20 January 2020). [48]

Balasubramanian, R., A. Libarikian and D. Mcelhaney (2018), *Insurance 2030-The impact of AI on the future of insurance*, https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Insurance%202030%20The%20impact%20of%20AI%20on%20the%20future%20of%20insurance/Insurance-2030-The-impact-of-ai-on-the-future-of-insurance.ashx (accessed on 23 August 2018). [36]

Bossmann, J. (2016), *Top 9 ethical issues in artificial intelligence | World Economic Forum*, WEF, https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/ (accessed on 29 August 2018). [47]

Bostrom, N. and E. Yudkowsky (2018), "The Ethics of Artificial Intelligence", in *Artificial Intelligence Safety and Security*, https://intelligence.org/files/EthicsofAI.pdf (accessed on 29 August 2018). [37]

Chen, Chiang and Storey (2012), "Business Intelligence and Analytics: From Big Data to Big Impact", *MIS Quarterly*, Vol. 36/4, p. 1165, http://dx.doi.org/10.2307/41703503. [9]

Deloitte Digital (2017), *Artificial intelligence: From mystery to mastery (AI in insurance whitepaper)*, https://www2.deloitte.com/de/de/pages/innovation/contents/artificial-intelligence-insurance-industry.html (accessed on 23 August 2018). [33]

EIOPA (2019), "Big data analytics in motor and health insurance: A thematic review", http://dx.doi.org/10.2854/54208. [6]

EIOPA (2018), *EIOPA seeks evidence on the use of Big Data*, https://eiopa.europa.eu/Pages/News/EIOPA-seeks-evidence-on-the-use-of-Big-Data.aspx (accessed on 19 March 2019). [27]

EIOPA and NAIC (2018), *EU-U.S. Insurance dialogue project big data issue paper*, https://www.naic.org/documents/committees_c_catf_related_price_optimization_white_paper.pdf (accessed on 19 March 2019). [7]

European Commission (2018), *A European approach to Artificial Intelligence*, MEMO, https://europa.eu/rapid/press-release_MEMO-18-3363_en.pdf. [44]

European Supervisory Authorities (2018), *Joint Committee Final Report on Big Data*, https://esas-joint-committee.europa.eu/Publications/Reports/Final%20Report%20on%20Big%20Data.pdf (accessed on 19 March 2019). [26]

European Union, J. et al. (2019), *European Union report Competition Policy for the digital era: Final report*, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf (accessed on 20 September 2019). [29]

FCA (2016), "FS16/5: Call for Inputs on Big Data in retail general insurance | FCA", No. FS16/5, https://www.fca.org.uk/publications/feedback-statements/fs16-5-call-inputs-big-data-retail-general-insurance (accessed on 13 March 2019). [12]

Fisher, M. and A. Taub (2019), *On YouTube's Digital Playground, an Open Gate for Pedophiles - The New York Times*, New York Times, https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html (accessed on 23 September 2019). [38]

Fliche, O. and S. Yang (2018), “Artificial intelligence:challenges to the financial sector”, ACPR, Banque de France, https://acpr.banque-france.fr/sites/default/files/medias/documents/2018_12_20_intelligence_artificielle_en.pdf (accessed on 17 September 2019). [42]

Gandomi, A. and M. Haider (2015), “Beyond the hype: Big data concepts, methods, and analytics”, *International Journal of Information Management*, Vol. 35/2, pp. 137-144, http://dx.doi.org/10.1016/J.IJINFOMGT.2014.10.007. [10]

Hehner, S. et al. (2017), *Smart claims management with self-learning software Artificial intelligence in health insurance*, https://www.mckinsey.com/~/media/McKinsey/Industries/Healthcare%20Systems%20and%20Services/Our%20Insights/Artificial%20intelligence%20in%20health%20insurance%20Smart%20claims%20management%20with%20self%20learning%20software/Artificial%20intelligence%20in% (accessed on 23 August 2018). [35]

High-Level Expert Group on Artificial Intelligence (2019), *Ethics guidelines for trustworthy AI | Digital Single Market*, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (accessed on 16 September 2019). [40]

Howlett, A. (2019), *Fitness trackers enter the pet insurance market | Financial Times*, FT, https://www.ft.com/content/7a5c06b8-4fcb-11e9-b401-8d9ef1626294 (accessed on 27 March 2019). [18]

IAIS (2020), *Issues Paper on Use of Big Data Analytics in Insurance*, https://www.iaisweb.org/page/supervisory-material/issues-papers//file/89244/issues-paper-on-use-of-big-data-analytics-in-insurance (accessed on 7 October 2020). [14]

Investopia (2018), *Data Analytics*, Investopia, https://www.investopedia.com/terms/d/data-analytics.asp (accessed on 18 March 2019). [13]

Jack, A. (2018), *How AI can spot exam cheats and raise standards | Financial Times*, Financial Times, https://www.ft.com/content/540e77fa-9fe2-11e8-85da-eeb7a9ce36e4 (accessed on 24 August 2018). [39]

Keller, B. et al. (2018), *Big Data and Insurance: Implications for Innovation, Competition and Privacy*, http://www.genevaassociation.org (accessed on 19 March 2019). [28]

Kessler, D. (2018), *The Impact of Artificial Intelligence on Tthe (Re)insurance Sector*, https://www.scor.com/sites/default/files/focus_scor-artificial_intelligence.pdf (accessed on 23 August 2018). [31]

Laney, D. (2001), *Application Delivery Strategies*, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (accessed on 13 March 2019). [8]

Manyika, J. (2017), *Technology, jobs, and the future of work | McKinsey*, McKinsey Global Institute Executive Briefing, https://www.mckinsey.com/featured-insights/employment-and-growth/technology-jobs-and-the-future-of-work (accessed on 18 June 2019). [2]

Miailhe, N. (2018), *Competing in the age of artificial intelligence: current state of AI & interpretation of complex data*, https://www.scor.com/sites/default/files/focus_scor-artificial_intelligence.pdf. [34]

NAIC, Big Data Working Group, S. (2018), *Summary - Big Data (EX) Working Group*. [25]

NZ, T. (2019), *IAG turning down new property insurance in Wellington region | 1 NEWS NOW | TVNZ*, TV NZ, https://www.tvnz.co.nz/one-news/new-zealand/iag-turning-down-new-property-insurance-in-wellington-region?variant=tb_v_1 (accessed on 18 March 2019). [24]

OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264311992-en. [1]

OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264282148-en. [5]

OECD (2017), *Technology and innovation in the insurance sector*, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf (accessed on 28 August 2018). [4]

Proust, O. (2015), *Getting to know the GDPR, Part 5: Your big data analytics and profiling activities may be seriously curtailed - Privacy, Security and Information Law Fieldfisher*, https://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-5-your-big-data-analytics-and-profiling-activities-may-be-seriously-curtailed (accessed on 17 September 2019). [43]

PwC (2018), *Explainable AI: Driving business value through greater understanding*, https://www.pwc.co.uk/audit-assurance/assets/explainable-ai.pdf (accessed on 23 August 2018). [32]

Ralph, O. (2019), *AI can streamline insurance claims — but at what cost? | Financial Times*, Financial Times, https://www.ft.com/content/2df82a56-9c22-11e9-9c06-a4640c9feebb (accessed on 24 September 2019). [46]

RMS (2018), *A risk-driven business | Exposure*, RMS Exposure, https://www.rms.com/exposure/a-risk-driven-business/ (accessed on 18 March 2019). [21]

Russell, J. (2019), *Fitbit's newest fitness tracker is just for employees and health insurance members | TechCrunch*, TechCrunch, https://techcrunch.com/2019/02/09/fitbit-inspire/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=1Z8DNEnppViJR8Mf2OdseQ (accessed on 18 March 2019). [16]

snapLogic (2019), *AI Skills — 93% of Organizations Committed to AI but Skills Shortage Poses Considerable Challenge | SnapLogic*, snapLogic, https://www.snaplogic.com/press-releases/ai-skills-shortage-research (accessed on 17 September 2019). [41]

Stepanova, K. (2018), *Premium hikes are here to stay as more insurers adopt risk-based pricing | Insurance Business*, Insurance Business Mag, https://www.insurancebusinessmag.com/nz/news/breaking-news/premium-hikes-are-here-to-stay-as-more-insurers-adopt-riskbased-pricing-103955.aspx (accessed on 18 March 2019). [22]

Swedloff, R. (2014), *RISK CLASSIFICATION'S BIG DATA (R)EVOLUTION*, http://www.weforum.org/reports/ (accessed on 18 March 2019). [20]

Taylor, C. (2018), *Structured vs. Unstructured Data*, Datamation, https://www.datamation.com/big-data/structured-vs-unstructured-data.html (accessed on 13 March 2019). [11]

thisMatter (n.d.), *Insurance Marketing Systems*, thisMatter, https://thismatter.com/money/insurance/insurance-marketing-systems.htm (accessed on 18 March 2019). [49]

thisMatter (n.d.), *Rate Making: How Insurance Premiums Are Set*, https://thismatter.com/money/insurance/rate-making.htm (accessed on 18 March 2019). [19]

Tibshraeny, J. (2018), *State and AMI home insurance policyholders in parts of the country deemed risky to receive premium increases of around $91 a year under IAG's new pricing model | interest.co.nz*, Interest.co.nz, https://www.interest.co.nz/insurance/94931/state-and-ami-home-insurance-policyholders-parts-country-deemed-risky-receive (accessed on 18 March 2019). [23]

Vitality (2019), *Fitness Tracker Offers*, https://www.vitality.co.uk/rewards/partners/activity-tracking/ (accessed on 27 March 2019). [17]

Wright, R. (2019), *Workplace automation: how AI is coming for your job | Financial Times*, Financial Times, https://www.ft.com/content/c4bf787a-d4a0-11e9-a0bd-ab8ec6435630 (accessed on 30 September 2019). [45]

Notes

[1] EIOPA Consultative Expert Group on Digital Ethics in Insurance https://eiopa.europa.eu/Pages/News/EIOPA-establishes-Consultative-Expert-Group-on-Digital-Ethics-in-Insurance.aspx.

[2] You can see a number of clearly spurious correlations at http://www.tylervigen.com/spurious-correlations for example.

[3] The Generalised Linear Model (GLM) is a generalisation of the general linear model. In its simplest form, a linear model specifies the (linear) relationship between a dependent (or response) variable Y, and a set of predictor variables, the X's, so that $Y = b_0 + b_1X_1 + b_2X_2 + ... + b_kX_k$. In this equation b_0 is the regression coefficient for the intercept and the b_i values are the regression coefficients (for variables 1 through k) computed from the data.

[4] Discrimination by gender is forbidden in the EU since December 2012 (According to the European Court of Justice's ruling on the Test-Achat case (Case C-236/09) of 1 March 2011).

[5] For example, in the United States, all states have unfair trade practices laws/regulations, modeled after the NAIC Unfair Trade Practices Act (#880). These laws prohibit unfair discrimination, which, among other things, includes refusing to insure or limiting coverage to an individual due to ethnicity, race, gender, religion, national origin, and other protected classes.

[6] A recent New York Times article exposed how YouTube's recommendation algorithm was exploited by paedophiles, by recommending videos with images of children in the background of home videos.

[7] From the G20 Ministerial Statement on Trade and Digital Economy (8-9 June 2019), https://www.mofa.go.jp/files/000486596.pdf.

[8] Some OECD countries have expressed a preference for innovation hubs given the need to maintain equal treatment of market participants.

[9] From the AI HLEG report:

- HITL refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable.
- HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation.
- HIC refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation. This can include the decision not to use an AI system in a particular situation, to establish levels of human discretion during the use of the system, or to ensure the ability to override a decision made by a system.

[10] The ACPR's list of AI jobs include:

- Data governance, chief data officer, data privacy officer, chief data quality officer.
- AI jobs more generally: data scientist, data analyst, data engineer, ontologist, expert in automated processing of natural language, expert in computer vision, and expert in human-machine interaction.

4 Blockchain as a digital enabler for sustainable infrastructure

This chapter explores how innovation and specifically distributed ledger technologies (DLTs), such as blockchain, integrated with other technologies like the internet of things (IoT) and artificial intelligence (AI), could accelerate a cost-effective low-carbon transition in key infrastructure services. It discusses blockchain's potential role in enabling sustainable infrastructure, presents blockchain's benefits for data and digital application integration, and provides relevant use cases where blockchain could address the key challenges and opportunities in supporting mitigation and adaptation-related activities, especially in the energy, transport and agriculture industries. The chapter also discusses challenges related to blockchain technology and provides a roadmap for blockchain implementation. The chapter concludes with implications for policy makers and suggested steps to leverage the technology's value-added.

Introduction

Embracing new technologies that enable drastic reductions in greenhouse gas (GHG) emissions will be crucial to mitigate the effects of climate change, but it is not always obvious what the big breakthroughs will look like. It is likely that many technologies, operating in concert, will be needed to tackle the complexity of the problem at hand. Investment and innovation in energy storage, renewable energy generation, materials, transportation services, agricultural sciences, and digital technologies are some of the areas that are vital to the low-carbon transition.

A number of digital innovations are emerging in the global economy and offer the potential to transform how systems operate by making infrastructure, manufacturing, trade, and agriculture more connected, intelligent, and efficient. One of the benefits of promoting digital innovation is that it could lead to further innovations, unlocking unforeseen possibilities. This is particularly true in infrastructure services as the potential for innovation within the sector is large. This chapter explores how innovation and specifically distributed ledger technologies (DLTs), such as blockchain, integrated with other technologies like the internet of things (IoT) and artificial intelligence (AI), could accelerate a cost effective low-carbon transition in key infrastructure services.

In principle, blockchains or DLTs, terms which are often used interchangeably, can be used for recordkeeping and the transfer of value (via cryptocurrencies or otherwise) without requiring a trusted central entity to maintain a database and validate transactions. Instead, these functions are accomplished by decentralising the network in which data is stored and by providing a validation mechanism through which all participants in the network have an immutable single "source of truth". The so-called "smart contracts" which are enabled by blockchain technology allow for the automated execution of a transaction when one or more preconditions are met, thus providing a potential for significant efficiency gains.

Physical and digital assets can be represented as "tokens" of value on the shared distributed registries, allowing the tokens to be directly traded among network participants. In essence, these core capabilities allow for the use of cryptocurrencies (e.g. Bitcoin, Ether) as well as tokenised digital records (e.g. property rights, physical property rights) in the context of the infrastructure lifecycle, from financing, and procurement, through tendering and operations.

The G20's 2018 Roadmap to Infrastructure as an Asset Class focuses on ways to improve the overall investment environment for infrastructure (G20, 2018[1]). This work combined with OECD work on infrastructure, data and performance measurement, and finance, yields several key points that are important in the blockchain context:

- Building **greater standardisation in infrastructure** across the value chain, including contractual standardisation and financial standardisation. Greater standardisation of contracts and documentation in the bidding and procurement stages of the infrastructure project life cycle is critical to reducing their cost and complexity, as well as facilitating their comparability. Greater financial standardisation would reduce investment costs and facilitate allocations by institutional investors into infrastructure investment.
- Stressing the **importance of data** to support well-informed investment decisions in infrastructure. New technologies can be leveraged to support greater data availability and quality, particularly when considering the possibilities of IoT, AI, geospatial (satellite), and blockchain in infrastructure systems.
- Solutions to **manage risks in infrastructure investment** through better transparency, identification, or measurement of risks, along with effective mitigation strategies. In particular, the management of political or currency risks associated with infrastructure could be improved by enhanced transparency, accountability, improved regulatory oversight, and enabling frameworks. Even a small reduction in these risks could have a real impact on investment levels in infrastructure, particularly in developing countries.

