DISCUSSION PAPER ON BLOCKCHAIN AND SMART CONTRACTS IN INSURANCE

European Insurance and Occupational Pensions Authority

#INSURANCE #PENSIONS #SOLVENCYII

https://www.eiopa.europa.eu

PDF ISBN 978-92-9473-295-8 doi:10.2854/136043 EI-01-21-124-EN-N

Luxembourg: Publications Office of the European Union, 2021

© EIOPA, 2021
Reproduction is authorised provided the source is acknowledged.

Images copyright:
First page: AdobeStock

For any use or reproduction of photos or other material that is not under the EIOPA copyright, permission must be sought directly from the copyright holders.

DISCUSSION PAPER ON BLOCKCHAIN AND SMART CONTRACTS IN INSURANCE

CONTENTS

TABLE OF FIGURES AND BOXES 3

RESPONDING TO THIS DISCUSSION PAPER 4

EXECUTIVE SUMMARY 5

1. INTRODUCTION 7

2. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS 9

3. BLOCKCHAIN AND SMART CONTRACTS USE CASES IN THE EU INSURANCE MARKET 12

4. CRYPTO ASSETS USE CASES IN INSURANCE 16

5. BLOCKCHAIN AND SUPTECH 19

6. RISKS AND BENEFITS OF BLOCKCHAIN AND SMART CONTRACTS 21

7. REGULATORY BARRIERS IN RESPECT OF BLOCKCHAIN AND SMART CONTRACTS 27

8. EUROPEAN APPROACH TO BLOCKCHAIN AND SMART CONTRACTS IN INSURANCE 29

ANNEX 1. CONSULTATION QUESTIONS 31

ANNEX 2. ABBREVIATIONS 32

ENDNOTES 33

TABLE OF FIGURES AND BOXES

Figure 1. How blockchain works? 10

Figure 2. Simplified smart contract coding example 11

Box 1. Overview of decentralised P2P insurance and parametric insurance business model 12

Box 2. Examples of blockchain and smart contract use cases in insurance reported by the NCAs 14

Box 3. EU legislative proposal on markets in crypto assets (MiCA) 16

Box 4. Initial Coin Offerings and tokenisation of assets 17

Box 5. How stablecoins could impact the insurance sector 18

Box 6. The FMA evaluation of blockchain use for supervision 19

Box 7. Innovation facilitators focusing on blockchain 28

RESPONDING TO THIS DISCUSSION PAPER

EIOPA welcomes comments on the 'Discussion Paper on blockchain and smart contracts in insurance'.

Comments are most helpful if they:

- respond to the question stated, where applicable;
- contain a clear rationale; and
- describe any alternatives EIOPA should consider.

Please send your comments to EIOPA **by 29 July 2021** responding to the questions in the survey provided at the following link:

https://ec.europa.eu/eusurvey/runner/EIOPA_Blockchain_insurance_survey

Contributions not provided using the survey or submitted after the deadline will not be processed and therefore considered as they were not submitted.

PUBLICATION OF RESPONSES

Contributions received will be published on EIOPA's public website unless you request otherwise in the respective field in the EU Survey Tool.

Standard confidentiality statements in an email message will not be treated as a request for non-disclosure.

Please note that EIOPA is subject to Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents and EIOPA's rules on public access to documents.

Contributions will be made available at the end of the public consultation period.

DATA PROTECTION

Please note that your personal contact details (such as names, email addresses and phone numbers) will not be published. They will only be used to request clarifications, if necessary, on the information you supplied.

EIOPA will process any personal data in accordance with Regulation (EU) 2018/1725 on the protection of national persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. More information on how EIOPA will treat your personal data can be found in the privacy statement.

https://www.eiopa.europa.eu/content/privacy-statement_en

EXECUTIVE SUMMARY

Blockchain and other distributed ledger technologies (DLTs), when properly used, have the potential to transform the functioning of a wide range of industries, including the insurance industry in Europe. Potential impacts are currently being explored across sectors and by a variety of organisations. For example, the European Commission recently published a proposal for a regulation on markets in crypto-assets[1] (MiCA), and a proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology[2] with the aim to provide a framework to allow for innovation in a way that preserves financial stability and protects consumers.

It is still early days for blockchain in European (re-)insurance sector. However, blockchain can be potentially used throughout the entire insurance value chain. It has the potential to deliver key digital opportunities, reduce duplication of processes, increase process automation, help cut costs, increase efficiency, enhance customer experiences, and improve data quality, collection and analytics. It could also enable the development of new products and services, facilitating the uptake of insurance platforms and ecosystems, improving the interaction with third parties, promoting completely decentralised peer-to-peer (P2P) insurance business models or implementing parametric insurance products.

Blockchain could also provide opportunities for both prudential and conduct supervisors (SupTech) as well as facilitate RegTech solutions. The combination of smart contracts and blockchain could help to automate regulatory reporting and make it more efficient and transparent, improve consistency and data quality across firms, and allow regulators to get data on new areas of interest or to gain real-time access to signed contracts and the information they contain (real-time regulatory monitoring).

While promising to drive efficiency in business practices and mitigate certain existing risks, the adoption of blockchain may also trigger new risks to insurance undertakings, supervisors, and consumers. As blockchain technology is still evolving, several challenges are emerging, such as the complexity of the technology, data protection and privacy, cyber risk, integration with legacy infrastructures, or interoperability and standardisation between different blockchains. Based on blockchain types and platforms chosen, performance scalability challenges could arise as well. Concerns about the legal status of smart contracts also have been aired.

Although the current regulatory and supervisory framework can be considered mostly effective to address emerging risks, specific issues should be considered, based on the evolution of the technology and its uses in business processes. It is also important to ensure appropriate understanding by insurance undertakings and supervisors as well as proportionate governance policies and processes, to guarantee that all relevant risks are identified and properly managed.

Given its wide range of applications and the early stage of adoption in the insurance industry, most jurisdictions are still exploring policy and supervisory responses. This can cause legal uncertainty and act as barrier to the use of blockchain and smart contracts

in insurance and could also lead to divergent regulatory and supervisory practices and different levels of consumer protection across the EU.

Hence a general European harmonised approach to blockchain could promote and facilitate the sound scaling of blockchain and smart contracts, including in the insurance context. This is particularly relevant to promote coherence with overall consumer protection, financial stability and prudential regulation objectives, and to ultimately promote a more integrated and efficient European insurance market.

EIOPA would like to gather from interested parties their views on this Discussion Paper. Specific questions are asked at the end of each chapter.

EIOPA will assess the feedback to this Discussion Paper in order to better understand blockchain developments in the insurance sector as well as the risks and benefits related to them. This could also help to provide informed input for the upcoming legislative initiatives foreseen in the European Commission Digital Finance Strategy[3]. It could also supplement EIOPA's overall work on digitalisation, including in areas such as (re)insurance value chain and new business models arising from digitalisation, insurance platforms and ecosystems, open insurance, digital ethics and RegTech/SupTech.

1. INTRODUCTION

1.1. BACKGROUND AND RATIONALE

Blockchain[4], when properly used, has the potential to transform the functioning of a wide range of industries and can provide significant benefits to the European industry, economy, and to European society as a whole. Those potential changes in the economy and society are currently being explored across sectors and by a variety of organisations, including by the European Commission, which is exploring the role of blockchain across policy, funding, legal and regulatory fronts.[5] More concretely, recently published Digital Finance Strategy[6] (DFS) states that by 2024, the EU should put in place a comprehensive framework enabling the uptake of distributed ledger technology (DLT) and crypto-assets in the financial sector. Together with the DFS, the Commission also published a proposal for a regulation on markets in crypto-assets[7] (MiCA) and a proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology[8], with the aim to provide a framework to allow for innovation in a way that preserves financial stability and protects consumers.

While it is still early days for blockchain in the European (re-)insurance sector, the number of potential use cases is constantly growing and can influence a number of insurance functions, such as IT, operations, product design and development, pricing and underwriting, distribution and claims management.

Blockchain is being applied to raise efficiency, reduce costs, develop new products, and lessen the need for intermediation and increase transparency.[9] Blockchain and smart contracts, often combined with other emerging technologies such as Internet of Things (IoT) and Artificial Intelligence (AI), can be used for managing claims in a responsive and transparent way, for Know-Your-Customer (KYC) assessment and accurate risk evaluation, lowering administration and underwriting costs and supporting more accurate pricing. Automated claims submission and processing could improve claims assessment, fraud detection, and ensure more timely payments.[10]

However, while promising to drive efficiency in business practices and mitigate certain existing risks, the adoption of blockchain may trigger new risks to insurance undertakings, supervisors and consumers. As blockchain technology is still evolving, several challenges are coming to attention, such as performance and scalability, energy consumption, data privacy and protection, cyber risk, integration with legacy infrastructures, or interoperability between different blockchains. Based on blockchain types and platform chosen, performance scalability challenges could arise as well. Concerns about the legal status of smart contracts could also arise.

As a response to EIOPA´s June 2020 consultation on (re) insurance value chain and new business models arising from digitalisation[11], some stakeholders highlighted blockchain and related business models such as the emergence of decentralised 'self-insurance' or P2P insurance as further areas to look at from a supervisory perspective.

