FEEDBACK STATEMENT

Discussion paper on blockchain and smart contracts in insurance

EIOPA-BoS-22-178
06 May 2022

eiopa

European Insurance and Occupational Pensions Authority

1. INTRODUCTION

Article 1(6) of the Regulation establishing the European Insurance and Occupational Pension Authority (EIOPA) (Regulation (EU) No 1094/2010) requires 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 EIOPA to monitor new and existing financial activities. The above is a key motivation underpinning EIOPAs work on digitalisation.

On 29 April 2021, EIOPA launched a public consultation on a "Discussion paper on blockchain and smart contracts in insurance" with the aim of providing a high-level overview of risks and benefits of blockchain and smart contracts in insurance from a supervisory perspective as well as to gather feedback from stakeholders.

EIOPA received responses from the industry, national and European industry associations, technology providers and academia.

A high-level summary of the responses received can be found in this feedback statement, together with EIOPA reactions. The full list of all the non-confidential comments provided can be found on the EIOPA public website.

EIOPA will consider the feedback in its on-going and future work on digitalisation, subject to prioritisation and EIOPA's work programme. Based on the feedback, the proposed follow-up work seems to remain generally valid.

EIOPA would like to thank all the participants to the public consultation for their comments on the Discussion Paper.

2. BLOCKCHAIN AND SMART CONTRACT USE CASES

2.1. USE CASES IN INSURANCE

Stakeholders noted insurers across the EU and beyond are currently developing blockchain and smart contract use cases across the insurance value chain to explore its potential to streamline business operations and to better serve consumers. However, blockchain and smart contract deployment in the EU seems to be still in the early stages. Many of the use cases are still small scale or in proof of concept (PoC) state. The feedback also indicated that often companies conduct PoCs to understand blockchain better and to build the required skills. Overall initial feedback based on PoC and use cases in the insurance sector seems to be positive and demonstrates blockchain´s potential as a technology that could benefit both customers and the industry. On the other hand, one stakeholder noted there seems to be few things blockchain can currently do better or more cost effective than other existing technologies. In his opinion, light adoption is expected in the mid-term, focused on niche players, products and business models. Use cases in industrial and transport insurance market seems to be more widespread than use cases for retail consumers. This might also explain why EIOPA did not receive any feedback from consumers.

In addition to use cases reported in EIOPA discussion paper, stakeholders referred to several additional use cases, actual or potential or PoCs, both in the EU and beyond.

Outside of the EU an industry-led consortium of property and casualty insurers have developed a blockchain-based system to streamline claims management and provide digital proof of insurance. Another use case outside of the EU mentioned was a mobile application with Artificial Intelligence capabilities to track all insurance policies on a single platform, allowing consumers to sign additional insurance contracts and to pay through a token issued by the platform.

As potential uses, stakeholders stated blockchain could reduce fraud, enable insurers, reinsurers, intermediaries and regulators to share data securely and in real time and give customers more control over their data, including access rights. More concretely, the following potential use cases were mentioned:

- The provision of blockchain-based marine cargo insurance certificates;
- Motor Third Party Liability Insurance (MTPL) claims clearance and processing (e.g. notification, proof of insurance, claims clearing, *Bonus-Malus* certification, etc.);

- Digitalising/managing risks pooling across the Europe (e.g. in case of terrorism or natural catastrophes[1]).
- Providing either a standard or a marketplace for reinsurance/co-insurance agreements;
- Use of blockchain in e-health (e.g. sharing documents between consumer, doctor and insurer; fraud mitigation);
- Traceability and certification of the vehicle's data during its entire life cycle;
- Providing a proof that the customer has read the documents (e.g. pre-contractual documents under the Insurance Distribution Directive), or even testing their understanding via a recorded and tamper-proof questionnaire (e.g. in the sale of unit-linked products);

Stakeholders also referred to different PoCs, often developed by national insurance associations and their members with the aim among others to learn more on blockchain. Among other following PoCs were mentioned:

- Use of blockchain and smart contracts for processing applications for private pensions with the aim to automate the whole process from application to payment;
- Blockchain-based digital platform with the aim to guarantee an efficient end-to-end issuance and management of parametric policies as well as to define the conditions under which it is possible to verify the claim and liquidate it automatically;
- Blockchain-based digital platform that allows the digitalization of both banks' and insurance companies' guarantees and enables an end-to-end full digital process management;
- Optimisation of the daily data exchanges between insurers in the context of requests for cancellation of car insurance policies;
- PoC on death insurance using national death register as an oracle and allowing the deaths of policyholders to be checked at regular intervals. When the death of the insured is noted, automatic compensation for the beneficiary(ies) of the contract could be triggered;
- PoC on connected lock aimed to link a physical object with a blockchain, so that smart contracts could interact with them to rent or lend the property and to explore how to issue risk coverage for this object.

Stakeholder also referred to national sandboxes dedicated to blockchain and agreed that blockchain could further facilitate the deployment of Peer-to-Peer (P2P) insurance. One stakeholder noted that an area that will require significant attention in the near future is Decentralized Finance (DeFi) which enables the creation of new insurance products and models.

[1] One stakeholder noted that Cat Bonds are easily digitised providing easier access to this market by guaranteeing the level of trust between players

2.2. USE CASES IN REGTECH AND SUPTECH

Stakeholders overall agreed there is a potential for blockchain to be used by supervisors to support their supervisory review process and make it more flexible and responsive (e.g. through automating regulatory reporting). Some stakeholders also noted that the key focus should be on solutions that lower the overall costs associated with regulatory compliance and supervision and reduce the burden for both the insurance industry and supervisors. Stakeholders also noted that blockchain can support RegTech solutions.