- Translating efficiency gains, risk identification and reduction into a **lower cost of capital and more efficient risk charges** for infrastructure assets. Tools such as IoT sensors could provide inputs into more accurate financial and credit risk modelling, using real-time data on asset performance. More accurate revenue and cost forecasting using AI tools that can process large amounts of data could also provide further cost savings.

Yet, infrastructure-related actions taken at the national and sub-national levels present some challenges. Firstly, capacity bottlenecks on sub-national levels restrict the investment opportunities of governments, leading to a financing deficit in infrastructure projects. The participation of investors is also often limited due to misalignments between the financial or risk profile of infrastructure projects and investor demands. Secondly, efforts are often not transparent in regards to their alignment with other entities' actions, or compliance with standards, including environmental, social, and governance (ESG) criteria. Thirdly, in some cases investment decisions are made without consideration to climate impact.

Blockchain can be applied as a digital backbone within infrastructure projects and operations. The technology can help to increase efficiency and transparency in global infrastructure systems. Although blockchain is regarded as an emerging technology, a number of working prototypes and collaborative initiatives targeting the transport, energy and agriculture industries have been developed and established to realise their proposed use cases.

When looking at blockchain use cases for infrastructure, the following aspects emerge as key areas to help facilitate investment:

- Improving access to markets and finance for infrastructure;
- Increasing transparency, standardisation, and the quality of data on infrastructure performance, including financial data, operations, and ESG criteria of infrastructure projects;
- Promoting compliance with standards, such as sustainability standards;
- Improving infrastructure operations, processes, transactions, and record keeping;
- Enhancing technological integration, further productivity gains, and new business models.

Transportation, energy, and connectivity infrastructures are essential services; when built to be resilient and consistent with a low-carbon transition, such investment can contribute to growth and development in a sustainable way. The opportunities and challenges of blockchain technology for sustainable infrastructure are discussed throughout this chapter, including a selection of blockchain technology's possible applications that may effectively facilitate climate mitigation and adaption measures, and facilitate further investment in infrastructure. A roadmap for blockchain implementation presents an action plan for bringing ideas to life through proof-of-concept and pilot programmes. The chapter concludes with implications for policy makers and suggested steps to leverage the technology's value-added.

Blockchain initiatives related to sustainable infrastructure

As with all technological developments, technology usually serves as a means for the purpose and should only be implemented if the technology's respective capabilities address specific needs. In regards to sustainable infrastructure, many conventional technologies (for example cloud computing, automation, traditional ERP systems, etc.) could be leveraged to improve current processes and build transparency between the relevant stakeholders. Pros and cons of different technologies should be considered for each problem or project before deciding on and building solutions. Blockchain is especially suited for problems that require coordination of various parties, where interests might be different, or where secure and immutable exchange of information and value is required.

With this in mind, blockchain could be transformative in changing traditional business models in infrastructure industries towards more customer centric models. Two of the largest infrastructure industries

(and emissions intensive), namely the energy and transportation sectors, represent some of the major ecosystems developing applications of blockchain technology.

In the energy sector, a number of initiatives, corporate efforts, and start-ups have emerged in the last two years. Blockchain-based systems and applications are being developed throughout the value chain from generation, transport, distribution and storage, to trading and retail.

One of the earliest technical pilots in the field was the Brooklyn Microgrid in New York City. The project aims to build a peer-to-peer energy exchange, in which citizens trade their self-produced renewable energy with each other (Papajak, 2017[2]). Another example of an early blockchain initiative is the incorporation of the Energy Web Foundation (EWF) as a global consortium of generators, integrated utilities, and related companies such as research institutes, IT service providers and start-ups. In addition to developing a new open-source core technology platform that is purpose-built for the energy sector, EWF has set up several specialised working groups and knowledge exchange forums in order for EWF "affiliates" to accelerate development of blockchain-based applications for certificate of origin markets for green power, demand response programmes, electric vehicle networks, and other application domains.

The transport and mobility sectors have just recently accelerated and increased the breadth of blockchain-related activity. On the one hand, the development and piloting of several blockchain-based digital services is increasing, as most auto original equipment manufacturers (OEMs), tier 1 suppliers, and many software firms are working on solutions to current pain points, such as inefficient processes and data sharing. On the other hand, new ecosystems are forming in the sector. In early 2018, an alliance named the Mobility Open Blockchain Initiative (MOBI) was launched. MOBI is aiming to align the activities of its members, in order to strengthen their collaboration and ultimately increase the effectiveness of their blockchain-based systems, building on network effects and standardisation.

Blockchain technology can also drive the convergence of sectors. By taking the example of mobility as a service (MaaS), otherwise highly isolated industries like the energy and automotive sectors are increasingly collaborating. Given the accelerated adoption of electric mobility and an increased demand of consumers for a seamless journey among transportation elements, the interoperability of infrastructure systems must be increased. Some initiatives have been launched to develop blockchain-based solutions seeking to help mediate mobility-related transactions, such as booking a shared car, or the charging of electric vehicles (Sümmermann et al., 2017[3]).

Reflecting the worldwide efforts and committed investments, it becomes evident that the technology could play a significant role in future technology and business architecture designs as well as enable novel and efficiency-increasing services.

Blockchain's potential role in enabling sustainable infrastructure

It is estimated that annual investment of USD 6.9 trillion through the year 2030 is needed in order to maintain growth trajectories and to achieve with increased confidence climate change objectives and the Sustainable Development Goals (SDGs) (OECD, 2017[4]). Significant challenges also arise regarding the lack of data transparency in current governing systems and the need to involve private and public institutions, as well as end consumers, in the infrastructure value chain. As for achieving the Paris Climate objectives, Figure 4.1 shows the key challenges, which could be effectively addressed by leveraging blockchain technology.

Figure 4.1. Key challenges of the Paris Climate objectives that could be addressed by blockchain technology

- **Financing infrastructure** – New sources of financing, including a well-aligned investment environment, represent key requirements going forward in the low-carbon transition. Transparent and clear processes can serve to gain the trust of investors. Blockchain technology provides a digital layer that helps to tackle these core requirements. New sources of capital can be leveraged by developing efficient blockchain-based investment platforms to finance projects globally. By employing an appropriate blockchain set-up, overall transaction costs could be reduced and the participation of small-scale investors such as small and medium-sized enterprises (SMEs) and individual consumers could be made feasible. Through end-to-end tracking and auditable data trails, investors may transparently track their investments. For successful implementation, an international legal framework would need to be established, which allows for simple investment transactions for the full spectrum of investors.
- **Visibility and alignment** – In the current system, it is difficult to track where climate finance is allocated and to measure its impact. The problem is even more severe as the top recipient countries for climate finance are often also countries with high levels of corruption (Transparency International, 2014[5]). Most countries lack comprehensive and consistent information systems that can show investment pipelines and existing infrastructure, thus impeding decisions on future investments. Visibility of investments through consistent, reliable and accessible data (including ESG reporting and climate-related financial disclosures) will be needed on a global scale in order to effectively steer climate action and reduce search costs for investors. For governments, a transparent information system showing infrastructure pipelines and current operational assets will be a key tool to coordinate and align climate action with other governments or the private sector. By provisioning the right digital infrastructure based on blockchain technology, deeply entrenched, but flexible monitoring, reporting and communication services can be developed in the future. The time to generate reports based on this data can be reduced significantly. As an example, the Intergovernmental Panel on Climate Change (IPCC) could be supported in the preparation of their regular Assessment Report (IPCC, 2018[6]).
- **Awareness and access** – As private and public institutions as well as the global population are important levers in the transition to a sustainable future, it will be essential to build global awareness around environmental issues and increasing consumers' willingness and ability to contribute to climate-friendly action (Nielsen, 2015[7]). Blockchain can act as the transaction-enabling infrastructure of new market models, in which users are incentivised to invest sustainably. Using token- or cryptocurrency-based models and gamification approaches, efficient markets for carbon offsetting activities can be built and scaled. This approach requires customer-centric market models and applications, which are easy to understand and use. Education and providing access to blockchain-based applications will be key for successful implementation.

Blockchain at the centre of data and digital application integration

To address the previously mentioned requirements to ensure that infrastructure is aligned with country and regional investment strategies, organisational and technology-based approaches have to be transformed. As observed in other areas in the public and private sectors, managing climate-related action will require the adoption of innovative digital enablers. Interoperable and well-entrenched "end-to-end" digital data services will be required to increase efficiency. Relevant data, particularly on ESG criteria, needs to be accessible through standardised interfaces, as opposed to being collected in a redundant and uncoordinated fashion through a multitude of databases. While a variety of databases and reporting platforms already exist, they are mostly fragmented. A decentralised network of systems could represent an option to reduce friction in data and transaction flows, while improving on data standards for infrastructure performance reporting (Mattila and Seppälä, 2015[8]).

Traditionally, a trusted centralised entity would be mandated to set up such a global "single source of truth". While centralised entities have many advantages, complex multi-party relationships that require a high degree of transparency and immutable data trails are arguably better served by decentralised blockchain ledgers. The advantages provided by blockchain technology are summarised in Table 4.1.

Table 4.1. Blockchain's benefits in addressing requirements of digital enablers and systems

Requirements	Solutions implementable on a blockchain
Transparency and visibility	The fragmented landscape of process standards and systems leads to many isolated entities holding valuable information for making choices on infrastructure investment, financial forecasting, mitigation and adaptive action. Decentralised ledgers and transaction networks can be a catalyst for standardisation and transparent monitoring, reporting and steering of data collection. For instance, infrastructure financing commitments made by governments, infrastructure contracts and pipelines, and complex public aid schemes can all be registered and analysed on shared ledgers. Reliable analytics services based on the trusted and accessible data trails add a unique opportunity to supporting the alignment of decision-making and investment flows. Accordingly, efficiency gains in supporting functions and administrative processes can be realised on treaty-level, as well as for local government- and company-levels. By deploying "track & trace" functionalities, blockchain can uniquely identify and keep track of movements of physical or virtual goods. The tracing of tangible objects is often achieved by using hardware (e.g. near-field communication "NFC" chips), and intangible objects could be represented by certificates. Challenges arise in the tagging of substances (e.g. in the chemical industry), where tracking is often achieved by tagging the tangible containers.
Data auditability and privacy	Due to the current isolation and fragmented governance, the integrity of data cannot be comprehensively assured. In addition, ensuring data privacy poses a key challenge. Given that redundant and mismatched data is collected within many organisations, the inter-company exchange of data is uncontrolled and opaque to their owners. Based on a single book of accounts, blockchain provides the means to maintain, monitor and analyse data without undermining data privacy and sovereignty. Depending on the blockchain protocol's design, transactions can be made visible only to the related parties, and in addition, parties can interact pseudonymously on the network. Pseudonymity assures an integral data trail and book of records, without revealing a transacting party's identity to the wider network or public.
Process efficiency and automation	The effectiveness of today's network of systems that is used to plan and finance sustainable infrastructure is limited, given numerous non-standardised interfaces and security issues. Cross-border transactions, for example, suffer from a high degree of manual intervention and non-transparent data trails. Building on a blockchain layer, smart contracts can further improve transaction efficiency by automating standardised business processes and payments. Processes like digital entity or asset registrations could be handled much faster for all involved stakeholders, and additionally provide full transparency and traceability of all registrations.

Leveraging blockchain as the digital infrastructure enabler, a foundational blockchain layer could be established, on top of which other blockchains, leveraging also other applications like IoT or AI could be deployed for various purposes.

As outlined in Table 4.1, transparency and visibility of the infrastructure pipeline is of essence. However, assigning a unique identification tag, according to a standardised convention, is not enough. Immutable IDs of assets and projects have to be seamlessly integrated with related IT systems and monitoring services. By adopting a decentralised registry based on blockchain, a new renewable power plant (as an example) with its key specifications can be registered globally. Rather than locating this process with various national and sub-national entities, an effective cross-border system could be provided by

participating governments. Government institutions, development finance institutions (DFIs), non-governmental organisations (NGOs), companies, users, and any other entities could be linked to such a platform. In addition, entities that submit information to such platforms (e.g. utility providers, transport authorities, livestock farms), remain the sole owners and are responsible for the data points in the shared ledger. The transparent, but pseudonymous, tracking of data flows and access management allows the data owners to manage their transactions and interfaces efficiently, without compromising data privacy protection.

Another example is the monitoring of compliance. Blockchains enable the tracking of compliance with technology standards. For instance, infrastructure owners or operators may be legally required to report status information and changes to their infrastructure. Air quality stations in urban locations could be standardised in terms of data quality, identification and software. By implementing an automated monitoring service (such as through sensors that automatically record and transmit quality checks), data from non-compliant air quality stations, and their operator can be flagged and reported to responsible authorities. As data is recorded on the blockchain, automated and even smart reporting and monitoring services can be enabled, bringing together a patchwork of data sources such as satellite imagery, remote IoT sensors, engineering reports, and regulatory reports. Authorised organisations may track the compliance of new infrastructure projects and their financing by setting a compliance and anti-corruption reporting standard that is incorporated on the blockchain network.

Looking beyond the technology's potential to tackle the aforementioned issues, it is important to note the implied depth of a blockchain's integration with the current systems, processes and infrastructures. Compared with other technologies like cloud storage and computing, blockchain technology provides a significantly deeper interaction with processes. Successful blockchain applications require an ecosystem of collaborating parties, who exchange and validate information. With regard to infrastructure, the orchestration of partners and suppliers could take a new dimension by IoT devices, e.g. when using sensors that provide real-time access for stakeholders or act as oracles, which provide information to smart contracts. In this regard, data and process standardisation is a crucial prerequisite for successful blockchain implementations. This applies to applications (e.g. streamlining data collection and availability with user journeys) as well as the organisational set-up (e.g. agreement between application owners and node operators) (Glaser, 2017[9]).

Adopting blockchain networks at the treaty-level, e.g. United Nations Framework Convention on Climate Change (UNFCCC), and government-level, will require standardised protocols and interfaces to leverage process efficiencies and transparent reporting. Through this, financial flows could be made visible and can thus be better aligned, as stipulated in Article 2.1.c, and Article 6 of the Paris Agreement (UNFCCC, 2015[10]). For example, under Article 6 of the Agreement, parties are authorised to negotiate the transfer of some portion of a signatory nation's intended nationally determined contributions (NDCs) to another signatory nation (deemed to be Internationally Transferred Mitigation Outcomes, ITMOs) (CLI, 2018[11]). In this respect, blockchain can encourage agreement on methodologies to track investment flows, and to ensure robust carbon accounting standards.