Although the current regulatory and supervisory framework addresses risks in a comprehensive way, specific issues could still be considered, based on the technology evolution and its use in business processes. It is important to ensure appropriate understanding by insurance undertakings and supervisors as well as proportionate governance policies and processes, to guarantee that all relevant risks are identified and properly managed.[12]

EIOPA has conducted a survey of National Competent Authorities (NCAs) on blockchain and smart contracts in insurance in Q2 2020.

The aim of this Discussion Paper is to provide a high-level overview of risks and benefits of blockchain and smart contracts in insurance from supervisory perspective, as well as to give an overview of the findings of the feedback received from NCAs through the aforementioned survey.

This Paper also assesses some issues related to crypto assets. EIOPA has monitored and will continue monitoring developments in the area of crypto-assets under a separate work stream.

1.2. LEGAL BASE

Article 1(6) of the Regulation establishing the EIOPA (Regulation (EU) No 1094/2010)[13] requires the EIOPA to contribute to promoting a sound, effective and consistent level of regulation and supervision, ensuring the integrity, transparency, efficiency and orderly functioning of financial markets, preventing regulatory arbitrage and promoting equal competition. In addition, Article 9(2) requires the EIOPA to monitor new and existing financial activities.

2. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS

2.1. BLOCKCHAIN AND DLT DEFINITION AND DIFFERENT TYPES OF BLOCKCHAIN

This chapter aims to summarise the key aspects raised in the recent literature on the blockchain features and its application in finance[14], while not going into technical details, which are already sufficently covered in other fora.

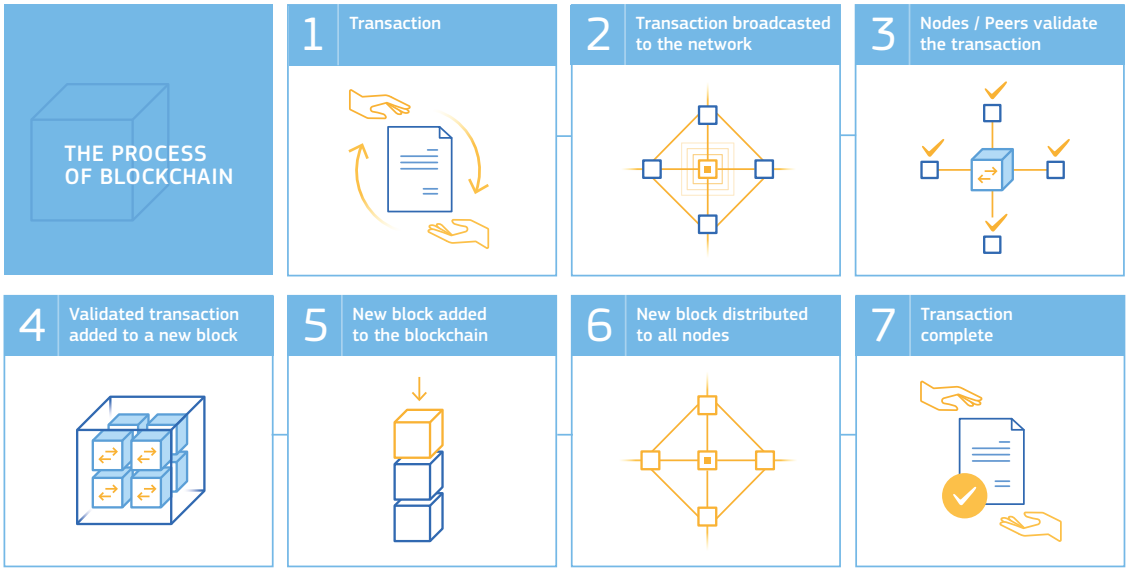
Distributed ledger technology (DLT) enables parties with no particular trust in each other to exchange any type of digital data on a peer-to-peer (P2P) basis with fewer or no third parties or intermediaries.[15] In this way it takes at least in part the place of traditional intermediaries or trusted third parties. Data exchanged could correspond to any transactions or assets that can be translated into digital form, including money transfers or storage, medical records, birth, marriage and insurance certificates, buying and selling goods and services, and insurance contracts.

Blockchain is a subset of DLTs, using 'blocks' of information to keep track of data transactions in a distributed network of multiple nodes or computers. A transaction with party B is requested by party A, such as transferring money, setting up a contract, or sharing records. This transaction is broadcasted to a distributed network of 'nodes' or computers which will validate it according to an agreed set of rules called 'consensus' mechanism. When the transaction is validated, a new 'block' will be added to the blockchain.[16] When a new block is added to the blockchain, it is timestamped, a pointer to the previous block in the chain is provided, and the transaction data entered. After that it is processed by the cryptographic technique of hashing where a hash is calculated on the hash of the previous block plus the data contents of the new block. The result then becomes the hash of the new block.[17]

This process ensures that each block is linked to the previous one, thereby forming a chain of blocks (hence the name 'blockchain'). The unique record that forms a blockchain is shared by each node or computer in the network and is constantly updated and synchronised. As a database or ledger, blockchain ultimately stores the records of all transactions executed across the network. A blockchain is essentially a continuously growing list of records and blockchain technology is thus well-suited for use-cases like recording events, managing records, processing transactions, and tracing assets.[18]

This Discussion Paper will mainly use the term blockchain and will refer to DLT where necessary.

Figure 1. How blockchain works?



Source: Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies, Publications Office of the European Union, Luxembourg, 2019

There are a large variety of blockchains. Based on their technical and functional configuration and internal governance structures, blockchains are often divided into four categories: public permissionless, public permissioned, private permissioned and private permissionless.[19]

A blockchain is called 'public' or 'open' when anyone can read and access the whole blockchain and, unless they are encrypted, read its contents. When only authorised entities have access, a blockchain is called 'closed' or 'private'. Blockchains can be further categorised as 'permissionless' or 'permissioned' depending on who can send and validate transactions. If anyone can send and validate transactions, the blockchain is called permissionless. If only authorised entities can execute or validate transactions, the blockchain is called permissioned. There can be also hybrid blockchains combining different aspects mentioned above.

2.2. SMART CONTRACTS AND ORACLES

From an insurance perspective, one important element for using blockchain in practice is smart contracts. Smart contracts are deterministic[20] computer programs that are deployed and executed on a blockchain and that are capable of carrying out the terms of an agreement between parties without the need for human coordination or intervention.[21] These agreements can be recorded and validated into a blockchain which can then automatically execute and enforce the contract, usually under 'if-then-else' instructions: 'if' something happens (for example, if your flight is delayed) 'then' certain transactions or actions are carried out (the payment for flight delay insurance is automatically transferred).

Figure 2. Simplified smart contract coding example

Source: EIOPA

The way in which transactions are verified and added to the blockchain guarantees that conflicts or inaccuracies are reconciled, and that in the end there is only one valid representation for each transaction (no double entries). Thus, it can be seen as an efficient way to automate some of the conditions and obligations described in the legal contract (e.g. insurance contract).[22]

In order to determine whether the conditions for the performance of a smart contract have been met, secure data (input) from outside the ledger will often be required. This data is provided by so-called 'oracles'. An oracle or data feed provider is typically a third-party service designed for use in smart contracts on a distributed ledger. Oracles find and verify real-world occurrences usually through external database and submit this information to a blockchain to be used by smart contracts (e.g. flight delay database or weather database). The key is for the parties in the smart contract to agree on the identity of the oracle. The challenge could arise when oracles are (third-party) services and are not part of the blockchain. The parties need to trust these sources of information and the sources must be secure from hacking. Trusted and secure information sources are crucial for the users of smart contracts. If the oracle alters the information taken from other sources or provides defective data, there may be no rewind or reset (immutability).[23]

Smart contracts are currently only feasible or applicable under limited and strictly circumscribed conditions – for instance, when there is no need for physical appraisals (e.g. for certain types of insurance claims[24]), no need for dispute resolution (although blockchain in itself could potentially be used for setting up a dispute resolution platform), or when there is a reliable oracle providing accurate information.

3. BLOCKCHAIN AND SMART CONTRACTS USE CASES IN THE EU INSURANCE MARKET

Blockchain and smart contracts, often combined with other emerging technologies such as IoT and AI, can be theoretically used throughout the entire insurance value chain.

From a **client on-boarding** perspective, by using a blockchain-enabled shared database, insurers could streamline and reduce the cost of their KYC/AML compliance. On-boarding of a customer needs to be done only once by one insurer/intermediary. When the customer wishes to engage a new insurer/intermediary, the latter can request access to documentation already on-chain in order to confirm due diligence. Encryption ensures that an institution has access only to the documents to which it is entitled, even as any change in the customer's file is transparent, both as to when the change was made and by whom. Transaction audits and surveillance can also be automated to a large extent.[25]

The use of blockchain in the **underwriting** process could result in improvements in efficiency and cost reduction as a result of the inherent trust and transparency within blockchain, particularly when combined with automated processes collating and assimilating information (e.g. external data can be included to decrease risk and provide semi-automatic pricing).[26]

It could also enable the development of **new products and services** such as completely decentralised P2P insurance or parametric insurance products.

BOX 1. OVERVIEW OF DECENTRALISED P2P INSURANCE AND PARAMETRIC INSURANCE BUSINESS MODEL

DECENTRALISED P2P INSURANCE

P2P insurance could be defined as a risk-sharing network where a group of individuals with mutual interests or similar risk profiles pool their 'premiums' together to insure against a risk. Thus, P2P insurance enables individuals with similar interests to share the risk between themselves.[27] Blockchain and smart contracts could increase both the scalability and decentralisation of P2P insurance/insurance-like products and services. With the blockchain design, each member of a pool can keep actionable records without the need for a trusted third party such as an insurer or platform provider. Additionally, smart contracts can be executed automatically once a certain criterion is fulfilled. In this way certain functions of a traditional insurer could be performed by a P2P network. These developments could potentially establish truly decentralised platforms/purely technical service providers/platform providers without an underlying insurance carrier. However, from a supervisory perspective it also raises the question of regulatory perimeter and applicable regulation (e.g. if these business models fall under the insurance distribution definition).[28]

PARAMETRIC INSURANCE

Parametric insurance is a type of insurance that does not indemnify the pure loss, but *ex ante* agrees to make a lump sum payment upon the occurrence of a triggering, objective and predefined event. A triggering event can be in relation to temperature (e.g. 30 days of drought in a given region), rainfall, wind speed, earthquake (e.g. up from certain magnitudes) or flight delay time (e.g. 45 minutes).

Blockchain can also automate large part of **claims-handling**, limiting the scope for disagreement between parties and reduce settlement times and claims handling cost. Claim events could be recorded in a blockchain. By enabling better coordination between insurers, blockchain can also be used to **combat fraud**. A blockchain-enabled shared database, with various levels of access and control, would enable insurers to eliminate processing of multiple claims from the same accident or establish ownership of high-value items through digital certificate and so reduce counterfeiting.[29]

Blockchain could **streamline information exchange and payments between insurers and reinsurers.** Using a blockchain-enabled shared database, insurers can enter primary data into smart contracts, with the information being accessible to reinsurers, retrocessionaires and regulators in real-time on a need-to-know basis. The data can be extracted from the blockchain for automated modelling, audits, and compliance checks. Risks can be ceded, and claims can be made with automated notification to all relevant parties.[30]

Blockchain could also facilitate **accessing and sharing insurance-related personal and non-personal data (open insurance)**.[31] Insurers already have access to their own policyholder data and claim records. By sharing this data within specific parameters on the blockchain, a policyholder no longer needs to obtain e.g. a no-claim certificate and could more easily shop around. Similarly, claims data is usually stored in independent databases within each entity (insurance undertaking, intermediary, repair shop in case of motor insurance), sometimes shared by e-mail. By collaborating together, insurers, intermediaries and repair shops can form a consortium where the focus is on simplifying the process of exchanging claims data. While some of the solutions with similar characteristic could also work through centralised databases, blockchain could arguably facilitate this kind of data exchange.

Although limited, there are already different 'live' or proof-of-concept phase blockchain use cases throughout the EU insurance value chain. Practical use cases reported include more efficient distribution processes, product design and development, claims management, back-office activities, re-insurance, dispute resolution as well as 'end-to-end' solutions. The use of smart contracts in the EU seems also rather limited yet, mainly including parametric insurance and P2P insurance solutions, or participation in the international project such as Insurewave. Many of the reported use cases are still in testing phase.

BOX 2. EXAMPLES OF BLOCKCHAIN AND SMART CONTRACT USE CASES IN INSURANCE REPORTED BY THE NCAS

KYC/AML/digital identity solutions

In Italy, solutions to improve KYC and customer on-boarding are under testing.

PRODUCT DESIGN AND DEVELOPMENTS

In Italy the use cases include parametric policies for travel and holidays insurance or for coverage of damages to crops in the agrifood industry as well as the management of suretyship coverage. **In the Netherlands** the developments are related to pension funds (e.g. value transfer and personal information sharing between pension fund and the Ministry of the Interior Relations (the latter keeps all personal record of Dutch citizens (passport etc.). **In Portugal**, Aliança Portuguesa de Blockchain is supporting an initiative that consists in developing a new insurance product based on smart contracts for sport events.

POST-SALE SERVICES AND ASSISTANCE

In Italy, blockchain has been tested for dispute resolution, allowing customers, the undertaking and their lawyers to collect and store all the documentation, to bid the amount to settle the dispute (a 'blind' auction scheme allows the two parts to agree on the amount) and eventually to manage the smart contract closing the dispute and executing the payment.

CLAIMS MANAGEMENT

In Hungary, ski insurance automatically compensates for the damage due to the bad weather conditions or the technical fault of the lifts.[32] The company allows users to customise the conditions of their travel insurance of the ski trips (e.g. the ideal percentage of functioning ski lifts during the trip), set the period of travel and expected compensation. The contract is going to be recorded as a smart contract in a public blockchain. In case the conditions are met, consumer will receive the compensation automatically, without claiming process.

There are also some international projects. E.g. **Insurwave**[33] was launched in 2018 with the idea to develop a working blockchain platform to connect all stakeholders in the insurance value chain with the same risk information. The platform uses blockchain technology to support marine hull insurance. A new vessel is registered on chain and a premium is set by an algorithm with policy documents automatically distributed to carriers. The ship's travel is recorded in real time, from location to weather conditions. When the ship moves through a risky area, this fact is recorded in its file and used for future underwriting. E.g. one large **Danish** shipping company has been part of this initiative.

REINSURANCE

The Blockchain Insurance Industry Initiative (B3i)[34] was incorporated in 2018 and is 100% owned by 18 insurance market participants around the world. Altogether, more than 40 companies are involved in B3i as shareholders, customers, and community members. Since 2017, B3i has endeavoured to put together a smart contract for property catastrophe excess of loss reinsurance that rapidly reconciles accounts between an insurer and its reinsurers, without redundancy or latency. Following an event, pay-outs are automatically calculated to affected parties.

BOX 2 (*CONTINUED*)

'END-TO-END' SOLUTIONS

In Italy there are limited experiences of blockchain-based P2P platforms. Similarly **in Lithuania** one P2P insurance platform has intention to use blockchain technology. **In Estonia,** a company currently in test phase advertises itself as providing the capital to agents, brokers and Managing General Agents (MGAs) to launch their own insurance products fast. It is built on a blockchain, which will, according to the website, improve the current insurance business model by connecting the insurance entrepreneurs with capital making it easier for them to launch new products and save costs.

In **Malta**, one entity is proposing to integrate into its platform (as nodes) the insurance undertaking, insurance broker and the bank, giving the option also for the regulator to run a 'regulatory node' - providing access in real-time to the regulator. The model is composed of an oracle that tracks and triggers the claims process once the death certificate is submitted. The process provides for integrated claims management system that enables rich data submissions (such as claims forms in pdf files) to be appended to the legacy systems of the stakeholders. It utilises blockchain encryption and private cloud storage combined with on-premises storage for transmitting the necessary information required for the process to occur.

OTHER

In Finland there has been a very small pilot, where blockchain was used for gathering data on cases where mandatory motor liability insurance had not been paid. It was a small technical pilot. **In Ireland**, the use case include helping (re)insurance undertaking share data in a managed and transparent way across a wide range of products and at all levels of the value chain.

Portuguese Insurers Association is testing some options to use blockchain in insurance, particularly in claims settlement systems.

Source: EIOPA NCA survey on blockchain

QUESTIONS TO STAKEHOLDERS

1. In addition to those described in this paper, can you report other blockchain and smart contract use cases or business models in the EU or beyond, that might be worth to look at from supervisory/consumer protection perspective?

2. Please describe your own blockchain/smart contract use case/business model and challenges you have faced in implementing it, if any.

4. CRYPTO ASSETS USE CASES IN INSURANCE

In addition to the blockchain use cases described in the previous chapter, the use of crypto assets in the insurance sector deserves special attention given that their use is already relatively extended in financial markets compared to other blockchain use cases that are mostly at a proof-of-concept stage. The European Commission's draft legislative proposal on markets in crypto assets (MiCA) defines crypto assets as a digital representation of value or rights, which may be transferred and stored electronically, using distributed ledger technology or similar technology. There are many different types of crypto assets. From a functional perspective, based on the work developed by ESMA[35] and EBA[36], crypto assets can be broadly classified into three categories:[37]

- **Payment-type**: often referred to as virtual currencies, crypto-currencies. They typically do not provide rights but can be used as a means of exchange (e.g. to enable the buying or selling of a good);
- **Investment-type**: they typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to shares, bonds or dividends);
- **Utility-type**: a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and is only accepted by the issuer of that token. For example, in the context of cloud services, a token may be issued to facilitate access.

BOX 3. EU LEGISLATIVE PROPOSAL ON MARKETS IN CRYPTO ASSETS (MICA)

On 24 September 2020 the Commission published a legislative proposal for a regulation on markets in crypto assets (MiCA)[38]. The new rules seek to clarify the application of existing EU rules to crypto-assets, and will allow operators authorised in one Member State to provide their services across the EU ('passporting'). To this extent, the legislative proposal introduces a number of safeguards including capital requirements, custody of assets, complaint handling processes, and common disclosure standards for the issuance of Initial Coin Offerings (ICOs). Issuers of significant asset-backed crypto-assets (so-called global 'stablecoins') would be subject to specific requirements.

Insurance undertakings have been explicitly excluded from the scope of MiCA (Article 2(3)), but this is not the case for insurance intermediaries and pension schemes. Therefore, the latter would need to comply with MiCA in case they would raise capital via Initial Coin Offerings (ICOs) or issue their own crypto-assets for paying insurance premiums/pay out claims. This would also be the case when insurance intermediaries sell with advice unit-linked life insurance products with crypto asset funds as underlying investments.