Given the highly complex relationships and high numbers of actors in the realm of financing and monitoring low-carbon infrastructure, close collaboration and mutual understanding of the technology will be of essence. Today, this advanced degree of corporate collaboration is already in full swing. Within several industries alliances and consortia have been formed, consisting of leading private corporations, public and private research institutions, and technology start-ups. Building viable approaches to adopting blockchain technology and accelerating its maturity, these projects have already yielded new business and market models.

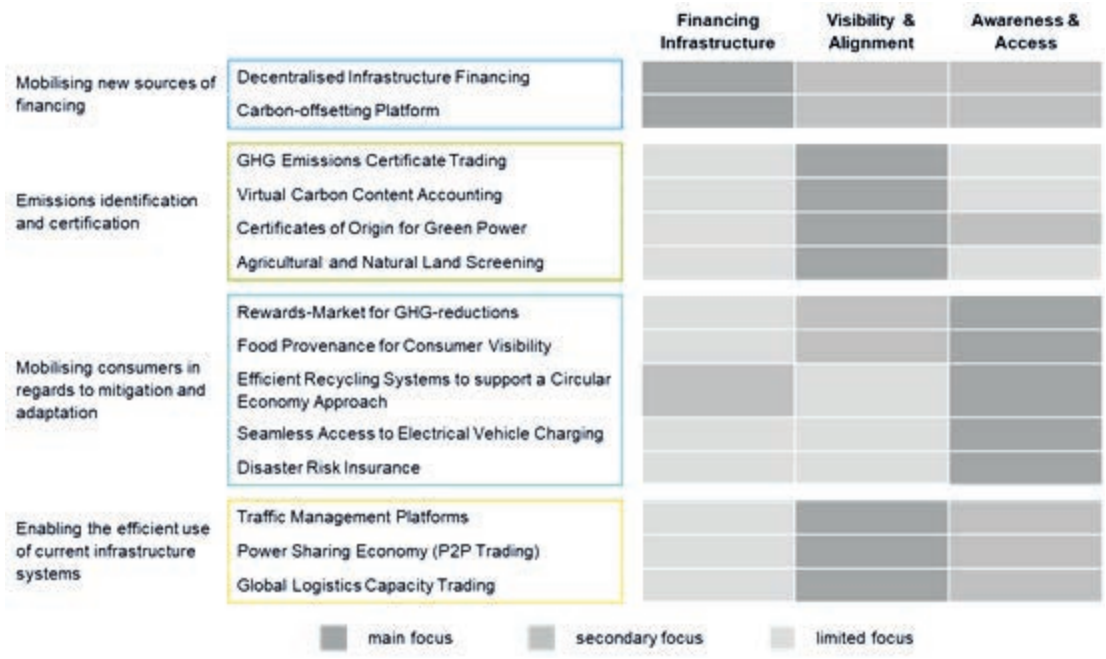
Blockchain as an enabler of mitigation and adaptation-related activities

The role of blockchain in the context of sustainable infrastructure is considered to be far beyond enabling efficient data collection, monitoring, reporting and steering services. The technology can potentially also address the key challenges and opportunities in supporting mitigation and adaptation-related activities, especially in the energy, transport and agriculture industries. Mitigation refers to the reduction of future GHG emissions, which can for example be achieved by assuring that newly planned and built infrastructure is compliant with climate objectives. Adaptation relates to action that helps to cope with inevitable effects of climate change, for example insurance policies for climate-related damages.

Today, a number of blockchain-based services relevant to both mitigation and adaptation have advanced to prototyping and piloting phases. Start-ups and corporate projects are continuing to advance the technology and validate market models. Consortia partnerships and development activities show great potential to scale blockchain networks among immediate stakeholders and beneficiaries.

In the following, a non-exhaustive selection of relevant use cases is presented, which are pursued in the realms of energy, mobility and agriculture. In Figure 4.2, the cases are clustered in categories of action that all account to addressing the three main challenges described in Figure 4.1.

Figure 4.2. Relevant use cases in regards to mitigation and adaptation



Mobilising new sources of financing

Leveraging new sources of financing for infrastructure will be one of the key determinants of reaching investment goals. One of blockchain technology's most promising applications is the idea of a decentralised financing platform for infrastructure. Similar to the investment platform, pollution-offsetting programmes can be supported by a decentralised ledger. Providing unique identification, allocation and tracking services, offsetting commitments can be integrated in corporate sustainability programmes.

Examples of relevant use cases include:

- **Decentralised infrastructure financing** - Similar to today's crowd-investment platforms, assets such as renewable power plants, bike paths, efficient agricultural facilities (e.g. aquaponics and

hydroponics), and many more, can be financed by direct participation of small to mid-size businesses, institutional investors, public sponsors and private individuals. Given blockchain technology's benefit of process efficiency, transparency and fast settlement, even microfinancing can become feasible to outweigh the operational transaction costs and allow for a wider spectrum of investors to participate.

- **Carbon-offsetting platform** - Companies and public institutions choosing to offset their footprint may easily commit a desired amount to a decentralised platform of infrastructure projects. By reducing the transaction costs and strengthening the auditability of their commitment, organisations will have the chance to commit more resources than before. A globally implemented blockchain-based solution, which operates as a not-for-profit, may minimise transaction costs and eliminate the risk of monopolistic behaviour observed in traditional digital marketplaces. In addition, commitments can also be efficiently disclosed to ongoing regulatory measures such as quotas and certificate trading schemes

Emissions identification and certification

Driving climate change-aware behaviour intrinsically or extrinsically through financial incentives requires a comprehensive, reliable and secure digital backbone that provides the necessary information. Whereby today some approaches exist, their restricted interoperability leads to a fragmented landscape of systems, thus hindering widespread adoption among customers and businesses. Blockchain technology can enhance the effectiveness of such solutions, by providing the overarching standard to unique identification and recording transactions of e.g. carbon certificates, their trading, and even the origin of GHG emissions. This transparent and immutable record makes it easier to monitor and incentivise, or impose penalties on, certain industrial practices. Building on existing carbon market models, more efficient and highly integrated trading platforms could be established.

Examples of relevant use cases include:

- **GHG emissions certificate trading** - By using blockchain technology, a highly automated and self-governing decentralised ledger that incepts, holds, tracks, and destroys unique certificates for real-world emissions could be globally implemented. Depicting a new foundational infrastructure layer for the currently implemented carbon certificate systems (e.g. EU emissions trading systems, ETS), a far more flexible and deeply entrenched certification and trading service can be established across all markets. Quota rules and certificate circulation can be controlled by the rules defined in smart contracts, which enforce certificate-related transactions in an automated fashion. On the other hand, climate-mitigating investments (e.g. forests and wetlands) could be sources of carbon credits, which could be monetised by creating, tracking and trading newly generated credits using blockchain technology.
- **Virtual carbon content accounting** - While ETS account for a company's emissions and monitor the adequate compensation through trading of emissions certificates within a specific geographical market, they do not account for emissions that are generated by these same companies outside the trading system's jurisdiction (i.e. "scope three" emissions under the GHG Protocol standard) (GHG Protocol, 2018[12]). In order to accurately assign all emissions that are caused globally by a single company, the carbon content of products and services needs to be identified and tracked across the value chain (lifecycle approach). The carbon content of products, unprocessed products or intermediate inputs can be registered on a blockchain-based system to track the virtual content of imported or exported products, allowing regulators to comprehensively enforce action against climate change.
- **Certificates of origin for green power** - By uniquely identifying and tracking power from renewable sources throughout the value chain (generation, distribution, storage, and consumption), a variety of use cases can be enabled. For instance, emissions caused by the generation of power used by electric vehicles can be uniquely identified and allocated to each

charging process. An open-source decentralised application (dApp) being developed by the Energy Web Foundation has already been tested on several sites. The application offers more granular data (about power ownership, location, time, and avoided marginal CO2 emissions for each kWh) while enabling direct, automated certificate of origin trading between renewable energy generators and buyers of any size (EWF, 2018[13]). This allows consumers to have an enhanced ability to identify and procure from renewable energy assets with greater avoided marginal emissions potential. Blockchain-based solutions modernise the technology tools available for renewable energy tracking, trading, and reporting systems while also disintermediating the process and reducing transaction and administrative costs in certificate of origin markets.

- **Agricultural and natural land screening** - By combining remote sensing, image processing and blockchain technology, a verifiable screening of forests and agricultural land can be established. The natural carbon sinks can be accounted for in near real-time and payments related to their growth, or shrinking can be settled automatically and securely on a blockchain-based platform. For example, the platform can allow screening for the achievement of company or country level mitigation commitments (CLI, 2018[14]).

Mobilising consumers in regards to mitigation and adaptation

Apart from industrial behaviour contributing to GHG emissions, end consumers are also an important lever for building inclusive infrastructure systems. In order to mobilise consumers, it is important to raise awareness, reward sustainable behaviour, provide suitable infrastructure to reduce consumer burden and accelerate adoption levels of individuals.

In this regard, blockchain may provide the IT backbone to transparent information on emissions and consumer choices. Genuine and auditable information on the blockchain can help to increase awareness and design incentives for behaviour that meets certain standards.

To effectively participate in mitigation and adaptation, consumers need to be provided with a suitable infrastructure, which reduces their own individual burden of making sustainable choices. To name one example, the electrification of vehicles is one of today's biggest challenges in the transport and mobility sectors because of the extensive consumer burden caused by lack of charging infrastructure, costly battery systems and user inconveniences in using battery electric vehicles. Consumers and institutions need to be given the right incentives as well as opportunities in order to change behaviours in the long run.

Examples of relevant use cases include:

- **Rewards-market for GHG-reductions** - A blockchain-based cryptocurrency and marketplace could be established, which rewards consumers and organisations that take decisions with a positive environmental impact. For instance, a start-up from the United Kingdom introduced a platform rewarding human activity by foot. By walking, a cryptocurrency is transferred to the user, who can use the credit on a decentralised exchange of merchants offering their services ranging from graphic designers, local food retailers, to NGOs receiving donations (Sweatco.in, 2018[15]). This idea can be transferred to decentralised platforms rewarding users with cryptocurrency. As the platform grows in users and merchants, the value of the cryptocurrency increases and network effects drive the platform's impact.
- **Food provenance for consumer visibility** - A blockchain-based solution for the tracking of food supply chains could provide transparency to consumers about the origin of production. By introducing a label on products indicating the source and including a link to an open database, consumers see whether their food has been sourced in a sustainable way. A prominent example is the track and trace case for tuna to combat illegal fishing. Using devices for tracing (e.g. radio-frequency identification (RFID) tags, quick response (QR) codes, near-field communication (NFC) devices, or cameras), information about the fish can be collected at almost any point throughout

the supply chain (Visser and Hanich, 2018[16]). As the data is recorded on a transparent and immutable registry, each fish can be tracked back to its origin by respective regulators, NGOs, and consumers. The technical implementation of this use case can be applied to other natural capital in agriculture, livestock, and forestry.

- **Efficient recycling systems to support a circular economy approach** - Participation in recycling programmes, although greatly contributing to a sustainable future, currently has few incentives. Through the use of blockchain technology, suitable reward systems can be established to provide transparency and to ensure secure transactions. As an example, a start-up company built an efficient plastic recycling system for developing countries. Individuals can collect and bring plastic refuse to established recycling centres, which in return repay collectors in the form of digital tokens. The received tokens can be used to buy goods like food, water or phone credit. As many of the targeted users are unbanked, the alternatives are cash or mobile payments. Cash payments are especially vulnerable to corruption and crime, making blockchain-based transactions an alternative (Frankson, 2017[17]). In developed countries, blockchain could be used similarly in order to set incentives for responsible consumption, giving different countries a means to help transition upwards in the waste hierarchy from disposal, to recycling and waste prevention, depending on the country's specific infrastructure and consumer prerequisites and needs (Cooper, 2018[18]).
- **Seamless access to electric vehicle charging** - So far, the expected and required rollout of electric vehicles has not yet occurred globally. In addition to high battery costs, there is room for improvement in the required charging infrastructure. Among other factors, the interoperability between charging networks is restricted and leads to an unattractive customer experience. To reduce the consumer burden of adopting e-mobility, a technology venture named Share & Charge has proposed a blockchain-based charging experience. The platform promises to provide open access to any charge pole, including a P2P sharing model. The utilisation of charging infrastructure can be increased to cater to more consumers, reduce costs and due to its technical flexibility, allow integration with adjacent services such as smart grids.
- **Disaster risk insurance** - Some unavoidable effects of climate change can lead to the loss and damage of property, with poor and vulnerable people disproportionately affected. Enhanced disaster risk insurances could provide rapid emergency assistance and financial help to reduce negative impacts from drought, floods or cyclones (Insuresilience, 2018[19]). A lack of full transparency on insurance contract designs, payment terms and the speed of claims pay-outs account for today's most pressing obstacles to effective disaster insurance. Adopting decentralised platforms and automation by smart contracts integrated with oracles (e.g. weather and disaster information), payments based on parametric insurance could be triggered automatically and instantly. By maintaining the complex insurance and re-insurance contracts on shared ledgers, an inclusive data foundation and transaction engine can be created to support disaster recovery efforts. This might not only increase the efficiency by cutting out administrative overhead, but also provide immediate help in situations of need. Such shared ledgers, with open interfaces to related data providers, would allow for a more efficient calculation of underlying volatility, thus leading to potentially reduced insurance premiums. Insurance for disasters may become gradually less cost-intensive given the transparency and access to better data.

Enabling the efficient use of current infrastructure systems

By creating an efficient transaction platform based on a suitable market model, the capacity of today's infrastructure systems can be better utilised. Based on a snapshot of today's infrastructure utilisation rates, all key industries, ranging from power grids, private and public transport assets, or agricultural land, will benefit from such action. Especially in the fields of urban mobility services and power grids, many emerging start-ups and other players have proposed suitable use cases. Blockchain technology supports this development as it enables micro-interactions between a large group of participants in an efficient and

secure way. Platforms rewarding, penalising or automating specific behaviours could be developed based on blockchain technology and, because of the required standardisation, would be highly interoperable.

Example of relevant use cases include:

- **Traffic management platforms** - By securely and selectively sharing the data from mobility assets in a relevant ecosystem of stakeholders, such as auto OEMs, municipal bodies, and map and routing service providers, specialised analytics software can evaluate the data and dynamically set incentives to prefer or avoid certain streets at certain times. In conjunction with today's discussions on restricting combustion engine vehicles in urban city centres, or implementing special tolls, the integration of sensor data (e.g. pollution measurement stations, virtual toll area screening, etc.) and collection of vehicle data on a blockchain network can significantly increase the effectiveness of such mechanisms. Each municipality could design an appropriate traffic control system and implement it as a real-time application on the blockchain layer. Monetary incentives (or fines) can be transferred directly between wallets held by the (shared) mobility assets, its owners or users.
- **Power sharing economy (P2P trading)** - So-called "prosumers", may use their "home-made" energy (e.g. through solar, wind turbines or combined heat and power plants), while also selling the excess energy on a highly automated decentralised platform. Selling the surplus power increases efficiency and resilience of the power plant portfolio, and provides an incentive for the private sector to invest in renewable power plants. Local grid operators and integrated utilities may benefit from more efficient grid operation and decreasing demand for traditional generation assets and power transport infrastructure. However, the shift to a decentralised grid also represents tremendous disruption to traditional power and utility business models (as well as to power grids themselves, which were designed to distribute power from generation to consumer, not from consumer to consumer) and requires increased awareness and knowledge on the part of consumers (Steinberger, Schwarz and Maznic, 2018[20]).
- **Global logistics capacity trading** - The global logistics industry faces many challenges. One of which is managing capacity and utilisation rates in a cost efficient manner. Today many companies are not utilising holding capacities to their fullest extent, as isolated digital systems and limited visibility of capacities result in varying levels of occupancy from low utilisation rates to full capacity. By developing an open registry and transaction backbone for logistics capacities (e.g. containers), available holding capacity can be offered to a broader spectrum of customers while fewer resources would be needed to transport the same amount of goods. Compared to a regular database approach, blockchain provides transparency and security through distribution of data and validation by independent parties. The technology also enables companies to control their data and decide which information is shared with which partner and competitor (e.g. pricing terms). Currently, shipping companies and ports are actively pursuing blockchain solutions for their logistics data in order to improve visibility and reduce fraud (Miller, 2018[21]).