Moreover, some innovative types of parametric insurance business models using smart contracts based on DLT or similar technology (e.g. crop insurance or flight delay insurance) could also potentially be considered as utility tokens, as well as other utility tokens (other than intra-group transactions) potentially offered by pension schemes or insurance intermediaries (e.g. gym voucher tokens). Moreover, decentralised insurance-like business models operating with DLT or similar technology such as some innovative types of peer-to-peer (P2P) insurance or those offering 'protection' to consumers by betting on the occurrence of a particular event (e.g. flight cancellation) could also potentially fall under the scope of MiCA.

One possible use of crypto assets in insurance is the **investment in crypto assets,** either directly by purchasing crypto assets as an investment, or indirectly by investing in financial instruments with crypto assets as underlying assets. Based on EIOPA's analysis of Solvency II data, a very limited number of European insurance undertakings already count with such types of investments, fundamentally via unit-linked life insurance products where the risks (and benefits) are borne completely or partially by the consumer.[39 40]

BOX 4. INITIAL COIN OFFERINGS AND TOKENISATION OF ASSETS

Other than the investments in crypto assets, insurance undertaking and intermediaries could also raise capital via **Initial Coin Offerings** (ICO's) across multiple jurisdictions in a relatively seamless and digital manner. No ICOs launched by insurance undertakings and intermediaries were reported by NCAs in 2020, as opposed to 3 ICOs reported in 2018.

In addition to ICOs, new types of **tokenisation of assets** (i.e. utility tokens and investment tokens) are emerging and could impact the insurance sector in different ways. This is for instance the case of crowdfunding initiatives where the money invested in a fund (and the inherent rights) is tokenised amongst the different investors. Similar developments could potentially take place, for instance, in the area of P2P insurance business models. Other reported examples of tokenisation of assets include in the area of real estate transactions recording the mortgage trajectory on a blockchain (not necessarily tokenised), or in the area of digital identities (tokenisation of identities) and intra-group transactions.

Moreover, only one NCA reported the case of an insurance undertaking in its jurisdiction allowing customers to **pay insurance premiums or receive loss refunds with crypto assets**. In several jurisdictions this is not possible since there are national legal requirements establishing that such payments need to be done in a legal tender. On the other hand, in other jurisdictions this would be possible given that there is no specific provision against it.

BOX 5. HOW STABLECOINS COULD IMPACT THE INSURANCE SECTOR

Stablecoins have been touted as one of the possible remedies to address the high volatility of some crypto assets. Stablecoins are crypto assets with the value pegged to another asset, typically fiat currencies, commodities, or to even another type of crypto asset. A stablecoin arrangement typically involves 3 key interconnected functions: (i) payments, whereby stablecoins are used as a transfer of value to make payments; (ii) asset management, whereby the proceeds are invested in low-volatility assets; and (iii) a user interface to link the users to with third parties offering additional functionalities (e.g. wallet providers).[41]

While stablecoins have existed for some time, during 2019 they attracted a lot of attention in the media following the announcement by Facebook of its intention to launch its own stablecoin through the Diem Association (formerly the Libra Association). Given Facebook's large and international customer base, its stablecoin could potentially trigger a global widespread adoption of stablecoins, which has led to international standard setting bodies to refer to this phenomenon as 'global stablecoins'.[42]

Specifically in insurance, stablecoins could potentially be used as means to pay insurance premiums and/or loss refunds in those jurisdictions where there is not a legal requirement to make such payments in legal tender. This could be done either by purchasing standalone insurance products (e.g. mobile phone insurance purchased via WhatsApp), or as an ancillary to other products or services like airplane tickets or holidays bookings (e.g. travel insurance cross-sold with an airplane ticket purchased online with Facebook's stablecoin).

In addition to bespoke insurance cover provided to corporate exchanges or wallet storage providers through the Lloyds Market,[43] two other jurisdictions have reported cases of **insurance products covering the loss or theft of crypto assets**. In one case, this was linked to a ransomware insurance product, and in another case there was an insurance undertaking considering the launch of a cyber-insurance product specifically covering the 'theft of electronic currency'. However, most NCAs consider that in their jurisdiction cyber insurance products typically exclude such coverage. Silent or non-affirmative cover could also potentially exist, i.e. instances where loss of crypto assets is not explicitly excluded in the terms and conditions of another insurance policy.

QUESTIONS TO STAKEHOLDERS

3. Are you aware of practical examples of crypto-assets use cases in insurance? Please describe these use cases, specifying the types of crypto assets concerned (e.g. payment-type, investment-type, or utility-type) and explain whether they are already being implemented or they are still at a proof-of-concept / early stage of development.

4. Without prejudice of your reply to the previous question, are you aware of insurance products covering the loss or theft of crypto assets being marketed to retail or commercial clients? Please explain your response.

5. How do you think that the investments in crypto assets by insurance undertakings will evolve during the next 3 years?

6. How do you think the European Commission's draft legislative proposal on markets in crypto assets (MiCA) will impact the use of crypto assets in the insurance sector?

5. BLOCKCHAIN AND SUPTECH

Around the world, supervisory authorities are assessing how to increasingly use new technologies, including blockchain, to support their supervisory review process, making it more flexible and responsive. EIOPA SupTech Strategy[44] already refers to blockchain as as a technology to be further explored.

Blockchain could in theory provide opportunities for both prudential and conduct supervisors, as well as facilitating RegTech solutions. E.g. in regulatory reporting, the combination of smart contracts and blockchain could help to automate regulatory reporting and make it more efficient and transparent, improve consistency and data quality across undertakings, and allow regulators to get data on new areas of interest with real-time access to signed contracts and information they contain (real-time regulatory monitoring), reducing compliance costs and making the whole insurance sector more transparent.[45]

For the time being, while data-driven supervision is high on the agenda of most NCAs, few NCAs are currently using blockchain as a substantial component to support the supervision. However, some NCAs are investigating the inclusion of this technology.

Management of registers and lists of undertakings/intermediaries together with supervisory reporting and publication of data and statistics are the main areas of supervision where NCAs potentially see the biggest impact in the future. E.g. **Central Bank of Hungary (MNB)** is planning to develop a register, based on DLT that may contain data on property insurance for real estates used as collateral for mortgage loans. Similarly, EIOPA, its Members and Observers are assessing the possibility to build a register of insurance undertakings where blockchain will be one of the options to be considered, where each NCA would host a node of the register, thus guaranteeing full consistency of the information shown in all national and European registers in the EEA.

The most important factor currently restraining the use of blockchain for supervision seems to be the fact that the efficiency of using blockchain for supervision has still to be evidenced. Further work is probably needed to address these concerns and small-scale projects or a study to analyse potential alternative business cases of blockchain could help in exploring the best way to harness the potential of blockchain technologies.

BOX 6. THE FMA EVALUATION OF BLOCKCHAIN USE FOR SUPERVISION

The Austrian Financial Market Authority (FMA) has actively promoted awareness of the potential uses, strengths and weaknesses of the blockchain technology across its departments. Multiple talks and trainings including external experts and researchers were organised. However, as of now no clear use case where a blockchain solution would be an efficient and effective tool to utilise has emerged. A more general reason is, that strong points of this technology make it especially suited to transparent/peer-to-peer based environments, whereas FMA´s position is that of a central supervisor handling highly confidential data, which undercuts the advantages of blockchain in many potential scenarios.

Source: EIOPA NCA survey on blockchain

QUESTIONS TO STAKEHOLDERS

7. Do you see other blockchain/smart contract use cases in RegTech/SupTech that might be worth to look at further from supervisory/consumer protection perspective?

8. Please describe your own blockchain/smart contract use case/business model in RegTech/SupTech and the challenges you have faced in implementing it, if any.

6. RISKS AND BENEFITS OF BLOCKCHAIN AND SMART CONTRACTS

While promising to drive efficiency in business practices and mitigate certain existing risks, the adoption of blockchain may trigger new risks to insurance undertakings, supervisors and consumers. As blockchain technology is still evolving, general concerns are showing up, such as uncertainties caused by absence of regulatory clarity, complexity of the technology, data privacy, integration with legacy infrastructures, or interoperability and standardisation between different blockchains. Based on blockchain types and platforms chosen, performance and scalability challenges could arise. Some risks are related broadly to its emerging technology status. Additionally, the decentralised nature of the blockchain might create risks that are different from traditional centralised solutions.

Given the very early stage of blockchain and smart contract development/implementation as well as lack of experience related to that, potential risks of blockchain and smart contracts (and consequently, necessary safeguards) but also benefits are difficult to foresee comprehensively. The probability and impact of those risks also depend on the specific use case and nature of the blockchain solution.[46] Possible regulatory course taken and further evolution of the market in future can also effect risks and benefits. Hence, any detailed classification of both risks and benefits can be seen as indicative only, although general potential risks that deserve scrutiny and adequate safeguards can be highlighted.

BLOCKCHAIN AND SMART CONTRACTS-RELATED RISKS FOR CONSUMERS

From a **consumer protection and transparency perspective**, the provision of advice and related disclosure regulations may need further analysis to address any confusing aspects of blockchain and smart contracts.[47] While smart contracts currently in place seem to be relatively simple and leading to further standardization and simplification, more complex products in the form of automatically executing smart contracts, could be expected to require especially close attention regarding customer information, disclosures and sales process. The complexity associated with the blockchain and smart contracts may produce misunderstandings about the products and respective risks, especially for consumers insuring material risks or signing up for long term products without an exit option.

The **automated execution and enforcement of contractual conditions** previously set by the relevant parties might also lead to inability to manage any contingencies arising during the execution of the smart contract.[48] This may also affect the submission of effective complaints by consumers. **Risk of exclusion** for customers that prefer more traditional methods of communication or that have a low level of technological education or skill could also occur.

Some new blockchain-based products might also lead to **regulatory perimeter risk**, or might experience **legal uncertainty** or different treatment in different jurisdictions (e.g. certain decentralised P2P insurance platforms), ultimately decreasing consumer protection. The legal validity of smart contracts vis-a-vis the applicable civil law principles could also raise issues.

Blockchain solutions could also increase **fraud and money laundering risk**. Information stored on the blockchain itself will usually be visible and transparent to the participants of the system. However, data protection needs could require the anonymisation of data and thus limit the identification of real identities.

From a **legal and data privacy** perspective there is a risk that the combination of large amounts of historic data about a consumer or a group of customers may result in an indirect use of sensitive data otherwise not allowed by laws. Given that records on the blockchain are largely tamper-resistant and immutable, the adverse impact on compliance with certain GDPR provisions, such as the right to be forgotten and data erasure requirements, needs to be also carefully considered.

From an **ICT/cyber risk** perspective, the security and reliability of the underlying technology as well as smart

contract programming mistakes are important. Smart contracts could be also subject to hacking. Possible cyber risks related to key management are also relevant.

There is also a significant **financial education/expectations gap** which needs to be addressed. Consumers may not be aware of all blockchain and smart contract features, including the importance of proper management of public-private keys, as necessary. Complexity and novelty can create a gap in consumer's know-how about the products they buy, and can also increase difficulty in court decisions when litigation arrives. In any case, potential consumers need to fully understand the contract they are entering, its features (e.g. when contract enters into force, coverage and conditions) and consequences, and the provision of advice and information has to meet the standards expected in traditional policies.

Specifically concerning crypto assets, the risk for consumers are outlined in the warning to consumers issued by the European Supervisory Authorities in February 2018.[49] The warning mentioned risks such as the unregulated nature of several types of crypto assets, their **high volatility and 'bubble risk'**, the lack of price transparency or risks that consumers could be provided with inaccurate or misleading information. In this regard, it should be noted that some of those risks are not applicable to all types of crypto assets (e.g. stablecoins are not highly volatile). The latest review of the Anti-Money Laundering Directive (AMLD5) has addressed some risks linked to anti-money laundering, and some jurisdictions have passed their own bespoke crypto assets legislation at national level. Once entered into force, the MiCA legislative proposal is also expected to mitigate several of these risks for consumers. However, for the time being most NCAs consider that the European Supervisory Authorities (ESAs) warning to consumers remains valid and that crypto assets are still not appropriate for unexperienced and/or unsophisticated retail consumers.

BLOCKCHAIN AND SMART CONTRACTS-RELATED RISKS FOR UNDERTAKINGS

Potential risks include **lack of knowledge on blockchain** as well as **governance challenges**, especially due to potentially high dependency on external platforms and IT suppliers. Setting up a blockchain solutions would also require the availability of **technical personnel with a specific skillset** (or accept a high risk of dependency on third parties). There might be also **interoperability risk** between different blockchains and lack of integration with internal legacy systems or issues related to the migration of legacy data into the new systems. There might be also a need to enhance **ICT/cyber resilience** and set up **adequate recovery plans** to address and manage potential risks. Similarly risks are related to maintain efficient internal controls, risk management and compliance functions. **Performance and scale-up risk** might also occur, e.g. the business risk of not arriving at profitable blockchain operations while having invested heavily in this technique.

Although still limited, the decentralised element of blockchain might also lead to reduced reliance on traditional insurance intermediaries, ultimately leading to new market structures (e.g. decentralised P2P insurance).

More concretely for smart contracts, the **issues related to oracles**, including dependency on, and reliability of oracles are also a major concern. The smart contract itself depends on input data for its execution, including often external data. These external oracles could introduce dependencies and may, in some cases, lead to heavily centralised contract execution.[50] This could also include the question who determines which oracles are necessary in smart contracts, how to guarantee their reliability (e.g. should they possibly be validated before use in order to secure the reliability) and who is ultimately accountable in case the information is not accurate. Related to that, **change and governance of smart contracts** could also be seen as an issue, including governance of the chain and ownership of data.

Concentration risk and vendor/service provider risk (lock-in risk) could also occur, e.g. when using external data vendors, oracles or other third parties. From **antitrust** perspective, there is a possibility of the creation of new barriers to entry in some market segments/lines of business due to the necessary investment in technology to achieve a viable business case. The latter might not be achievable for smaller insurance undertakings (although less complex blockchain solutions seem to be more accessible also for SMEs). This can again increase the concentration risk.

Insurers need also consider the manner in which the use of blockchain and smart contracts may **adversely affect consumers** and mitigate risks related to customer information and provision of advice, e.g. entities need to ensure that the necessary disclosures are made and the demands and needs/suitability and appropriateness assessments are effectively carried out notwithstanding the use of blockchain technology (see above on consum-

er risks). Otherwise, **regulatory as well as reputational risks** might occur.

Finally, **legal uncertainty** can occur. While blockchain could support (depending on the solutions, e.g. public and permissionless vs private and permissioned blockchain) KYC/AML compliance[51], the anonymity inherent to a blockchain-type technology can also represent a risk concerning the compliance with AML regulatory requirements, and, the new type of products that can arise from this technology (e.g. products structured on crypto-assets; products using virtual currencies). Similarly it might be difficult to comply with some of the provisions of the GDPR (e.g. right to be forgotten). Additionally, the legal status of 'smart contract' can raise questions e.g. how does it interact with general contract law principles.[52]

As far as the risks arising from crypto assets are concerned, to date their impact is very limited due the low materiality of insurance undertaking's investments in crypto assets. Should these investments increase in the future, insurance undertakings would be exposed to a number of risks including **market risks** (namely due to high volatility of some crypto assets), **credit and counterparty risks** (e.g. a default from a crypto-assets exchange or wallet provider) or **operational risks** (including cyber risks). Moreover, as noted by several international standard setting bodies the so-called global stablecoins have not received a widespread adoption yet so their potential financial stability implications are also limited, although developments in this area could unfold very quickly. However, the ongoing trends in stablecoins and Central Bank Digital Currencies (CBDCs) could eventually influence how undertakings approach the use of crypto assets.

Insurance undertakings could also face **compliance risks**, namely with the prudent person principle included under Article 132 Solvency II, since it can be challenging for insurance undertakings to properly identify, measure, manage and control the risks of several types of crypto assets. From a conduct of business perspective, insurance undertakings will also need to comply with the requirements included in the Insurance Distribution Directive (IDD). In the particular case of unit-linked life insurance products with crypto assets as underlying assets, they will most likely need to manufacture and distribute these products to a tightly defined target market of sophisticated consumers, who understand the risks involved around crypto assets. Special attention should also be given to the development of reliable performance scenarios and risks indicators required in the Key Information Document (KID) under the Package retail investment and insurance-based products (PRIIPs) Regulation.

BLOCKCHAIN AND SMART CONTRACTS-RELATED RISKS FOR SUPERVISORS

Most of the risks mentioned above in regard to consumers and undertakings are relevant also for NCAs when they use blockchain themselves for e.g. SupTech solutions, as well as when conducting supervision (e.g. **ICT/cyber risk, fraud risks, data privacy, interoperability risk** etc.) as the mission of the NCAs is to ensure a sound regulatory and supervisory framework for the insurance market.

From the perspective of the use of blockchain for supervision, it is important that NCAs obtain a proper understanding of the potential risks associated with deployments of this technology, and, to the extent necessary, monitoring that undertakings and intermediaries appropriately manage and mitigate relevant risks, understanding and overseeing market developments, assessing governance arrangements (especially in permissioned chains) and checking the substantial application of the **regulatory perimeter**. Indeed, the biggest challenge for NCAs seems to keep track on market developments and to understand the blockchain technology, and assess the risks and benefits of its usage in the insurance market.

It can be also predicted that NCAs will inevitably oversee **increased co-operation** between insurance companies/intermediaries and relevant third parties/start-ups[53] in order to plan or establish part/most of their operations based on blockchain technology. Indeed, despite the decentralised nature of blockchain, undertakings will inevitably be placing reliance on certain third parties (such as blockchain developers and nodes themselves). This will inevitably have an impact on the governance of undertakings and bring changes to their legacy systems and responsibilities. Hence, NCAs need to ensure that in this respect, companies build the necessary resilience in their governance to ensure appropriate intervention to adapt accordingly. **Concentration risk** is also important from supervisory perspective, e.g. the use of few networks or oracles by the insurance sector. Moreover, industry specific blockchain platforms such as Hyperledger, Corda are gaining momentum.

Finally, although blockchain and smart contract use cases in insurance are still limited, the decentralised element of blockchain might also lead to reduced reliance on traditional insurance intermediaries, ultimately leading to new market structures. Impact of this on consumers is also important to consider, including from possible financial exclusions perspective.