Challenges related to blockchain technology

Although blockchain promises improvements through decentralised systems, several challenges are associated with the technology.

Blockchain has been highly criticised for its high energy and resource consumption (Box 4.1). At a closer look, this criticism is often specifically directed at the Bitcoin blockchain or, more generally, the Proof-of-Work (PoW) consensus mechanism, which encourages specific participants ("miners") to continuously deploy resources to increase their chances of winning the race to validate the next block in the chain. Using other consensus mechanisms than PoW, energy consumption can be significantly reduced. In addition, any comparison would need to consider the degree of energy efficiency in traditional centralised systems.

Box 4.1. Blockchain and energy consumption

Blockchain, or more specifically its first application Bitcoin, is often times linked with high-energy consumption, especially in mainstream media. The immense power consumption is mainly the result of the proof-of-work (PoW) consensus mechanism. This consensus algorithm requires high computational power to solve a mathematical puzzle in order to validate transactions, while many computers compete with each other in order to solve the puzzle and extend the blockchain with new blocks. The decentralised approach to validating transactions and amending new blocks to the blockchain allows for resilience and immutability, yet, coming at the cost of high resource intensity. Another result of the PoW mechanism is that tampering the transaction history recorded on the blockchain requires a significant resource investment, reducing the financial viability of such attacks.

Since the early experiments with blockchain technology, many more platforms that adopted different consensus algorithms (e.g. proof-of-stake) have emerged. Aiming at widespread adoption in enterprise settings, less resource-intensive mechanisms have been developed and implemented. Given that within business networks and enterprises, there is already an initial degree of trust between the participants, a high degree of decentralisation of trust is often traded for less resource intensive consensus mechanisms.

Blockchains in the business context, especially within consortia, are predominantly set up as private blockchains using algorithms like proof-of-authority (PoA). If designed accordingly, private blockchains do not consume more energy than traditional database solutions.

Other applications of DLT like Holochain, Tangle, and Hashgraph have emerged using differing approaches to build decentralised networks. The market for cryptographic technologies is still relatively young and is continually evolving to address known challenges – new algorithms, consensus mechanisms, and methods for sharing data or validating transactions are likely to emerge as DLT matures.

As noted, blockchain technology is deemed to be immutable and tamper-proof. However, the security of a blockchain highly relies on a suitable technical set-up, especially with regard to the degree of distribution, the choice of the consensus protocol and the cryptographic tools used (Deloitte, 2017[22]; Berke, 2017[23]). Firstly, the degree of distribution of network participants, or in other words, the concentration of mining resources in one economic or decision-making entity (e.g. company) can influence security. In theory, a company or state could own, operate or influence more than 51% of a given network's nodes and dominate the proof-of-work consensus mechanism, thereby representing a security risk to the overall system. Secondly, the choice of consensus protocol directly affects the security of a blockchain. Depending on how new blocks are created (e.g. through mining), this process can inherently include measures, which protect the system from malicious attacks. Thirdly, a protocol's underlying cryptographic elements play a decisive role in determining the security standard for a given blockchain. A number of key mechanisms are used in blockchain implementations, most notably key-pairs and hash functions (Badey and Chen, 2014[24]; Böhme et al., 2015[25]).

Due to this highly complex structure, it is almost impossible to manipulate previously captured transactions. The technology can therefore be regarded as a high security technology, but not without vulnerabilities. While the decentralised network is relatively safe from serious hacking attacks due to its set-up, an insecure storage of private keys might enable hackers to gain access to sensitive data. In addition, all interfaces to systems outside the blockchain environment are potentially targets for hacker attacks, if not properly secured.

It is important to note that while data securely recorded on a blockchain is immutable, it might not necessarily be correct. Incorrect data will still stay incorrect after putting it on the blockchain ("garbage in,

garbage out"). The use of blockchain does not change the correctness of data. Data quality and validity checks that are written on the blockchain are key factors for consideration, as information that has been introduced to the blockchain cannot be reversed, but only corrected by adding a new block (Bauerle, 2018[26]).

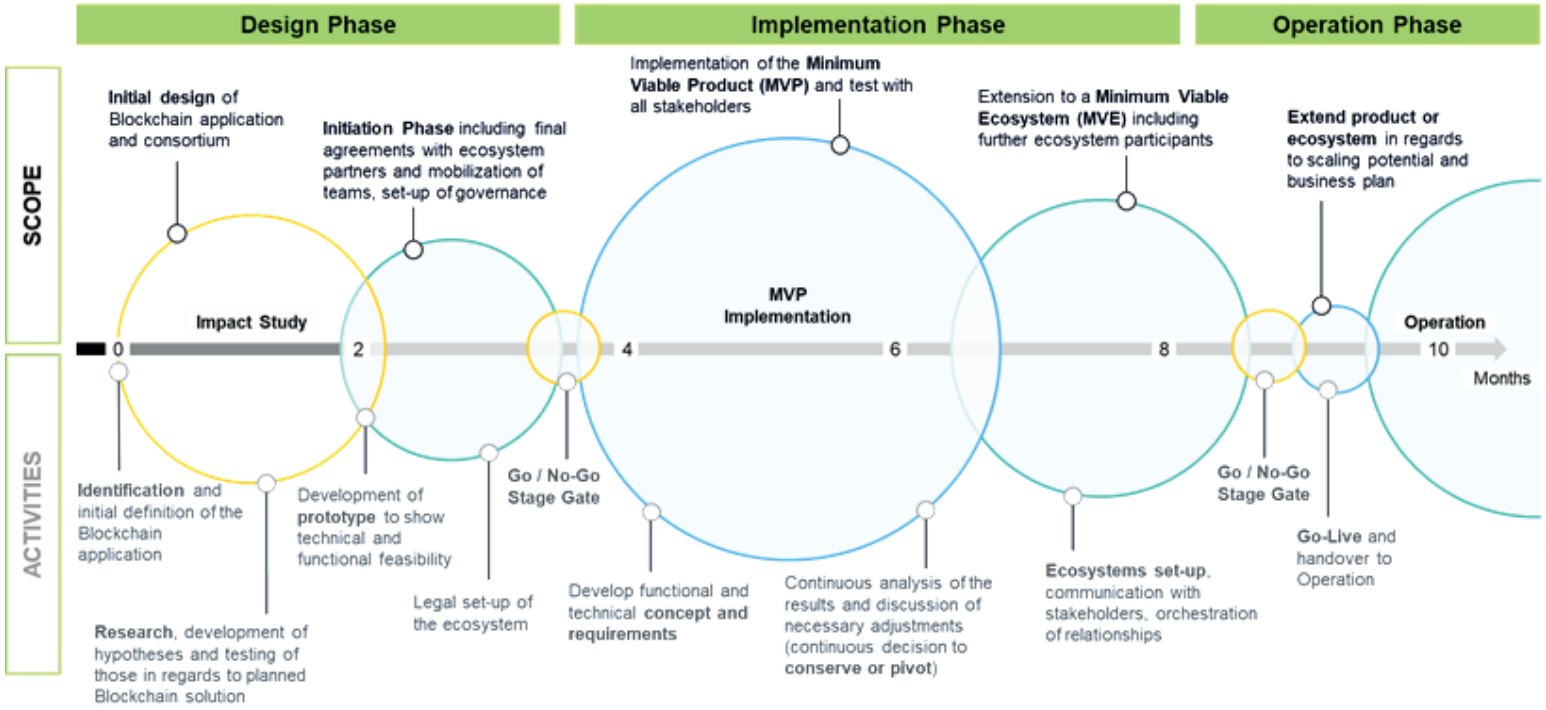
Scalability and processing speed represent additional challenges. Many blockchains are currently not projected to handle high throughput, fast processing speeds, or the large number of participants that may be required for a given application. However, continuous improvements are coming to market as the technology matures, while further theoretical developments are taking place.

A roadmap for blockchain implementation and pilot programmes

In discussing possible use cases for blockchain in regards to sustainable infrastructure, it is important to keep in mind the process of setting up blockchain environments, taking into full account the business case as well as technical set-up. As mentioned earlier, blockchain projects tend to be developed within consortia due to the network nature of the technology. Consortia usually consist of a group of companies and partners, such as technology providers, but may also include regulators or other relevant institutions. It is beneficial to develop pilot programmes for blockchain applications that bring together the main stakeholders, as many additional topics need to be agreed upon (e.g. legal set-up), which are unique to consortia work.

Pilot implementations, meaning implementations with a product and business ecosystem limited in scope and features, are an effective way to test blockchain products in a smaller scale before deciding to propagate into a live operation phase and further develop the solution. In the blockchain space, pilots generally consist of three phases: the design phase, implementation phase and operation phase. As shown in Figure 4.3, various scopes and activities are connected to each phase.

Figure 4.3. Roadmap for a three-phase approach to blockchain pilot implementation



Within the design phase, the overall goal is to identify, describe and set guidelines for the planned blockchain solution and consortium. In the beginning, workshops should be conducted between cross-functional stakeholders and specialists in order to discuss the most pressing issues, where blockchain can pose a valuable solution. The hypotheses developed within these workshops should then be tested and verified through extensive research, potentially including surveys of intended target groups. Implementation costs should be estimated, along with alternatives, comparing also to the status quo: it is important to determine early in the design phase whether a blockchain application is value-adding to its intended use case. By developing a prototype, technical and functional feasibility of the concept can be tested, and the application can be demonstrated to stakeholders. If all decision makers approve the general concept for the prototype, initiation of the business ecosystem of relevant stakeholders can start.

Implementation includes the definition of functional and technical requirements, the concept design for the solution (i.e. blockchain protocol, network architecture, use of smart contracts), as well as the technical development of the solution. Typically, in an agile project approach, the minimum viable product (MVP) and the minimum viable ecosystem (MVE) are developed iteratively. Within the development sprints, there should be continuous analysis of the MVP, its features and its results, and necessary adjustments should be made accordingly. As the solution is ready to launch, the ecosystem needs to be set up by communicating with the stakeholders and orchestrating the relationships.

After completion of the MVP and set-up of the MVE, the pilot can go live. This is usually done as a parallel solution to traditional systems and transactions, in order to fully gauge blockchain potential. From this point on, the pilot programme moves to the Operation Phase and is managed according to the pre-defined plan.

Blockchain implementations are unique in the sense that they operate in a network, often times as a consortium. Not only do the consortium participants need to decide on the type of blockchain solution they want to build, but they also need to agree on adjacent issues before going further into development of the solution. Often times, the most pressing question is around legal set-up and guidelines of collaboration. For example, agreement needs to be reached on which legal form should be chosen for initial and future collaboration, who is contributing how much in investment and resources, how governance of the project should be set up, or who owns the intellectual property created during the project. Once these decisions are made, the teams consisting of individuals from various partners or even external parties need to be brought together and mobilised for development.

Implications for policy makers

For a successful low-carbon transition enabled by blockchain technology, this chapter considers three key activities for policy makers as major areas of focus. First, due to the technology's highly influential and disruptive nature in any business model, related stakeholders must be educated and included in a transparent governance approach. Second, in order to ease friction and pave the way for sustainable blockchain development, a number of regulatory issues need to be addressed. Third, a multi-stakeholder collaboration and active co-innovation approach is needed to design feasible pathways for adoption, especially given that blockchain is still a developing technology. Looking into the future, blockchain could also be leveraged as a regulatory tool for monitoring global standards and laws relating to sustainability.

Support education and research and development

A lack of knowledge regarding the technology is widely observed in the markets. Raising awareness of the technology's value-adding characteristics, as well as education about its drawbacks due to inefficient designs (e.g. energy consumption for proof-of-work consensus algorithm used in Bitcoin), are essential and need to be broadly understood by decision makers. This could also result in mitigating blockchain designs with high-carbon footprints by actively engaging with industry consortia and the private sector to develop protocols and network designs that are less energy intensive. Observing a variety of DLT

technologies (e.g. hashgraphs and tangles) with differing contribution and adverse effects in the low-carbon transition, it will be of essence to develop a strong understanding of the key differences.

It is also important to ensure that careful consideration and analysis are employed in order to assess whether there are clear benefits of deploying a blockchain-based solution rather than utilising existing infrastructures and databases. The OECD has highlighted a number of policy actions to promote technology and innovation, while making sure that digital transformation benefits society. Effective policy actions will seize on opportunities and maximise benefits while addressing challenges and minimising costs. A recent OECD report provides a number of detailed policy actions available to governments in order to facilitate a digital transformation (OECD, 2019[27]).

- In conjunction with the need for education, **an openly accessible, standardised "toolbox" and education material may be compiled**, aiming to support further research and development in the field. In this way, countries and their private and public research institutions can be supported in developing or building on blockchain solutions. The toolbox can be developed and made available in working groups or by international organisations. Developing the toolbox is not expected to involve high costs, as blockchain technologies are already available and are mostly made accessible by developers under open source licensing.
- **Transferring knowledge to developing economies** will also be key to generate buy-in from related stakeholders, and will be essential to implement the case studies presented in this chapter. Through research-based collaborations and partnering with public and private organisations, use case concepts and technologies can be jointly validated.

Take initial steps to improve legal and regulatory environments

Blockchain technology comes with an array of legal and regulatory implications. Due to the nascent status of the technology, legal frameworks and specific laws are yet to be designed and enacted. Because of the physically distributed nature of blockchain networks, sometimes across national borders, the applicable laws and regulations differ for each node (West, 2018[28]). Due to the immutable nature of decentralised registries, and the capability to transfer value by virtue of digital transactions approved by a consensus algorithm, many open questions remain in areas like service level and performance, liability, intellectual property, data privacy, and compliance. The domains of securities law, tax law, legal recognition of data stored on blockchain networks, data privacy laws, and the related improvement of legal and regulatory environments, are discussed due to the proximity of these issues with the previously discussed case studies.

- **In the realm of securities law**, an array of regulatory actions occurred. Various securities and exchange agencies globally have issued statements on their view on blockchain-based token registries (SEC, 2017[29]; Russel, 2017[30]). Yet, the actions are not aligned and treated heterogeneously across different economies. For example, some countries such as China have banned ICOs, whereas they are allowed in countries like Canada, Germany or Israel (Reese, 2018[31]).
- Closely interlinked with the issue introduced above, **tax laws need to be clearly defined in the different jurisdictions**. This is especially relevant for applications in which tokens or coins are issued. For example, the characterisation of tokens has to be aligned for tax purposes, as there is no global agreement on the legal framework for tokens. Hence, the platform may be less attractive to users under more stringent regulatory treatment.
- **The path to a frictionless legal recognition of data** stemming from blockchain registries has been advancing. For example, the US state of Tennessee has passed a bill, which recognises that blockchain data and smart contracts have legal effects (DE, 2018[32]). Yet, a global coverage of this recognition will be a key success factor for blockchain-based networks.

- Beyond recognising data and its immutable trail on the blockchain, **data privacy regulation is to be considered as well**. With the introduction of the European Union's General Data Protection Regulation (GDPR), the question of blockchain technology's compatibility with GDPR arose (Toth, 2018[33]). The "EU Blockchain Observatory and Forum" created a dedicated working group for "blockchain and the GDPR" and launched a report at the end of 2018 stating that compliance can be achieved by blockchain initiatives, but further investigations and rulings are needed (EU Blockchain Observatory and Forum, 2018[34]). **A closer collaboration between governmental regulators and the ecosystem** consisting of actors in the private sectors, such as blockchain consortia and research institutes, needs to be nurtured to cover open questions.

Recently, several communities have formed to drive the exchange and bridging of knowledge gaps between legal practitioners from different jurisdictions and developers (Vidal, John and Rodriguez Jaramillo, 2017[35]). Moreover, comprehensive legal frameworks on blockchain networks and the data stored therein are being proposed in the market. Nonetheless, the complexity of harmonising jurisdictions is a persisting issue, due to differing approaches in treating the technology. While it is not feasible to strive for global standardisation of legal environments across all jurisdictions, policy makers should work on taking initial steps to clarify regulatory treatment for blockchain adoption. In this regard, adjacent standards might need to be adapted, especially in the realms of consumer protection and banking.

Creating a platform for communities by international organisations, such as the OECD Blockchain Policy Forum and the newly established OECD Blockchain Policy Centre, helps to drive the exchange of information and experiences. The OECD has also recently launched the *Sustainable Infrastructure Policy Initiative* in order to pilot the development of tools, standards, and research, along with the promotion of data to inform decision-making in infrastructure investment and policy. The initiative reaches across many subject areas with technological innovation in infrastructure a key component. The next step would be institutionalisation and formalised working groups bringing key stakeholders together.

Encourage co-innovation and collaboration

In view of the presented use cases and their proposed positive impact on sustainability and infrastructure investment, it will be key to take a holistic and collaborative approach to developing and adopting blockchain technology. As observed in the market, a multitude of consortia and alliances have already formed across industries and competitors, to jointly shape the underlying technology standards. Interoperability of blockchains across various initiatives will be key to ensuring progress is made.

- A proactive approach is needed to engage with the major alliances of skilled technology firms and players in their respective sectors. Using the existing technology scouting and ecosystem engagement approach, **relevant national and international organisations and NGOs may initiate and govern dedicated working groups** consisting of selected technology providers and industry representatives, working to study the potential benefits of blockchain. The participation of climate-focused organisations in these working groups will be essential. While providing access to required infrastructure and stakeholders, they may convey the necessary knowledge and experience needed to establish measures on a global level and support the timely alignment with regulatory stakeholders. Partners of the working groups can therefore develop concrete approaches to adopting the technology and validate concepts. The working groups need also to ensure careful consideration and analysis in order to assess whether there are clear benefits of deploying a blockchain-based solution rather than utilising existing infrastructures and databases.
- Throughout the development of new blockchain-based approaches, **a significant standardisation effort will be required for globally established networks**. For example, a global infrastructure registry and performance monitoring system will require countries and their regulators to accept common approaches. While moving towards a global standardised system, hybrid standard models may be required. It should be ensured that while countries can decide on their own blockchain standards, these could be aligned on a global level in the future. Careful consideration

and analysis is required in order to assess whether the immense standardisation efforts associated with deploying a blockchain-based solution are worth the benefits rather than using existing infrastructures and databases.

- **Support could include the creation of standards, methodologies, and the sharing of data on infrastructure performance**, including financial and sustainability metrics, by using blockchain-enabled technology platforms that facilitate transparency and stakeholder engagement.
- Beyond closely supporting the prototyping and development of technical systems via the working groups, **governments and relevant national organisations may govern blockchain networks themselves**. In this way, blockchain nodes that span across the participating regulators globally could be governed by a jointly mandated neutral party. Similar to the not-for-profit foundation model leveraged in the realm of ICOs, blockchain systems can be governed legally and from a management perspective by organisations mandated by the UNFCCC, or other international organisations.

References

Badey, A. and M. Chen (2014), "Bitcoin: Technical background and data analysis", *Finance and Economics Discussion Series, Division of Research and Statistics and Monetary Affairs*, Vol. 104, https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf. [24]

Bauerle, N. (2018), *What are Blockchain's Issues and Limitations?*, https://www.coindesk.com/information/blockchains-issues-limitations/. [26]

Berke, A. (2017), "How Safe Are Blockchains? It Depends", *Harvard Business Review*, https://hbr.org/2017/03/how-safe-are-blockchains-it-depends. [23]

Böhme, R. et al. (2015), "Bitcoin: Economics, technology and governance", *The Journal of Economic Perspectives*, Vol. 29/2, http://dx.doi.org/10.1257/jep.29.2.213. [25]

CLI (2018), *Navigating Blockchain and Climate Action*. [11]

CLI (2018), *Sustainable Land Use*, https://climateledger.org/en/Innovation/Use-Cases.33.html. [14]

Cooper, J. (2018), *Waste Hierarchy: Challenges and Opportunities*, https://www.letsrecycle.com/news/latest-news/waste-hierarchy-challenges-and-opportunities/. [18]

Deloitte (2017), *Blockchain & Cyber Security. Let's Discuss*. [22]

Deloitte (2017), *ICOs – The New IPOs? How to fund innovation in the crypto age*. [37]

DE, N. (2018), *Smart Contracts Now Recognized Under Tennessee Law*, https://www.coindesk.com/blockchain-bill-becomes-law-tennessee/. [32]

EU Blockchain Observatory and Forum (2018), *Blockchain and GDPR*, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf. [34]

EWF (2018), *Origin*, https://energyweb.org/origin/. [13]

Frankson, S. (2017), *Plastic Bank Deploys a Blockchain to Reduce Ocean Plastic*, https://www.ibm.com/blogs/systems/plastic-bank-deploys-blockchain-to-reduce-ocean-plastic/. [17]

G20 (2018), *Communiqué, Finance Ministers & Central Bank Governors Meeting, 19-20 March 2018*, https://back-g20.argentina.gob.ar/sites/default/files/media/communique_g20.pdf. [1]

GHG Protocol (2018), *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*, https://ghgprotocol.org/sites/default/files/standards/Corporate-Value-Chain-Accounting-Reporing-Standard_041613_2.pdf. [12]

Glaser, F. (2017), *Pervasive Decentralisation of Digital Infrastructures: A framework for Blockchain Enabled System and Use Case Analysis*. [9]

Insuresilience (2018), *About the Insuresilience Global Partnership*, https://www.insuresilience.org/about/. [19]

IPCC (2018), *Organization*, https://archive.ipcc.ch/organization/organization.shtml. [6]

Mattila, J. and T. Seppälä (2015), "Blockchains as a Path to a Network of Systems - An Emerging New Trend of the Digital Platforms in Industry and Society", *The Research Institute of the Finnish Economy* 45. [8]

Miller, R. (2018), *IBM Teams with Maersk on New Blockchain Shipping Solution*, https://techcrunch.com/2018/08/09/ibm-teams-with-maersk-on-new-blockchain-shipping-solution/?guccounter=1. [21]

Momtaz, P., K. Rennertseder and H. Schröder (2019), *Token Offerings: A Revolution in Corporate Finance?*, https://ssrn.com/abstract=3346964. [36]

Nielsen (2015), *Green Generation: Millennials Say Sustainability Is a Shopping Priority*, http://www.nielsen.com/ie/en/insights/news/2015/green-generation-millennials-say-sustainability-is-a-shopping-priority.html. [7]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264312012-en. [27]

OECD (2017), *Investing in Climate, Investing in Growth*, http://www.oecd.org/investment/investing-in-climate-investing-in-growth-9789264273528-en.htm. [4]

Papajak, U. (2017), *Can the Brooklyn Microgrid Project Revolutionise the Energy Market?*, https://medium.com/thebeammagazine/can-the-brooklyn-microgrid-project-revolutionise-the-energy-market-ae2c13ec0341. [2]

Reese, F. (2018), *ICO Regulations by Country*, https://www.bitcoinmarketjournal.com/ico-regulations/. [31]

Russel, J. (2017), *First China, Now South Korea Has Banned ICOs*, https://techcrunch.com/2017/09/28/south-korea-has-banned-icos/. [30]

SEC (2017), *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities, U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations*, https://www.sec.gov/news/press-release/2017-131. [29]

Steinberger, T., R. Schwarz and S. Maznic (2018), *Blockchain: From Disruption to New Business Models*, https://www.powerengineeringint.com/articles/2018/05/blockchain-from-disruption-to-new-business-models.html. [20]

Sümmermann, D. et al. (2017), *The Joint Journey Towards Seamless Mobility*. [3]

Sweatco.in (2018), *Sweatcoins*, https://sweatco.in/. [15]

Toth, A. (2018), *Will GDPR Block Blockchain?*, https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/. [33]

Transparency International (2014), *Keep Corruption out to Halt Climate Change*, https://www.transparency.org/news/feature/keep_corruption_out_to_halt_climate_change. [5]

UNFCCC (2015), *Paris Agreement*, https://unfccc.int/sites/default/files/english_paris_agreement.pdf. [10]

Vidal, M., M. John and A. Rodriguez Jaramillo (2017), *LegalBlock: A Blockchain Legal Community Promoting Collective Wisdom*, http://legalblock.co/documents/LegalBlock%20Paper%20I%20.pdf. [35]

Visser, C. and Q. Hanich (2018), *How Blockchain Is Strengthening Tuna Traceability to Combat Illegal Fishing*, http://theconversation.com/how-blockchain-is-strengthening-tuna-traceability-to-combat-illegal-fishing-89965. [16]

West, K. (2018), *Where Is Blockchain?: Jurisdictional Issues That May Affect Distributed Ledgers*, https://www.lexology.com/library/detail.aspx?g=35f40e2e-38d8-49d7-81ca-9872d8ab9532. [28]

5 A consumer-centric analysis of personal data use in financial services

This chapter presents the implications of the use of personal data in financial services from a consumer perspective. It presents the technological, economic and societal developments that have led to an exponential increase in personal data generation, and in data processing capacity. The chapter then focuses more specifically on the financial services sector. It explains how financial services providers collect and use consumers' personal data, analyses the implications this has for consumers, both in terms of advantages and risks, and describes consumer response to these developments. The chapter finally describes specific financial literacy competencies related to personal data that should be considered by policy makers to inform a financial education response to these developments.

Background

Introduction

Personal data have come to play an increasingly important role in our economies and societies. While new technologies and responsible data uses are yielding great societal and economic benefits, the abundance, granularity and persistence of personal data brings new risks to the privacy of individuals. Personal data are increasingly used in ways that were not anticipated at the time of creation and collection, with citizens not fully aware of how their personal data is captured, stored and used.

These trends have an impact on the financial services sector and on financial services consumers. Technological innovations have greatly improved the capacity of financial services providers to capture, store, combine and analyse a much greater variety of consumer data, ranging from their current or previous location to consumer behaviours and preferences. This can bring benefits to consumers, but also new risks that are specific to the financial services sector and that might require a dedicated policy response.

Addressing the implications of the use of personal data in the financial services sector goes beyond financial education. It involves a sound financial consumer protection framework that is fit to protect consumers in digital environments, the existence of national data protection agencies or national data protection strategies with effective resources and enforcement powers, and the need to take into account the levels of digital and financial literacy.

This chapter contributes, from a financial education perspective, to the identification of approaches to foster behaviours that can protect consumers and entrepreneurs from any negative consequences of such developments in the financial sector.

This chapter first highlights the different components of a policy response; it then defines personal data, and presents the technological, economic and societal developments that have led to an exponential increase in personal data generation, and in data processing capacity.

The analysis then focuses more specifically on the financial services sector, explaining how financial services providers collect and use consumers' personal data, before moving to analyse the implications this has for consumers. The chapter describes in particular the risks that can be incurred by consumers, discriminatory decisions based on the use of big data and threats stemming from cybercrime, before presenting the consumer response to these developments, based on evidence collected through global and national surveys that captured their attitudes with respect to use of their personal data.

In light of these developments and the issues they raise, the chapter describes specific elements related to personal data that can complement the policy checklist in the G20/OECD INFE Policy Guidance Note on Digitalisation and Financial Literacy (OECD, 2018[1]).

This chapter was developed as part of the programme of work of the OECD/INFE Working Group on Digital Financial Literacy (see list of members in Annex 5.A).

The components of a policy framework for the use of personal data in the financial services sector

Privacy and personal data protection

The OECD has pioneered international work in the field of privacy and personal data protection.[1] In 1980, this led to the Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, revised in 2013 (OECD, 2013[2]). The societal and technological environment for which these Guidelines were devised has, however, gone through structural changes. As

highlighted in the 2013 work conducted for the review of the Guidelines and its privacy principles, today's economies present substantial differences in:

- the volume of personal data being collected, used and stored;
- the range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- the value of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- the extent of threats to privacy;
- the number and variety of actors capable of either putting privacy at risk or protecting privacy;
- the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate;
- the global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

Amongst other things, the Principles call for:

- the provision of reasonable means for individuals to exercise their rights;
- the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy.

Financial Consumer Protection

Privacy and data protection in relation to financial services can be seen as part of a broader framework of financial consumer protection. The G20 High-level Principles on Financial Consumer Protection (G20, 2011[3]) address this through Principle 8 "Protection of Consumer Data and Privacy". This Principle states:

> *"Consumers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties). The mechanisms should also acknowledge the rights of consumers to be informed about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data".*

The implementation of this principle often involves the presence of authorities with a legal mandate for the protection of personal data. Increasingly, across jurisdictions, this is done through a privacy and data protection authority (OECD, 2019[4]). These independent public authorities supervise, through investigative and corrective powers, the application of the data protection law, provide expert advice on data protection issues, and handle complaints.

As part of its ongoing work on financial consumer protection in the digital environment, the G20 OECD Task Force on Financial Consumer Protection is in the process of developing policy guidance on the protection of consumer data and privacy for financial consumers in the form of updated Effective Approaches to support the implementation of Principle 8.

Financial education and awareness

The need to strengthen financial literacy and awareness on issues around personal data has been addressed in the work undertaken by the OECD/INFE and its Working Group on Digital Financial Literacy.

The G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy (OECD, 2018[1]), transmitted to G20 Leaders in July 2018, calls for the development of specific core competencies on financial literacy that would support consumers in their use of digital financial services.[2] Two areas in particular are relevant in the context of personal data use by financial services providers:

- empowering consumers, including the most vulnerable, to counter new types of exclusion due to the misuse of various data sources, including big data and digital profiling; and
- protecting consumers and small businesses from increased vulnerability to digital crimes such as phishing scams, account hacking and data theft.