From a broader supervisory perspective the question arises as to who oversees the correct and legitimate functioning of the complex structures of blockchain and smart contracts and how. This could also include more **systemic risks**, e.g. as there is no central authority to correct the contract in case there are some wrong transactions, being activated automatically, a lot of contracts can be settled in a short time, leading to sudden market moves.

Particularly concerning crypto assets, the European Commission's draft legislative proposal will address certain gaps in the existing legislation. Specifically from an insurance perspective, given the current stage of development of crypto asset markets and their materiality for the insurance sector the **supervisory review process** rules seems sufficient. It is important that insurance undertakings inform the supervisory authority of actual and planned crypto-asset exposure in a timely manner and provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and how it has mitigated these risks. If crypto-asset investments become significant, closer supervisory attention may be required. Supervisors should also closely monitor the **potential financial stability implications arising from global stablecoins**. Moreover given rapidly evolving technical capacities, a focus on building expertise and maintaining this remains important for supervisors.

BLOCKCHAIN AND SMART CONTRACTS-RELATED BENEFITS FOR CONSUMERS

Blockchain could **enhance consumer experiences** through higher efficiency/automation and **new products and services** better tailored to consumer needs (e.g. P2P insurance or on-demand insurance or parametric products), easier and faster access to insurance cover or better and faster claims and settlement processes. It could also facilitate better integration with payment infrastructure (e.g. for premiums payments).

Opportunities for **voluntary data sharing by customers** (under the GDPR provisions) could also facilitate open insurance/open finance developments[54], providing opportunities for new products and services, so that insurers can e.g. better assess consumer behaviour and risk profiles on an ongoing/real-time basis (e.g. compiled through the use of connected devices and exchanged directly on the blockchain). This can result in more dynamic pricing and, again, in more flexible and personalised products and services. It could also facilitate advice services. E.g. insurers could choose to convert multiple policies into smart contracts, enabling them to produce a single, consolidated view of policy data and documentation in near real-time. All this could potentially **lower administrative costs**, which would be an obvious benefit for the policyholders, but also **improve competition**, ultimately again of the direct interest to customers.

Blockchain could also **increase transparency**, e.g. in theory, the openly visible nature, where implemented in public, 'if-then'-based architecture and potentially automatic execution of smart contracts can enhance understanding of the pay-out conditions of insurance policy or can gain an insight into the actual settlements between their peers and an insurance undertaking. This could be an incentive for insurers to apply more generous conditions for pay-out than would be the case if the claim was only settled between customers and undertakings in private. Increased transparency could also **facilitate fraud detection**.

Potential benefits for consumers arising from crypto assets could include **more efficient and cheaper transactions** when purchasing insurance products, namely as a result of fewer intermediaries being involved. Crypto-assets also offer a **wider range of investment opportunities** for consumers with different risk profiles. Crypto assets could also foster **financial inclusion** amongst those populations that do not have easy access to traditional financial services such as bank accounts or credit cards, and thus enhancing their access to insurance products (e.g. they would not need a bank account to purchase insurance products and make renewal payments, since this could potentially be done through their social media account).[55]

BLOCKCHAIN AND SMART CONTRACT-RELATED BENEFITS FOR UNDERTAKINGS

Blockchain could be used to support existing business models as well as to gain a competitive advantage by allowing the introduction of **new products and services**, better tailored to consumer needs. By combining data from contracts, claims and consumer documentation in general, blockchain could enhance wider and more rapid development of **personalised insurance and services**

and innovative product design (e.g. P2P insurance; parametric insurance; and IoT-based products).

Blockchain-based systems might allow for **high degrees of automation** in some processes (e.g. underwriting, price optimisation). E.g. it could allow to automate some of the conditions and obligations within insurance contracts as well as facilitate standardisation of contracts and facilitate integration with public databases or information exchange with third parties (if accessible via API and web services). It could also help to conduct automated audits. By deploying relevant rules within smart contracts, insurance entities can have **improved and more efficient underwriting** (e.g. setting rates, by relying on big data analytics and access to demographic data, GPS data used to collect premiums based on kilometres driven), **pricing and claims management processes.** For instance, smart contracts would automatically activate and determine pay out to or from policyholders as a response to the triggering of pre-determined events or information.

Benefits could also include e.g. better integration with payment services. Better data integrity and accuracy and the use of smart contracts also enables real-time settlement of claims or automation of a large part of claims handling, leading to **more efficient claims management.** Blockchain could also reduce duplication of processes and data duplication thereby improving quality of data. This all can lead to **increased efficiency and lower operational costs.**

Blockchain could also provide **enhanced security**, offering a single source of truth. This enables **better coordination between insurance entities**, since it facilitates the establishment of a transparent permissioned network/database to optimise secure sharing of relevant data records essential to all parties, possibly with different levels of access to information. It could also open up **new cross-selling options** that might help in opening new consumer segments. This all can be seen again as indirectly improving the overall customer experience.

Similar to consumers, insurance undertakings could also benefit from more **efficient and cheaper transactions** (including cross-border transactions) when using crypto assets to sell insurance products and/or to pay loss refunds. Crypto-assets also offer a **wider range of business models (e.g. P2P insurance) or investment opportunities** to insurance undertakings. Insurance undertakings and more particularly InsurTech start-ups could also use crypto assets as an alternative funding tool and benefit from the possibility to **raise capital on a cross-border and frictionless basis** with the launch of ICOs. The tokenisation of tangible assets (e.g. in the area of real estate properties) and intangible assets (e.g. data, software, intellectual property rights) also have the potential to increase the liquidity, transparency and tradability of such assets.

BLOCKCHAIN-RELATED BENEFITS FOR SUPERVISORS

RegTech and SupTech solutions can help NCAs and insurers to cope with administrative burden and keep the quality of supervision up-to-date with increasing regulatory requirements and amount of data to analyse.

Data as well as the fostering of SupTech solutions provide NCAs with **improved data quality and a wider source of reliable data**. Blockchain also enables immutable record-keeping and transaction processing through P2P exchange of digital data which is constantly updated and synchronised. The inherent trust and transparency could facilitate the establishment of collaborative efforts between insurers and the relevant NCAs, who may be granted **access to data** in the database in real time, as necessary granting an updated and unified view of core information relevant to the insurance market supervision. In addition, it enables more accurate and increased **predictive analytics** for the NCAs to undertake better risk-based supervision and more targeted audits and compliance checks.

Questions to stakeholders

9. Do you agree the potential risks for the a) industry, b) consumers and c) supervisors are accurately described?

10. Are there additional risks?

11. Do you consider that the current regulatory and supervisory framework is adequate to capture these risks? If not, what can be done to mitigate these risks?

12. Do you agree the potential benefits for the a) industry, b) consumers and c) supervisors are accurately described?

13. Are there additional benefits?

14. What can be done to maximise these benefits?

7. REGULATORY BARRIERS IN RESPECT OF BLOCKCHAIN AND SMART CONTRACTS

The existing regulations are grounded on centralised governance structure while blockchain as a DLT enables a distributed governance structure. Therefore, the effective adoption of blockchain could require the amendment of the existing regulations. For example Know-Your-Customer (KYC) processes and requirements on legal archiving of documents. While electronic archiving of documents is generally allowed, the compliance of blockchain with such requirements needs to be fully assessed. NCAs also highlighted barriers especially regarding data protection legislation (even if justified), e.g. the 'right to be forgotten' in the GDPR.

As to existing EU law provisions where additional clarity might be needed, the development of blockchain solutions could be delayed by the need for an indisputable and harmonised interpretation of regulations with particular regard to regulatory perimeter, customers' on boarding, risk management and consumer protection. E.g. the qualification of certain event-based derivative tokens could be difficult and applicable compliance rules not certain. Those tokens could bore similarities with derivatives like spread betting, binary options or contract for differences (CFDs) whilst keeping a certain insurance product characteristics.

From the Insurance Distribution Directive[56] (IDD) perspective, the assessment of suitability for the customer for advised sales, and appropriateness for most non-advised sales (except in 'execution only') has been mentioned. It has also been argued that product oversight and governance (POG) and Insurance Product Information Document (IPID) requirements might be too complex for simple and standard products, hence there might be a need for streamlining the process (without reducing customer protection) and improving the possibility to share digital documentation. One NCA also mentioned the issue of collecting and storing documents for identification and on-boarding of the customer just once (at registration) and limit the amount of further data required for each product bought on the same platform.

Some of the proposed barriers also stem from national law. One NCA pointed out that a barrier for smart contracts is the fact that according to national law life insurance contracts are only concluded when the contract is signed by the policyholder, the insured person and the insurer. Another NCA mentioned national requirements on legal archiving and record keeping of documents which might not be possible to fulfil when using blockchain.

So far most of the NCAs have not undertaken any specific measures related to barriers, other than using innovation facilitators as a fora for discussing possible blockchain and smart contract developments and engaging with the industry to build technical capacity and identify significant risks. While the exact scope of those innovation facilitators vary in different countries, they could be open for entities willing to launch their blockchain solutions, or include improving the early dialogue with market operators when setting up a new service to discuss potential standards and remove regulatory barriers. Interesting there are also some innovation facilitators approaching directly blockchain. Additional engagement with the industry seems to be mainly through traditional regular or ad-hoc dialogue with the companies on their plans for utilisation of new technologies such as blockchain.

BOX 7. INNOVATION FACILITATORS FOCUSING ON BLOCKCHAIN

In Italy, a public-private initiative called **Insurance Blockchain Sandbox** (IBS)[57] allows insurance companies and brokers to test products, services, processes, business models and distribution models in the real market, with real stakeholders (companies and / or customers). Participation takes place on the basis of the single use case to be tested, which must have the following requirements: blockchain-based; innovative, allowed by regulations in force and with a beneficial impact on the consumers. IVASS is participating as an institutional partner in this Sandbox.

Lithuania has created project LBChain that is combination of blockchain sandbox and regulatory sandbox where they together with market players can experiment with blockchain products in controlled environment.

Source: EIOPA NCA survey on blockchain

Questions to stakeholders

15. Do you agree the barriers highlighted in this chapter exist?

16. What additional regulatory barriers do you see?

    a) in EU insurance legislation;

    b) in EU non-insurance legislation.

17. What are in your view the main regulatory and non-regulatory barriers preventing the use of crypto assets in insurance?

8. EUROPEAN APPROACH TO BLOCKCHAIN AND SMART CONTRACTS IN INSURANCE

This Discussion Paper identifies different aspects, use-cases as well as risks and benefits of blockchain and smart contracts in insurance from supervisory and risk perspectives, with the aim to start a broader multi-stakeholder engagement on the topic.

All the emerging technologies identified raise questions as to whether existing regulation specifically addresses the new possibilities as well as new risks.

Indeed, there are a number of features of blockchain which have the potential to be seen as inconsistent with, or ambiguous under current insurance, data protection and civil law regulations. Most of the issues are related to the nature of blockchain and smart contracts and are not specific to the insurance sector. Nonetheless, it may be useful to identify possible insurance-specific issues for the broader policy debate.

Depending on its application, the use of blockchain and smart contracts by insurance undertakings or intermediaries may be subject to various regulations. For example, civil law governs basic ownership and contractual rights and obligations, potentially also the validity of smart contracts, whereas insurance regulation dictates how the industry processes e.g. transactions, payments and how it ensures cyber resilience. Data privacy and security and consumer data transmitted through blockchain is under the remit of privacy/data protection laws.

Smart contracts specifically could also raise regulatory and supervisory questions with their self-executing nature which potentially could be damage an insured party with inappropriate claim denials, or where a bug in the smart contract or tinkering by a cyber-attacker causes the contract to fail to perform as intended. The immutable nature of smart contracts could also pose again a challenge in terms of the GDPR rights to be forgotten, or in an insurance delinquency proceeding, where for example, a court-appointed administrator may seek to cut off or delay future claims payments.

Given its wide range of applications and the early stage of adoption in the insurance industry, most jurisdictions are still investigating policy responses through exploratory analysis and discussion papers that analyse the blockchain unique features, opportunities and risks, different use cases, potential implications for insurance market and regulatory considerations. This can cause legal uncertainty and act as a barrier to the use of blockchain and smart contracts in insurance, but could also lead to divergent regulatory and supervisory practices and different level of consumer protection across the EU.

Hence a general European harmonised approach to blockchain could promote and facilitate the sound scaling of blockchain and smart contracts, including in insurance. This approach should achieve coherence with overall consumer protection, financial stability and sound prudential regulation objectives and ultimately support a more integrated and efficient European insurance market.

Steps have already been taken in this direction. The European Commission's Digital Finance Strategy set a target that by 2024 the EU should put in place a comprehensive framework enabling the uptake of DLT and crypto-assets in the financial sector. To achieve this, the Commission published a proposal for a regulation on markets in crypto-assets (MiCA) as well as a proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology[58] with the aim to provide a framework to allow for innovation in a way that preserves financial stability and protects consumers. These proposals ultimately aim to help overcome some of the challenges highlighted in this Discussion Paper, especially with regards to crypto assets.

In addition to the above-mentioned legislative proposals, further actions might be needed in the area of crypto assets at European level, in particular concerning the prudential and accounting treatment of crypto assets. Indeed the accounting treatment of the different types of crypto assets may require further clarification, taking into account that diverse accounting practices could give rise to different capital requirements under Solvency II. The DFS already outlines that 'in light of ongoing work carried out by the Basel Committee, the Commission will consider updating the prudential rules for crypto-assets

held by financial firms'. It should also be noted that in July 2020 the European Financial Reporting Advisory Group (EFRAG) launched a one-year public consultation on the accounting treatment for crypto assets (liabilities).[59] Previously, the International Financial Reporting Standards Interpretations Committee (IFRS IC) had analysed the accounting treatment of payment-type crypto-assets, broadly concluding that they should be treated as 'inventories' or 'intangible assets', but not as 'financial assets'.[60]

Furthermore, there might be also additional insurance-specific issues where further steps might be needed. Hence EIOPA aims to continue facilitating information sharing and the identification of main use cases and best practices on blockchain and smart contracts in insurance, and related risks, barriers and opportunities, as well as monitoring future developments in this area to identify the trends to ultimately promote level playing field at EU level, promote EU convergence of supervisory approaches and assess the evolution of these technologies in the insurance market.

This could include broader discussion on EU insurance legislation and its application to blockchain and smart contracts, e.g. whether it is fit for purpose to allow blockchain use and mitigate relevant risks (e.g. IDD conduct of business and disclosure rules). This could also include focusing on the areas of oracles and data vendors, as this arguably includes main vulnerabilities for the industry and for consumers. From regulatory perimeter perspective this could also include discussion on common European approach on blockchain-based P2P insurance/protection products to provide level playing field and sufficient consumer protection.

Additionally, integrating these considerations on blockchain with existing EIOPA guidelines (e.g. Information and Communication Technology security and governance guidelines[61] and guidelines on outsourcing to cloud service providers[62]) could be further explored.

EIOPA will assess the feedback to this Discussion Paper in order to better understand the developments and risks and benefits related to that. This could also help to provide informed insurance supervisory specific input for the upcoming legislative initiatives foreseen in the European Commission DFS. It could also supplement EIOPA´s overall work on digitalisation, including work on areas such as complex insurance value chain, insurance platforms and ecosystems, open insurance, digital ethics and RegTech/SupTech.

Questions to stakeholders

18. Do you agree there is a need for coherent European approach to blockchain and smart contracts in insurance? What could be done to achieve this and specifically what EIOPA could do?

19. Do you consider that there is a case for clarifying or updating the prudential rules for in relation to crypto-assets if held by insurance undertakings? Please explain your response. In particular, taking into account the developments in international financial reporting standards, are you aware of examples where it is not clear how to apply insurance prudential rules to crypto assets? Please provide those examples and specify the rules which are not clear.

20. Do you agree with the proposed follow-up actions stated in this chapter?

ANNEX 1. CONSULTATION QUESTIONS

1. In addition to those described in this paper, can you report other blockchain and smart contract use cases or business models in the EU or beyond, that might be worth to look at from supervisory/consumer protection perspective?
2. Please describe your own blockchain/smart contract use case/business model and challenges you have faced in implementing it, if any.
3. Are you aware of practical examples of crypto-assets use cases in insurance? Please describe these use cases, specifying the types of crypto assets concerned (e.g. payment-type, investment-type, or utility-type) and explain whether they are already being implemented or they are still at a proof-of-concept / early stage of development.
4. Without prejudice of your reply to the previous question, are you aware of insurance products covering the loss or theft of crypto assets being marketed to retail or commercial clients? Please explain your response.
5. How do you think that the investments in crypto assets by insurance undertakings will evolve during the next 3 years?
6. How do you think the European Commission's draft legislative proposal on markets in crypto assets (MiCA) will impact the use of crypto assets in the insurance sector?
7. Do you see other blockchain/smart contract use cases in RegTech/SupTech that might be worth to look at further from supervisory/consumer protection perspective?
8. Please describe your own blockchain/smart contract use case/business model in RegTech/SupTech and the challenges you have faced in implementing it, if any.
9. Do you agree the potential risks for the a) industry, b) consumers and c) supervisors are accurately described?
10. Are there additional risks?
11. Do you consider that the current regulatory and supervisory framework is adequate to capture these risks? If not, what can be done to mitigate these risks?
12. Do you agree the potential benefits for the a) industry, b) consumers and c) supervisors are accurately described?
13. Are there additional benefits?
14. What can be done to maximise these benefits?
15. Do you agree the barriers highlighted in this chapter exist?
16. What additional regulatory barriers do you see?

    a) in EU insurance legislation;

    b) in EU non-insurance legislation.
17. What are in your view the main regulatory and non-regulatory barriers preventing the use of crypto assets in insurance?
18. Do you agree there is a need for coherent European approach to blockchain and smart contracts in insurance? What could be done to achieve this and specifically what EIOPA could do?
19. Do you consider that there is a case for clarifying or updating the prudential rules for in relation to crypto-assets if held by insurance undertakings? Please explain your response. In particular, taking into account the developments in international financial reporting standards, are you aware of examples where it is not clear how to apply insurance prudential rules to crypto assets? Please provide those examples and specify the rules which are not clear.
20. Do you agree with the proposed follow-up actions stated in this chapter?