Personal data and financial services

What are personal data

Personal data are defined by the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013[2]) as "any information relating to an identified or identifiable individual (data subject)". Any data that are not related to an identified or identifiable individual are therefore "non-personal" data. However, data analytics has made it easier to relate seemingly non-personal data to an identified or identifiable individual, thus blurring the boundaries between non-personal and personal data (OECD, 2015[5]).

Indeed, the European Union General Data Protection Regulation (GDPR) (European Union, 2016[6]) (see Box 5.5), defines personal data as "any information that relates to an identified or identifiable living individual" and stresses that "different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data". The EU framework also stresses that personal data that has been de-identified or encrypted but can be used to re-identify a person remains personal data and falls within the scope of the law.

What contributes to "big data" in the financial services sector and how it is collected

The financial services industry is among the most data intense of today's economies (OECD, 2015[5]).

From a consumer-centric perspective, the flow of personal data from the consumer to financial services providers can be categorised broadly based on the consumer's awareness (see Table 5.1).

Table 5.1. Data collection channel by consumer awareness

Consumer awareness	Data collection channels
Consumer is aware	Data provided by the consumer as part of the KYC process Data given by the consumer in order to support a specific product purchase Data given by the consumer in order to use a specific service such as data aggregation tools Data collected when consumers are using specific financial products such as payment services
Consumer is not aware	Data collected by the provider during consumer interactions Data collected by the provider on publicly available information (social media) Data shared with the provider by a third party such as credit reference bureau

As described in the next section, the amount of information that consumers provide without awareness (or consent) is constantly increasing, because of technological developments that are pervasive to every aspect of our societies and that determine the creation and the capacity to analyse growing amounts of personal data.

However, it is important to note that even the information that is provided with consumer awareness contributes to the pool of data that is created about consumers: the digitalisation of consumer interactions with financial services providers allows them to capture and indefinitely store information about exchanges between consumer and provider, their nature, duration and content. Even a phone call to a consumer's bank manager contributes to the pool of consumer data.

Increased personal data generation and processing capacity

The generation of new personal data

Almost universal access to mobile broadband and smartphones, but with regional and socio-economic differences

The last decade witnessed a steady and significant increase in the number of internet users. The developments in mobile technology have also increased the possibilities of accessing the network "on the go" as well as at home. Internet is used more and more by citizens to conduct their daily lives, make economic transactions of any kind, and interact with public authorities. This creates new personal data, which can – to varying extents- be collected and analysed by third parties.

In 2005, around 56% of the adult population in OECD economies accessed the Internet, and 30% used it daily. In 2016, these percentages rose to 83% and 73% respectively (OECD, 2017[7]). Across mature and emerging economies alike, mobile subscribers followed the same upward trends and by 2025 the number of unique mobile subscribers expected to reach 5.9 billion, which is equivalent to 71% of the world's population (GSMA, 2018[8]).

These general trends do however include differences among countries and sectors of the population. Among OECD countries, in 2016, over 97% of the adult population accessed the Internet in Denmark, Iceland, Japan, Luxembourg and Norway, but 60% or less did so in Mexico and Turkey. There are also differences in usage: in Iceland, Italy, Luxembourg and Norway, the share of daily users is very similar to that of total users, whereas in Mexico and Turkey, many users access the Internet on an infrequent basis (OECD, 2017[7]).

Differences among user groups are mostly based on age and education, often intertwined with income levels. Uptake by the younger generations is nearly universal, but the picture changes for older consumers: over 95% of 16-24 year-olds in OECD countries used the Internet in 2016 compared to less than 63% of 65-74 year-olds. Among older people, education is the major factor affecting internet usage: Internet usage rates for 55-74 year-olds with a tertiary education are generally above or in line with those of the overall population, and in some countries approach the usage rates among 16-24 year-olds.

The Internet of Things

An additional source of consumer data can be traced back to the connected objects and devices that consumers purchase and use. The Internet of Things (IoT) includes all devices and objects whose state can be altered via the Internet, with or without the active involvement of individuals. While connected objects may require the involvement of devices considered part of the "traditional Internet", this definition excludes laptops, tablets and smartphones already accounted for in current OECD broadband metrics (OECD, 2018[9]).

This network of Internet-connected objects is able to collect and exchange data using embedded sensors and contribute to the collection of consumers' locations and behaviours: telematics insurance systems that capture car drivers' behaviours, smart wearables that can capture health-related information such as distance walked each day or physical activity, and smart homes systems. Globally, the number of connected devices is expected to grow to 50 billion by 2020, up from 9 billion in 2013 (OECD, 2017[7]).

Consumers might not be able to select what they share through an IoT device; the device will constantly capture and transfer information, in an unobtrusive way and in the background (OECD, 2018[10]). This creates new risks for consumers. As more and more devices become "smart" (i.e. connected), individuals might lose the capacity to understand the amount of data shared and its privacy implications, let alone monitor its flow and exert some level of control over it. Moreover, consumers are unlikely to have full

awareness of what is done with the data collected (Rosner and Kenneally, 2018[11]). In addition, IoT data might be more easily hacked.

Biometrics

An additional source of personal data is biometric data. Biometric data mostly comes from identity authentication through uniquely physical or behavioural characteristics (e.g. facial recognition, fingerprints, voice recognition). This data had never been generated before, or if it had (such as fingerprints), it had not been digitised. This means it can therefore exist without a clear policy framework.

Biometrics carry yet another risk. Unlike passwords that can be changed after hacking, biometric authentication is not so easy to alter.

Box 5.1. Big Data

Economic and social activities have already migrated or are increasingly migrating to the Internet. This takes place while the cost of data collection, storage and processing continues to decline dramatically. In addition, new sources of data are emerging and ever-larger volumes of it will be generated from the Internet of Things, smart devices, and autonomous machine-to-machine communications.

The generation of these huge amounts of data, at levels that are unprecedented in human history, is often referred to as “big data”. The OECD defines big data as follows:

Big data relates to the huge amount of data generated from activities that are carried out electronically and from machine-to-machine communications (e.g. data produced from social media activities, from production processes, etc.).

Big data have characteristics summarised as “3V” (volume, variety and velocity):

- volume, referring to vast amounts of data generated over time;
- variety, referring to the different formats of complex data, either structured or unstructured (e.g. text, video, images, voice, documents, sensor data, activity logs, click streams, co-ordinates, etc.);
- and velocity, referring to the high speed at which data are generated, become available and change over time (OECD, 2015[5]).

This is in contrast to data processing focusing on low-variety, (relatively) small scale and static datasets, such as consumer satisfaction surveys.

Advances in data analytics

These large volumes of data would bear no economic or social value – and no consequences for financial services consumers- if they were not matched by increasing analytical capacities.

Predictive analytics refers broadly to the technologies and procedures followed to process great volumes of data to reveal patterns or correlations, to unlock income-generating insights, and importantly, to predict future events in a more accurate and timely manner.

Advances are most notable, and have the most important consequences in the financial services industry, in the following areas (OECD, 2015[12]):

- *Data mining*: the set of techniques used to extract information patterns from data sets.

- *Profiling*: the use of data analytics for the construction of profiles and the classification of individual consumers in specific profiles. Credit scoring, price discrimination and targeted advertisements are typical examples of activities involving profiling.
- *Machine or statistical learning* is a subfield in computer science, and more specifically in artificial intelligence, with potentially pervasive and far-reaching consequences for societies and economies (Box 5.3) It is concerned with the design, development and use of algorithms[3] that allow computers to "learn" – that is, to perform certain tasks while improving performance with every empirical data set they analyse. Machine learning involves activities such as pattern classification, cluster analysis, and regression.

These advances allow financial services providers to infer sensitive information from data that is unrelated to the financial services profile of an individual, such as past individual purchasing behaviour, electricity consumption, or the activities of circles of contacts on social media.

A further development that should be taken into account by financial education policy makers looking into issues relating to the use of personal data is blockchain, despite this not being strictly-speaking a development generating personal data per se, but rather storing it.

Blockchain is a technology with huge potential across a wide range of applications.[4] It utilises distributed ledger technology (DLT) to store information verified by cryptography, which is agreed through a pre-defined network protocol, often without the control of a central authority. The technology can be used to secure the transfer and traceability of value as well as the transfer of data. Its distributed nature of nodes makes it attractive for cyber-security and privacy.

The key point to note with respect to this technology is that the personal information that is stored on the blockchain, because of its decentralised character with immutable blocks, cannot be deleted as these are designed to last forever.

How various sources of data are used by financial service providers

The increasing wealth of consumers' personal data, and the possibility to analyse it through more and more sophisticated tools and artificial intelligence, can be used by financial services providers - depending on the regulatory framework - in the following functions and services in particular:

- Consumer profiling: data stemming from on-line behaviour, geolocation tools, electronic payments and wearables can provide financial services providers with valuable insights on the financial lives of their consumers and deliver more detailed consumer segmentation.
- Risk assessment: data contributes to an assessment of risks based on multiple sources.
    - Credit: in jurisdictions with positive credit scoring systems (i.e. in which not only negative credit marks are reported by a central authority), big data (see Box 5.1) and augmented analytics determined the emergence of credit scoring tools that integrate thousands of data points about individuals.
    - Insurance: providers could use data aggregation for risk assessment in many different fields, to achieve more precise risk segmentation and risk-based pricing. For example, data generated by activity sensors or physical activity tracker on a mobile phone can be used to determine a policyholder's potential life expectancy. Data analytics can also be applied to telematics data that monitor the behaviour of policyholders and used to mitigate risk in advance based, for example, on location. This can be applied to a range of insurance products, such as health insurance (where consumer's behaviour is tracked and rewarded through wearable devices and/or home connected sensors), car insurance ("Pay as you drive" and telematics), or home insurance (OECD, 2017[13]).

Face recognition technology and longevity data can be used for underwriting the provision of life insurance. Face recognition technology is used to predict factors such as chronological age, gender, smoking habits and body mass index (BMI) (OECD, 2017[13]).

- Robo-advice applied to develop a personal financial plan with a view to saving, saving for retirement, or investing. Consumer data is processed by robo-advice platforms to understand clients' needs and assess risk tolerance, as well as monitoring and adjusting the financial plan (OECD, 2017[14]).
- Fraud detection, thanks to the near-time (i.e. almost instantaneous) monitoring allowed by artificial intelligence (AI) and, in particular machine learning, which permits a continuous analysis of spending and account management patterns.
- Account aggregation, i.e. the compilation of information from different accounts (checking, investments, savings accounts) into one single place to facilitate personal financial management (see Box 5.2).

Box 5.2. Account aggregation tools

Account aggregation tools, which allow consumers to access their accounts (banking, savings, investments, etc.) in one single place, through a website or a mobile app, can function through two mechanisms:

- Screen scraping, through which consumers provide to a third party their login details, passwords and additional security information such as personal questions, which the third party can use to log in as the consumer.
- Open banking, as in the European Union (European Union, 2015[15]). This does not require consumers to provide passwords to third parties to access accounts on their behalf, and passwords are not shared. Third parties, who are authorised by the financial services authority, connect directly with the consumers' banks, through standardised applied programming interfaces (APIs).

Open banking can deliver enhanced capabilities to the marketplace and allow consumers to access all their accounts (banking, savings, investments, etc.) in one single place, through a website or a mobile app. This can contribute to the emergence of improved and innovative products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services, with new entrants in the market and with incumbents innovating as a response.

The key aspect to consider from a financial education perspective is consumer consent[5] and authorisation, and issues around consumer control. Any provider wishing to access the financial information of a consumer's account must ask for an authorisation, which can focus just on the retrieval of information, or can go further and authorise payment services for example.

Consumers should not feel coerced into granting access to sensitive personal information, such as past bank statements, unless they are aware of this and understand the implications. They should also be aware that, with different modalities according to the applicable regulations, they have the right to revoke authorisation to access, use, or store data.

What are the implications for consumers?

The implications of the increased use of personal data in financial services can be positive for consumers, if they take place within a sound financial consumer protection framework and are matched by sufficient financial literacy and awareness. The increased use of personal data does however also create new risks,

which call for an integrated policy response spanning financial education and awareness and financial consumer protection.[6]

Cheaper, tailored products with extended reach

The advantages brought to consumers by the digitalisation of finance and by the increasing use that can be made of personal data were presented in the G20 OECD/INFE Policy Guidance Note on Digitalisation and Financial Literacy (OECD, 2018[1]). Among these, those that are more influenced by the increased availability of personal data and enhanced data analytics tools are:

- Providing access to consumers that are currently excluded from some financial services, for example thanks to the use of big data that can build on non-financial data points to define an alternative credit rating system for those without a credit history.
- Offering more convenient, faster, secure and timely transactions.
- Broadening the range of providers, with new FinTech firms entering the market.

This has already brought benefits for consumers:

- Lower costs, through increased competition and the emergence of FinTech companies in particular in the payments and lending segments.
- Aggregator services that use financial and payment data from bank accounts of consumers for dashboard and accounting products.
- Robo-advice, which has made financial advice available to consumers that could not afford to receive financial advice through human interaction (OECD, 2017[14]).
- The possibility of creating personalised built-in nudges in the personal financial management tools used by consumers.

However, the increased availability of personal data and augmented processing capacity also gives financial services providers (whether traditional ones or FinTech) the ability to send targeted offers, which can make it more difficult for consumers, especially those with low levels of financial literacy and awareness, to compare products.

Use of big data and machine learning to inform credit or insurance decisions

Depending on the applicable regulatory framework in each jurisdiction, big data and machine learning can be used to inform or determine the risk profile of consumers, notably in the field of credit and insurance.

While it is not new to analyse personal data to determine clients' risk profiles, this can now be done through a range of data points collected about the individual consumer of which the consumer might not be fully aware. Depending on the algorithm, this can also take place by inferring information on the consumer based on consumers in similar data sets.

Analysis methods increasingly link different datasets and pieces of information from different sources in a way that was not possible before. This blurs the distinction between personal and other data, and makes non-personal data increasingly traceable to individuals, expanding the analytical possibilities of financial services providers (OECD, 2019[16]).

In the insurance sector, the segmentation of risks and the increased effectiveness of risk-selections can allow insurers to pre-determine which policyholders are likely to bring losses. On this basis, some consumers might be offered excellent rates, while others can be excluded from the provision of insurance services.

In the credit sector, the use of alternative data can have important consequences on credit scoring ratings. Traditional credit information, obtained from credit card usage and payments history, can be combined

with data points obtained from consumers' online and offline activities. Most of this data does not necessarily have a direct link to individuals' creditworthiness: where consumers shop, what they buy, their social media networks and the activities of their social contacts and/or of people in similar digital networks. Credit providers in the United States have reported a rise of 15% in the accuracy of predictions on consumers.[7]

Research conducted on the creditworthiness of online consumers of a German e-commerce company (Berg et al., 2018[17]) shows the superior discriminatory power of a model using both the credit bureau score and the digital footprint variables.[8] This suggests that a lender that uses information from both sources can make more profitable but also more exclusionary lending decisions.