ANNEX 2. ABBREVIATIONS

AI	Artificial Intelligence
AML	anti-money laundering
API	application programming interfaces
CBDCs	Central Bank Digital Currencies
CFD	contract for differences
DFS	European Commission Digital Finance Strategy
DLT	distributed ledger technology
EIOPA	European Insurance and Occupational Pensions Authority
ESAs	European Supervisory Authorities (EBA, ESMA and EIOPA)
EU	European Union
GPS	global positioning system
GDPR	General Data Protection Regulation (2016/679/EU)
ICT	Information and Communication Technology
IDD	Insurance Distribution Directive (2016/97/EU)
IoT	Internet of Things
IPID	Insurance Product Information Document
KID	Key Information Document
KYC	know your customer
MiCA	proposal for a regulation on markets in crypto-assets (COM(2020) 593)
NCA	national competent authority
P2P	peer-to-peer
POG	product oversight and governance
PRIIPs	Packaged Retail Investment and Insurance Products

ENDNOTES

[1] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, COM(2020) 593.

[2] Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for market infrastructures based on distributed ledger technology - COM(2020)594.

[3] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions ' Digital Finance Strategy for Europe', COM(2020)591 http://ec.europa.eu/finance/docs/law/200924-digital-finance-strategy_en.pdf.

[4] For the sake of simplicity, this Discussion Paper will mainly use the terms blockchain and will distinguish between DLTs where necessary. See more in definitions in chapter 2.

[5] See e.g. OECD Blockchain Primer. See also https://ec.europa.eu/digital-single-market/en/blockchain-technologies.

[6] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions ' Digital Finance Strategy for Europe', COM(2020)591 http://ec.europa.eu/finance/docs/law/200924-digital-finance-strategy_en.pdf

[7] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, COM(2020) 593.

[8] Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for market infrastructures based on distributed ledger technology - COM(2020)594.

[9] See e.g. BIS 2020, Policy responses to fintech: a cross-country overview https://www.bis.org/fsi/publ/insights23.htm See also The Tokenisation of Assets and Potential Implications for Financial Markets, OECD, 2020.

[10] 30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission, 2019.

[11] https://www.eiopa.europa.eu/content/discussion-paper-reinsurance-value-chain-and-new-business-models-arising-digitalisation

[12] Insurance and Distributed Ledger Technology: A risk manager´s guide, CRO Forum, 2019.

[13] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[14] See e.g. 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.htm;European Commission, 'Study on Blockchains: Legal, governance and interoperability aspects' (SMART 2018/0038).

[15] Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies, Publications Office of the European Union, Luxembourg, 2019.

[16] Ibid.

[17] See 30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission, 2019.

[18] Insurance and Distributed Ledger Technology: A risk manager´s guide, CRO Forum, 2019.

[19] See European Commission, 'Study on Blockchains: Legal, governance and interoperability aspects' (SMART 2018/0038). See also Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies, Publications Office of the European Union, Luxembourg, 2019.

[20] A computer program is deterministic if, given specific input and initial state, it will always generate the same output.

[21] Insurance and Distributed Ledger Technology: A risk manager´s guide, CRO Forum, 2019.

[22] 30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission, 2019.

[23] Insurance and Distributed Ledger Technology: A risk manager´s guide, CRO Forum, 2019.

[24] AI tools could be used to remove the need for physical access to the accident location, with the advanced analysis of photos and other relevant evidence.

[25] Blockchain and Insurance: New Technology, New Opportunities, ConsenSys Insights, 2019.

[26] https://www.ibm.com/blogs/blockchain/2018/03/three-areas-in-the-insurance-industry-to-use-blockchain/

[27] EIOPA Report on Best Practises on Licencing Requirements, Peer-to-Peer Insurance and the Principle of Proportionality in an InsurTech Context, EIOPA, 2019 https://www.eiopa.europa.eu/content/report-best-practises-licencing-requirements-peer-peer-insurance-and-principle_en.

[28] See Report on Best Practises on Licencing Requirements, Peer-to-Peer Insurance and the Principle of Proportionality in an InsurTech Context, EIOPA 2019, https://www.eiopa.europa.eu/content/report-best-practises-licencing-requirements-peer-peer-insurance-and-principle_en.

[29] Blockchain and Insurance: New Technology, New Opportunities, ConsenSys Insights, 2019.

[30] Blockchain and Insurance: New Technology, New Opportunities, ConsenSys Insights, 2019.

[31] See EIOPA Discussion Paper on open insurance: accessing and sharing insurance-related data, 2021, https://www.eiopa.europa.eu/content/open-insurance-accessing-and-sharing-insurance-related-data_en.

[32] The product has been developed, but it has not been started until the finalization of this Discussion Paper

[33] https://insurwave.com/

[34] https://b3i.tech/home.html

[35] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[36] https://eba.europa.eu/file/40451/download?token=dD44Fb9A

[37] It is important to note that there are also some hybrid types of crypto assets that can perform different functions at the same time.

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593

[39] Nearly all the relevant assets identified are Bitcoin and Ether ETF trackers invested via unit linked life insurance products. It is important to note that the materiality of these investments is very low; based on a more granular analysis performed in Q2 2019, these investments represented less than 0.2% of the total assets of the two insurance undertakings with a higher exposure to crypto assets.

[40] In order to identify insurance undertaking's investments in crypto assets, EIOPA has used Solvency II prudential solo reporting data. It has sought to identify these investments by assessing the name of the asset, the issuer of the asset, and the list of funds provided by ESMA and by one NCA. Most of the relevant assets identified are Bitcoin and Ether ETF trackers. While EIOPA has not identified any investments in other crypto assets like Bitcoin cash or Ripple, it is important to note that the identification method used is not comprehensive and does not ensure the detection of all investments in crypto assets. For a complete analysis it would be necessary to request undertakings to identify this type of investments, for example via the CIC code, which currently does not exist for these types of investments.

[41] https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202005_1~3e9ac10eb1.en.html#toc2

[42] In order to address concerns that the multi-currency Libra Coin (LBR) could interfere with monetary sovereignty and monetary policy if the network reaches significant scale and a large volume of domestic payments are made in LBR, the Diem Association recently announced its intention for augmenting the Libra network by including single-currency stablecoins in addition to LBR, initially starting with some of the currencies in the proposed LBR basket (e.g., LibraUSD, LibraEUR, LibraGBP, LibraSGD).

[43] https://www.lloyds.com/news-and-risk-insight/press-releases/2020/02/lloyds-launches-new-cryptocurrency-wallet-insurance-solution-for-coin-cover

[44] https://www.eiopa.europa.eu/content/supervisory-technology-strategy_en

[45] See Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies, Publications Office of the European Union, Luxembourg, 2019 referring to Kavassalis, P., Stieber, H., Breymann, W., Saxton, K. and Gross, F. (2018), 'An innovative RegTech approach to financial risk monitoring and supervisory reporting', Journal of Risk Finance, Vol. 19 No. 1, pp. 39-55.

[46] E.g. some risks on private permissioned blockchain might be less relevant, but on the public permissionless blockchain the same risks may be more relevant.

[47] See in general World Bank Group. 2020. Smart Contract Technology and Financial Inclusion. Fintech Note; No. 6. World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/33723

[48] Schär: Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets 2020:18.

[49] https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf

[50] See e.g. https://www.coindesk.com/the-flash-loan-attacks-explained-for-everybody and https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137.

[51] See more on AML compliance and blockchain in World Bank Group. 2020. Smart Contract Technology and Financial Inclusion. Fintech Note; No. 6. World Bank, Washington, DC. https://openknowledge.worldbank.org/handle/10986/33723.

[52] See e.g. P. Paech, The Governance of Blockchain Financial Networks, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487 p. 1100. See also World Bank Group. 2020. Smart Contract Technology and Financial Inclusion. Fintech Note; No. 6. World Bank, Washington, DC. © World Bank. https://openknowledge.worldbank.org/handle/10986/33723.

[53] See EIOPA Discussion paper on (re)insurance value chain and new business models arising from digitalisation, 2020. https://www.eiopa.europa.eu/content/discussion-paper-reinsurance-value-chain-and-new-business-models-arising-digitalisation_en. See also proposal for a Regulation of the European Parliament and the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 - COM(2020)595. The proposal might help to mitigate some of the risks.

[54] Discussion Paper on open insurance: accessing and sharing insurance-related data, EIOPA 2021, https://www.eiopa.europa.eu/content/open-insurance-accessing-and-sharing-insurance-related-data_en.

[55] This could also entail certain risks, in particular in view of the numerous reported cases of security issues linked to social media accounts (e.g. hacking of social media profile, fake profiles etc.). Hence, eventually providers of social media providers could need to increase their security measures.

[56] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19–59).

[57] https://www.insuranceblockchainsandbox.com/

[58] Proposal for a Regulation of the European Parliament and of the Council on a Pilot Regime for market infrastructures based on distributed ledger technology - COM(2020)594

[59] http://www.efrag.org/News/Project-430/EFRAGs-Discussion-Paper-on-the-accounting-for-crypto-assets-liabilities---holder-and-issuer-perspective

[60] https://cdn.ifrs.org/-/media/feature/supporting-implementation/agenda-decisions/agenda-decision-compilations/agenda-decision-compilation-volume-1.pdf

[61] https://www.eiopa.europa.eu/content/guidelines-information-and-communication-technology-security-and-governance_en

[62] https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

EI-01-21-124-EN-C

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

Westhafenplatz 1,
60327 Frankfurt am Main, Germany

Publications Office
of the European Union

ISBN 978-92-9473-296-5