However, recent research also identifies possible additional discriminatory effects deriving from the use of big data, such as exclusion by association, by which consumers are not evaluated according to their own individual characteristics but by predictions inferred from their social, familial or religious associations (Hurley and Adebayo, 2017[18]). Moreover, the ways in which non-traditional data are used and analysed, which might not be regulated in some jurisdictions, might not be transparent to consumers (and to regulators) as this is based on proprietary analytical tools. This might be done without the accuracy, use limitation, access and dispute protections applicable for example to credit bureaux. In these cases, consumers do not have the ability to challenge what might be an unfair decision, and cannot understand which steps to take to build a better credit score.

Box 5.3. Responsible stewardship of trustworthy Artificial Intelligence

In September 2018, the OECD set up a 50+ member expert group on AI to develop a set of principles, with representatives of 20 governments leaders from the business, labour, civil society, academic and scientific communities.

The rationale behind the creation of this group and of subsequent work is the recognition that AI has pervasive, far-reaching and global implications that are transforming societies and sectors of the economy. These developments have the potential to improve welfare and well-being, but may also have disparate effects in our societies and economies, notably regarding economic shifts, competition, transitions in the labour market, inequalities, and have consequences on the future of democracy and human rights, privacy and data protection, and digital security.

The efforts of OECD governments in this domain resulted in the approval in June 2019 of the OECD Council Recommendation on Artificial Intelligence (OECD, 2019[19]), which includes the OECD Principles on AI. OECD members plus Argentina, Brazil, Costa Rica, Peru and Romania are adherent to the AI Principles.

Two of the Principles are particularly relevant in the field of personal data and financial services:

Human-centred values and fairness

- AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.
- To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art.

Transparency and explainability

AI actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

- to foster a general understanding of AI systems,
- to make stakeholders aware of their interactions with AI systems, including in the workplace,
- to enable those affected by an AI system to understand the outcome, and,
- to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

The Recommendation also calls on governments to "work closely with stakeholders to prepare for the transformation of the world of work and of society. They should empower people to effectively use and interact with AI systems across the breadth of applications, including by equipping them with the necessary skills".

Source: OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Rising digital security risks

The digitalisation of our economies and of finance is enriching the wealth of data stored by financial institutions, and offering new ways of accessing them. Financial institutions, because of the potential value of the information stored in their IT systems, are a profitable target for cyber criminals (see Box 5.4). Data intensity (measured as the average volume of data stored per organisation) is highest in the financial services sector (including securities and investment services and banking) (OECD, 2015[5]).

In the United Kingdom alone, data breaches reported by financial services firms to the Financial Conduct Authority (FCA) increased by 480% in 2018, to 145 up from just 25 in 2017.[9]

Box 5.4. Digital security incidents in financial services

Digital security incidents affecting the integrity, availability and confidentiality of data stored by financial services providers have become more and more common, and are on the rise globally. Below is a non-exhaustive list of some of the major digital security incidents affecting financial services firm in recent years:

- In 2014, the data of 20 million individuals – 40% of the Korean population – were stolen from three Korean credit card companies[10] (KB Kookmin Bank, Lotte Card and Nonghyup Bank). Personal data included identification numbers, addresses and credit card numbers.
- In 2014, JP Morgan Chase, the largest retail bank in the United States, was the victim of a hack that compromised the data of more than half of all US households – 76 million – plus 7 million small businesses.[11] The data included contact information – names, addresses, phone numbers and email addresses – as well as internal information about the users.
- In 2016, Tesco Bank was victim of a cyber-attack affecting 8 261 out of 131 000 Tesco Bank personal current accounts.[12] Although Tesco Bank's controls stopped almost 80% of the unauthorised transactions, personal current account holders received text messages that were likely to cause consumers distress in the early hours of the morning. Some consumers suffered embarrassment and inconvenience when they were unable to make payments using their debit cards.
- In 2017, hackers stole the personal data of nearly 150 million people from the databases of Equifax, a consumer credit reporting agency.[13]

Consumers' attitudes towards privacy and data as a commodity

The response of consumers to these developments and to the opportunities and risks offered by big data is mixed: if on the one hand a majority of consumers are aware of threats to their privacy, on the other hand they are also willing to share additional personal information in exchange for better and cheaper services. However, recent research suggests that when consumers consent to share their data to providers they lack an understanding of terms and conditions, including the privacy statement.

Data privacy concerns and awareness of digital security risks[14]

Evidence suggests that consumers value their privacy and are aware of how this can be compromised in today's technological environment. They have concerns about how their personal data can be unlawfully accessed and used, and are aware of the risks posed by cybercrime (access to their accounts, misuse of their personal information).

Consumers are aware of the increasing risks to the integrity of their personal data and their privacy. A 2018 CIGI-Ipsos Global Survey on Internet Security and Trust[15] shows that over half of internet users surveyed globally were more concerned about their online privacy than they were the previous year. In a special 2014 Eurobarometer survey on digital security, online consumers in the European Union reported their top two concerns to be the misuse of personal data and the security of online payments (European Commission, 2015[20]). National surveys confirm these trends: in the United Kingdom, for example, 42% of those surveyed think it is likely that they will be a victim of cybercrime in the next two years (Ipsos MORI, 2019[21]).

Indeed concerns over data security (data leaks, hacking, etc.) are the second most important reason that would push a consumer to leave their current provider, according to a recent global study conducted by the private sector on the behaviour and preferences of financial services consumers (Accenture, 2019[22]).

Despite these concerns, not all consumers apply the necessary steps to safeguard their personal data online. In the United Kingdom, for example, almost half do not always use a strong, separate password for their main email account. In addition, only 15% say they know a great deal about how to protect themselves from harmful activity, with around 33% stating they rely to some extent on friends and family for help on cyber security (Ipsos MORI, 2019[21]).

Differences in risk perception and in response by target audience

For financial education policy makers, it is important to note that there are differences in perception of online security risks. A recent survey conducted in the United Kingdom (Ipsos MORI, 2019[21]) indicates that 37% of surveyed consumers agree with the statement "losing money or personal details over the internet is unavoidable these days". Those who strongly agree with the statement are more likely to be above 65 years old or have no formal qualifications.

Differences by target audiences are also worth noting with respect to the strategies adopted by consumers to minimise the likelihood of being victim of cybercrime. Indeed, if consumers are concerned about their privacy, not all of them take actions to protect it. Surveys conducted in the Unites States (Pingitore et al., 2017[23]) and the United Kingdom (Ipsos MORI, 2019[21]) indicate that younger consumers take more proactive actions to safeguard their online privacy, such as adjusting privacy settings on their mobile phones or social media.

Trading personal data for additional benefits

Evidence suggests that consumers are also willing to share additional personal data with financial providers if this results in perceived benefits. Two global surveys conducted by the private sector shed some light on this trend.

The first one addresses data sharing in general and is not focused just on financial services (GfK, 2017[24]). It finds that more than a quarter (27%) of internet users across 17 countries strongly agree that they are willing to share their personal data in exchange for benefits or rewards, such as lower costs or personalised services. The percentage of users who are firmly unwilling to share their data is around 19%. The survey also indicates that Internet users aged 30-40 are most likely to share data for rewards.

A second survey focuses in particular on the financial services sector (Accenture, 2019[22]). This indicates that around 60% of the consumers surveyed globally indicate that they would share more data with banks, insurers, or investment advisory firms if this translated into priority services, pricing benefits, more personalised products or non-regulated financial advice. This percentage increases among categories of consumers that are younger and more digitally keen. These consumers are open to begin making financial transactions through GAFAs (Google LLC, Apple, Inc., Facebook, Inc. and Amazon.com). For these consumers, and for the generations born after the 1990s in particular, GAFAs are also attractive alternatives to traditional financial services providers, with 40% of them that would consider banking with Facebook, Google or Amazon. This is even higher in markets such as the United States, where 50% would be willing to make this switch (Accenture, 2019[22]).

Consent is not informed

These shifts are taking place despite consumers not fully understanding the value of their personal data. Research conducted in the United Kingdom (Financial Services Consumer Panel, 2018[25]) to assess how willing consumers are to share their data with third parties in the framework of open banking confirms that consumer consent is not well informed. More than three quarters of consumers (even among those with higher socio-economic and educational background) state that they do not feel informed when they read terms and conditions. In addition, most consumers who give consent to the treatment of their personal data

by third-party providers do not understand some of the terms and conditions they have agreed to and hence indicate that their consent it not informed.

Finally, the degree to which they can exercise control over the use of their data is not clear to them – no more than their rights over their data. This point in particular is relevant for financial education and awareness policy makers, as recent landmark advances in the regulation of privacy and personal data use aim to give more control and more rights to consumers (see Box 5.5).

Box 5.5. The European Union General Data Protection Regulation (GDPR)

The GDPR became effective in May 2018 and aims to give more control to EU citizens over their personal data, and how these data are accessed, processed and used. The GDPR sets out seven key principles covering personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); accountability.

The GDPR also gives "data subjects", i.e. all natural persons whose personal data are processed by a controller or processor, specific (new) rights. The Regulation codifies the following fundamental data subject rights:

- The right of access.
- The right to rectification.
- The right to erasure or right to be forgotten.
- The right to restriction of processing.
- The right to data portability.
- The right to object.
- The right not to be subject to a decision based solely on automated processing, including profiling, when this bears legal effects or significantly affects him or her.

Financial education and awareness

Public policies dealing with the personal data of financial services consumers have so far focused mostly on data protection and financial consumer protection regulation. National strategies for financial education, apart some notable exceptions (see Box 5.6), have yet to systematically include this element within the content of their programmes.

The development of new core competencies relating to personal data is made even more relevant as recent changes to privacy regulations in some jurisdictions seek to empower consumers and give them specific rights over their data (see Box 5.5). Consumers should possess the necessary knowledge and skills to understand the use that is made of their personal data and to fully exercise their consumer rights in this domain.

Box 5.6. Digital financial literacy initiatives among OECD/INFE members

Members of the OECD/INFE have begun to include financial education and awareness on the importance of personal data within their national strategies and initiatives.

Germany

In Germany, the Federal Ministry of Justice and Consumer Protection (BMJV), as the competent authority for consumer policy relating to amongst other things the Information society and financial services, published a comprehensive article on the consumers' rights to their data. The article includes a section on the protection of personality by data protection, a section on how an individual consumer can get information on the data collected already about him or her as well as guidance on how to avoid providing unnecessary data and on how to safely use the internet. There is a free download available with information tailored to elderly consumers.[16]

The German Federal Financial Supervisory Authority (BaFin) provides consumers with practical guidance on the use of their personal data when using financial services. In 2019, BaFin gave an online seminar for elderly people on the Second Payment Services Directive (PSD2)[17] explaining the impact of the directive on electronic payment and online Banking and on alternative payment solutions. There was a special focus on data protection issues.

Portugal

Digital financial literacy is among the key goals of the Central Bank of Portugal's Strategic Plan for 2017-2020. This strategic goal addresses in particular the safe use of digital channels. The adoption of safety procedures by consumers is encouraged through awareness campaigns on the Bank Customer website (https://clientebancario.bportugal.pt). The website also features a dedicated page, with contents on digital security such as risks associated with digital channels, and the explanation of what Big Data is, as well as its benefits and risks. This information is accessible to consumers through plain language and an intuitive interface, supported by audio-visual tools.

In 2018, the Central Bank of Portugal launched a digital financial education campaign addressed at young people (#toptip), to raise awareness amongst digital natives on the necessary precautions to be adopted when using digital financial services. The first tip "When using the internet, do you have any idea of the risks?" gives hints on how users should protect their equipment and internet connection from risks such as phishing, pharming, spyware and SIM card swap. The second tip "Do you use your smartphone to access social networks or email? Or home banking? Do you also make payments with your mobile phone?" focuses on the importance of protecting the large amount of confidential and private information that users have on their mobile phones. The third tip "Is social media your second home?" warns about the risk of sharing personal data in social media. The fourth tip "Do you safely buy online?" clarifies the steps that users should follow before, during and after an online purchase. The fifth tip "What if you are a victim of online fraud?" helps users who have been (or suspect they were) victims of online fraud. The campaign was also delivered through the Instagram account of the Central Bank (@bancodeportugalofficial). The Central Bank sent a brochure with these tips was to all secondary schools and regularly conducts financial education sessions in secondary schools which are in high demand.

Spain

Digital financial literacy is among the key goals of the National Financial Education Plan implemented by the Central Bank of Spain and the Spanish Financial Market Authority (CNMV) for 2018-2021. Digitalisation of financial products and services and the consequent need to strengthen digital financial

literacy are seen as key areas of action. The Financial Education Plan is in particular aware of the opportunities and challenges presented by the digital delivery of financial education and an effort will be made in the identification and promotion of financial education initiatives in this area. Digital tools, applications and software will be used to improve access to financial education, strengthen the key competences of financial services users and increase skills in the field of management and control of their finances.

With respect to personal data, the Spanish National Strategy website, *Finanzas para Todos* (www.finanzasparatodos.es), includes an entire section related to protecting personal information, with answers to questions such as: "What personal information should I protect?", "What should I do if I receive an email asking me to confirm my personal information?", "What is spyware?" and "What precautions should I take with online banking?".

Similarly, a section on safeguarding personal information is included in the Financial Education Programme for Schools, for students 14–18, and addresses the same questions mentioned above. This programme also includes practical classroom activities with the following learning objectives:

1. Understand the importance of safeguarding our personal information to avoid falling victim to financial fraud;
2. Identify the necessary precautions to take with online banking and other Internet activities;
3. Know the importance of reporting the theft or loss of documents and keeping a written record of the report; and
4. Know the precautions to take for online banking and other Internet activities.

The G20/OECD INFE Policy Guidance action checklist: Focus on personal data

In light of the need to address the use of personal data within financial education programmes, and to encourage positive behaviours on personal data awareness and management, this chapter suggests specific elements pertaining to personal data in support of the implementation of the G20/OECD INFE Policy Guidance Note on Digitalisation and Financial Literacy (OECD, 2018[1]).

These new elements should be considered as an additional implementation tool for policy makers and programme designers addressing financial education and personal data, and should be read taking into account the regulatory framework and the financial and digital literacy levels in each jurisdiction.

Table 5.2. New elements pertaining to personal data in selected building blocks of the G20/OECD INFE Policy Guidance Note

Selected building blocks of the G20/OECD INFE Policy Guidance Note	Specific elements pertaining to personal data
1.Develop a national diagnosis	*Supply side* Scan the current landscape to understand: • How financial services providers use consumers' personal data, in the framework of the applicable national legislation • The presence of specific actionable rights over personal data in financial services, as per financial consumer protection or data protection legislation *Demand side* Draw on existing data and analysis, or commission research to understand: • Attitudes towards privacy and personal data use • Consumers' understanding of digital footprint • Online security awareness and behaviours • Appetite for data sharing • Awareness of actionable rights over personal data in financial services, as per financial consumer protection or data protection legislation
2.Ensure coordination	Among public authorities: • Coordinate with, or at a minimum consult, the national data protection authority, if existing, or the public authorities with a legal mandate and effective means in the field of privacy and data regulation.[18] With the private and not-for-profit sector: • Public authorities should seek to harness the knowledge of the private sector, and in particular of FinTech actors, to understand new developments in the field of personal data sharing.
3.Support the development of a national core competency framework on digital financial literacy *3.a Empowering consumers, including the most vulnerable, to counter new types of exclusion due to the misuse of various data sources, including big data, and digital profiling*	
• Appropriately manage their digital footprint to the extent possible:	• Consumers should be aware of the analytical possibilities offered by big data, and that any online activity can be used by financial services providers to customise offers and define cost and range of product offer. • In countries with positive credit scoring systems in particular, consumers should understand that credit scoring decisions can be influenced by personal information that is not related to their personal credit history.
• Avoid engaging in risky behaviours involving their personal data, and understand the consequences of sharing or disclosing personal identification numbers, account information, or other identifying information such as address, birth date or government-issued numbers whether digitally or through other channels:	• Target groups that display the lowest familiarity with online transactions and lowest levels of digital literacy should be prompted regularly to take effective measures to safeguard their personal data and privacy.

• Assess the kind of information that is requested by (financial) services providers to decide whether it is relevant and understand how it may be stored and used.	• Target groups that are willing to share more personal information with financial services providers in exchange for benefits, notably younger generations and the more technologically savvy, should be aware of the consequences to their privacy and should share non-essential additional information based on informed consent.
• Increase awareness of consumer rights with respect to personal data, and on the applicable regulatory framework, especially if this gives consumers new rights and discretionary control over their personal data.	• In jurisdictions where changes to personal data regulations have assigned new rights to consumers, they should be informed through awareness campaigns. • Inform consumers of the mechanisms behind the decisions made on their financial lives, in particular when these have been taken without human intervention. • When consumers have the legal right to challenge a decision taken by an algorithm, they should be informed and know how to seek recourse.
3.b Protecting consumers and small businesses from increased vulnerability to digital crimes such as phishing scams, account hacking and data theft	
• Increase awareness of the existence of online fraud. The existence of online fraud and of cyber security risks when choosing and using digital financial services, making financial transactions online, and using account aggregation tools ("screen scraping").	• Consumers - and the most vulnerable target groups in particular - should be alerted to the need of using strong passwords to protect their personal data and financial transactions online and informed about what to do in case of a security breach.
• Increase awareness of the possibilities offered by account aggregation tools, and how to use and stop using such tools safely given that they are providing access to their account information to third parties.	• Consumers understand data sharing revocation terms and when to revoke authorizations to access, use, or store data. • Consumers understand that through screen-scraping, the passwords and login information remains with the third-party provider also when they stop using the service, increasing the likelihood of the password being stolen or misused.

Conclusions

In today's economies, the capacity of financial services providers to capture, store, combine, and analyse a wide variety of consumer data, such as their financial situation, habits or physical location, has prompted an adaptation of data protection and financial consumer protection frameworks. While this is necessary, public policies should also aim to reinforce awareness among consumers of the implications of the use of their personal data, and foster behaviours that can protect their personal data while helping them to take a proactive stance to data sharing that is consistent with their own preferences. Such a consumer-centric approach also responds to an evolving regulatory context in which individuals are assigned new rights covering their personal data.

The analysis conducted in this chapter presents the implications of the use of personal data in financial services from a consumer perspective. It covers both the possible advantages and risks, drawing on existing data to describe consumer attitudes to personal data sharing.

Based on this analysis, financial education policy makers are encouraged to take into account issues related to personal data when gathering evidence to inform their policies and programmes. This would ideally cover both the supply side, i.e. the use that is made of personal data by financial services providers and the applicable regulatory framework, and the demand side, i.e. consumer attitudes to data sharing and their understanding of the value and implications of their personal data.

Authorities in charge of financial education in each jurisdiction are invited to coordinate or consult with the authorities in charge of personal data protection and financial consumer protection, to ensure that financial education policies and initiatives benefit from their expertise and are coherent with existing national frameworks on personal data protection. Similar coordination or consultation should also take place with Fintech providers, in order to fully understand new developments in personal data sharing.

Finally, the chapter identifies specific financial literacy competencies that would benefit individuals and entrepreneurs in this domain, providing new elements pertaining to personal data in support of the implementation of the G20/OECD INFE Policy Guidance Note on Digitalisation and Financial Literacy. These additions are for consideration by policy makers, and should be read taking into account the financial consumer protection and personal data protection frameworks in each jurisdiction.

The OECD, through its International Network on Financial Education (INFE), and through its horizontal project on digitalisation, will continue to monitor policy solutions implemented at the national level, and to engage in a fruitful discussion at the international level to identify good practices. Thanks to its global nature, the OECD/INFE will also foster the necessary cross-border approach to personal data policies.

References

Accenture (2019), *Accenture Global Financial Services Consumer Study*, https://www.accenture.com/_acnmedia/PDF-95/Accenture-2019-Global-Financial-Services-Consumer-Study.pdf. [22]

Accenture (2017), *Accenture Financial Services 2017 Global Distribution & Marketing Consumer study: financial services report*, http://www.accenture.com/t20170111T041601__w__/us-en/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Financial-Services-Global-Distribution-Marketing-Consumer-Study.pdf. [31]

Berg, T. et al. (2018), *On the Rise of FinTechs – Credit Scoring using Digital Footprints*, https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf. [17]

Cormen, T. et al. (2009), *Introduction to Algorithms*, MIT Press. [29]

EU Financial Services Users Group (2016), *Assessment of current and future impact of Big Data on Financial Services*, https://ec.europa.eu/info/sites/info/files/file_import/1606-big-data-on-financial-services_en_0.pdf. [26]

European Commission (2015), *Special Eurobarometer 423 Cyber Security - Report*, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf. [20]

European Union (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504. [6]

European Union (2015), *Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366. [15]

Financial Services Consumer Panel (2018), *Consenting adults? - consumers sharing their financial data*, https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf. [25]

G20 (2011), *G20 High-level Principles on Financial Consumer Protection*, http://www.oecd.org/daf/fin/financial-markets/48892010.pdf. [3]

GfK (2017), *Willingness to share personal data in exchange for benefits or rewards - Global GfK survey*, https://www.gfk.com/fileadmin/user_upload/country_one_pager/NL/images/Global-GfK_onderzoek_-_delen_van_persoonlijke_data.pdf. [24]

GSMA (2018), *The Mobile Economy 2018*, https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf. [8]

Hurley, M. and J. Adebayo (2017), "Credit scoring in the era of Big Data", *Yale Journal of Law & Technology*, Vol. 18/1, https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5. [18]

Ipsos MORI (2019), *UK Cyber Survey Key findings – General public, conducted on behalf on behalf of the National Cyber Security Centre and Department for Digital, Culture, Media and Sport (DCMS)*, https://s3.eu-west-1.amazonaws.com/ncsc-content/files/UK%20Cyber%20Survey%20-%20analysis.pdf. [21]

Joint Committee of the European Supervisory Authorities (2016), *Discussion Paper on the Use of Big Data by Financial Institutions*, https://esas-joint-committee.europa.eu/Publications/Discussion%20Paper/jc-2016-86_discussion_paper_big_data.pdf. [32]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://dx.doi.org/10.1787/eedfee77-en. [16]

OECD (2019), "Good practice guide on consumer data", *OECD Digital Economy Papers*, No. 290, OECD Publishing, Paris, https://dx.doi.org/10.1787/e0040128-en. [4]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [19]

OECD (2018), "Consumer policy and the smart home", *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, https://dx.doi.org/10.1787/e124c34a-en. [10]

OECD (2018), *G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy*, http://www.oecd.org/finance/G20-OECD-INFE-Policy-Guidance-Digitalisation-Financial-Literacy-2018.pdf. [1]

OECD (2018), *G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age*, https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf. [33]

OECD (2018), "IoT measurement and applications", *OECD Digital Economy Papers*, No. 271, OECD Publishing, Paris, https://dx.doi.org/10.1787/35209dbf-en. [9]

OECD (2018), *Toolkit for Protecting Digital Consumers: A resource for G20 policy makers*, https://www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf. [27]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264276284-en. [7]

OECD (2017), *Robo-Advice for Pensions*, https://www.oecd.org/finance/Robo-Advice-for-Pensions-2017.pdf. [14]

OECD (2017), *Technology and innovation in the insurance sector*, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf. [13]

OECD (2016), *G20/OECD INFE Core competencies framework on financial literacy for adults*, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Adults.pdf. [28]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264255258-en. [36]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [5]

OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264245471-en. [35]

OECD (2015), *OECD/INFE Core competencies framework on financial literacy for youth*, http://www.oecd.org/daf/fin/financial-education/Core-Competencies-Framework-Youth.pdf. [12]

OECD (2014), "Consumer Policy Guidance on Mobile and Online Payments", *OECD Digital Economy Papers*, No. 236, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jz432cl1ns7-en. [34]

OECD (2013), *The OECD Privacy Framework*, http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf. [2]

Pingitore, G. et al. (2017), *To share or not to share*, Deloitte University Press, https://www2.deloitte.com/content/dam/insights/us/articles/4020_To-share-or-not-to-share/DUP_To-share-or-not-to-share.pdf. [23]

Reserve Bank of India (2016), *Master Direction- Non-Banking Financial Company - Account Aggregator*, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598. [30]

Rosner, G. and E. Kenneally (2018), *Clearly Opaque: Privacy Risks of the Internet of Things*, https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54. [11]

Annex 5.A. List of members of the OECD/INFE Working Group on Digital Financial Literacy

Country	Name
Austria	Martin Taborsky, Central Bank of Austria (Co-leader)
Netherlands	Olaf Simonse, Ministry of Finance (Co-leader)
Australia	Laura Higgins, Australian Securities and Investments Commission
Austria	Elisabeth Ulbrich, Central Bank of Austria
Brazil	João Evangelista de Sousa Filho, Banco do Brasil
Brazil	José Alexandre Cavalcanti Vasco, CVM
Brunei Darussalam	Rina Hayane Sumardi, Autoriti Monetari Brunei Darussalam
Canada	Chris Poole, Financial Consumer Agency of Canada
Chile	Carolina del Río, Financial Markets Commission (formerly SBIF)
Czech Republic	Alex Ivanco, Ministry of Finance
France	Astrid Delacour, Banque de France
India	Gautam Prasad Borah, Reserve Bank of India
India	Girraj Prasad Garg, NISM
Indonesia	Rela Ginting, OJK
Italy	Roberta Nanula, Banca d'Italia
Italy	Nadia Linciano, CONSOB
Korea	Jin Yong Kim, Bank of Korea
Latvia	Dace Jansone, Financial and Capital Market Commission
Luxembourg	Danièle Berna-Ost, Commission de Surveillance du Secteur Financier
Malaysia	Jeremy Lee Eng Huat, Bank Negara Malaysia
Mexico	Pedro Garza López, Banco de México
Mongolia	Myendu Nurgul, Central Bank of Mongolia
Morocco	Imane Benzarouel, Fondation Marocaine pour l'Education Financière
New Zealand	Celestyna Galicki, Commission for Financial Capability
Pakistan	Syed Samir Hasnain, State Bank of Pakistan
Peru	Juan-Carlos Chong, Superintendency of Banking, Insurance and Private Pension Funds
Portugal	Lucía Leitão, Central Bank of Portugal
Portugal	Lucélia Fernandes, Portuguese Insurance and Pension Funds Supervisory Authority
Republic of North Macedonia	Kristina Pavleska, Coordinating Body of the Regulatory Authorities for Financial Education in Macedonia
Romania	Anton Comanescu, National Bank of Romania
Singapore	Abigail Ng, Monetary Authority of Singapore
South Africa	Lyndwill Clarke, Financial Sector Conduct Authority
Spain	Emilio Ruiz, Banco d'España
Sweden	Thèrese Wieselqvist Ekman, Financinspektionen
Turkey	Nihal Degirmenci, Central Bank of the Republic of Turkey

Notes

[1] Other relevant OECD instruments in this field are the OECD Consumer Policy Guidance on Mobile and Online Payments (OECD, 2014[34]), the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (OECD, 2015[35]), the OECD Recommendation on Consumer Protection in E-Commerce (OECD, 2016[36]). These principles, together with relevant practice, have informed the OECD G20 Toolkit for Protecting Digital Consumers (OECD, 2018[27]).

[2] See also the G20/OECD INFE Core competencies framework on financial literacy for adults (OECD, 2016[28]) and for Youth (OECD, 2015[12]).

[3] An algorithm can be described as "any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as an output. An algorithm is thus a sequence of computational steps that transforms the input into the output" (Cormen et al., 2009[29]).

[4] For more information on technological and policy developments linked to blockchain, see: www.oecd.org/finance/blockchain/.

[5] See for example the regulatory framework introduced by the Reserve Bank of India for Account Aggregators in September 2016 (Reserve Bank of India, 2016[30]) that, inter alia, includes provisions for consumers' explicit consent, and the guarantee of the protection of consumers' rights, data security and consumer grievance redressal mechanism.

[6] For a discussion of privacy and security risks incurred by consumers in the digital environment, see also the Consumer Policy Guidance on Mobile and Online Payments (OECD, 2014[34]).

[7] "Equifax and SAS leverage AI and deep learning to improve consumer access to credit", Forbes, 20 February, https://www.forbes.com/sites/gilpress/2017/02/20/equifaxand-sas-leverage-ai-and-deep-learning-to-improve-consumer-access-tocredit/2/#2ea15ddd7f69.

[8] The variables taken into account by the study focus only on the interactions with that company, and are: the device type (tablet or mobile); the operating system (iOS or Android); the channel through which a consumer comes to the website (such as search engine or price comparison website); a do not track dummy equal to one if a consumer uses settings that do not allow tracking device, operating system and channel information; the time of day of the purchase (for example, morning, afternoon, evening, or night); the email service provider (for example, Gmail or yahoo); two pieces of information about the email address chosen by the user (includes first and/or last name and includes a number); a lower case dummy if a user consistently uses lower case when writing; and a dummy for a typing error when entering the email address.

[9] https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/

[10] www.economist.com/finance-and-economics/2014/01/25/card-sharps

[11] https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

[12] www.fca.org.uk/publication/final-notices/tesco-personal-finance-plc-2018.pdf

[13] www.gao.gov/assets/700/694158.pdf

[14] For additional information on digital security and privacy, see www.oecd.org/going-digital/topics/digital-security-and-privacy/.

[15] https://www.cigionline.org/internet-survey-2018

[16] Available in German at: www.bmjv.de/DE/Verbraucherportal/DigitalesTelekommunikation/Datenschutz/Datenschutz_node.html

[17] The presentation held in the online seminar can be downloaded at www.bafin.de/SharedDocs/Downloads/DE/Veranstaltung/dl_191017_digitaler_stammtisch_digitalisierung.html.

[18] For a global list of national data protection authorities, see: https://www.dlapiperdataprotection.com/index.html?t=authority&c=AR&c2=

Financial Markets, Insurance and Pensions: Digital technologies and Finance

This publication compiles a series of articles that focus on the impact of digitalisation and technology in the areas of financial markets, insurance, and private pensions. It also discusses the tools and policies needed to ensure that the challenges posed by digitalisation result in better outcomes and better management of the risks involved.

www.oecd.org/finance

This report contributes to the OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.