As for potential use cases, several stakeholders highlighted identity verification for Anti-Money Laundering (AML) / Know Your Customer (KYC) purposes as well as for fraud detection and prevention and processing of invoices via a blockchain.

However, it was also stated that real-time access to insurance company's data for supervisory purposes is difficult to achieve and creates many challenges from both the security and practical perspectives. One stakeholder also expressed view that real-time access to individual contract data does not seem consistent with the EU's supervisory principles. Additionally it was noted that despite the automation in the reporting requirements being a welcomed innovation, it is worth considering that the more the process is automated without proper quality checks the more difficult it becomes to spot any potential error related to the information submitted.

Stakeholders also stated there would also appear to be merit in exploring the potential for blockchain solutions to facilitate and further enhance the exchange of data between supervisory authorities.

3. RISKS AND OPPORTUNITIES

3.1. Risks

Most of the stakeholders agreed with the risks of Blockchain and smart contracts identified in the consultation paper, although it was highlighted that the risks would differ depending on the concrete use case and the contexts in which they are applied. It was also emphasized the importance of adequately training staff on IT and digitalization issues to reduce compliance risks and enable them to provide adequate information and advice to consumers. Enhancing the financial and technological education of consumers was also seen as a positive development that would limit the risks.

Cyber and operational IT risks were frequently mentioned by stakeholders, for instance as a result of an unauthorized access to the chain or the erroneous duplication of the chain. Indeed, protecting against potential errors in the code was seen as a key priority, given that in Blockchain and smart contracts "the code is law". The issue around the trustworthiness of oracles was not seen as a risk exclusively linked to Blockchain and smart contracts, given that third-party data providers are already used as a source of evidence in other contexts in insurance.

Moreover, it was also referred to the incipient evolution of quantum computing, which could eventually be able to break the encryption technology used in many financial applications like blockchain. The development of robust and trustworthy digital identity systems was recognised by stakeholders as a key enabler for reliable Blockchain and smart contracts in insurance.

Finally, specific reference was also made to the importance of carefully assessing the risks of Decentralised Autonomous Insurers (e.g. decentralised peer-to-peer insurance), for instance concerning possible liability or redress shortcomings that could arise from them. In this regard, some stakeholders considered that these entities should be included in the regulatory perimeter following an activity-based approach to regulation so as to ensure a level playing field and enhance consumer protection. One stakeholder also referred that certain industry consortiums could potentially distort competition.

3.2. Opportunities

Most of the stakeholders agreed with the benefits described in the consultation paper, although it was highlighted that they would depend on the concrete use case and that many of the opportunities have mostly not materialised yet given that it is still early days of this technology in

insurance. It was also highlighted that in order to be able to leverage the benefits, insurance undertakings would need to put in place adequate governance measures to mitigate the risks mentioned in the previous section. It was also pointed out that new benefits may arise as technology evolves, and also that similar benefits could potentially be obtained from other data-storing solutions not necessarily involving blockchain technology.

The benefits of Blockchain in terms of more secure and faster transactions, low operational costs, greater transparency and reliability of the data and improved traceability were seen as some of the most prominent ones by some stakeholders. Stakeholders also referred to faster claims handling process (e.g. with the use of parametric insurance contracts in natural disasters), lower loss adjustment costs (e.g. by leveraging on trusted oracles to automate pay-outs) and the absence of "loss creep" (due to predefined terms and conditions in the smart contract) which would lead greater certainty about reserving and capital requirements.

Some stakeholders highlighted the need to transparently communicate to consumers how their data is used (including requiring their explicit consent), also considering that information about consumers available in a ledger could eventually be used to offer them new products and services.

Some of the benefits mentioned in the consultation, such as supervisors and auditors leveraging on Blockchain technology to access real-time market data to develop their activities, were seen as not so likely to happen and even counterproductive, considering that it may require implementing significant changes to critical and complex IT infrastructures which could present a number of risks from an operational perspective. Other potential benefits such as the use of Blockchain technology in the context of open insurance were seen as a possibility but stakeholders considered that before assessing the use of the technology, the data standards should first be defined.

4. CRYPTO-ASSETS USE CASES IN INSURANCE

4.1. Different types of use cases in insurance

Respondents acknowledged that there are different types of crypto-asset use cases in insurance, which the consultation document broadly divided into three categories: payment-type, investment-type and utility-type.[2] As far as payment-type crypto-assets are concerned, respondents reported a number of cases, mostly outside the European Union where insurance undertakings where already accepting crypto-assets to pay insurance premiums and claim compensations. It was also reported the potential use of crypto-assets (and also possibly Central Bank Digital Currencies (CBDC)) in settlement related applications of payables and receivables that arise from smart contracts within a private permissioned blockchain network.

Concerning investment-type crypto-assets, respondents pointed towards certain insurance undertakings, again mainly outside Europe, that were directly investing in crypto-assets. Stakeholders also mentioned the case of national legislations of certain European Member States that specifically allowed such investments. Interestingly, it was also reported the case of a re-insurer that had established a blockchain system to issue a Cat Bond to six private investors (insurance-linked securities funds), reportedly circumventing like this the procedural constraints of traditional clearing houses. The tokenization of assets (and in particular utilities) such as renewable energies or real estate and the subsequent placement in the market of the relative "crypto-securitization" of such assets was also seen as a promising use case in insurance.

Fewer cases of utility-type crypto-assets were reported, although it was acknowledged their potential as an instrument to enhance customer engagement and to leverage the existent eco-systems and partnerships, including non-insurance service providers. One stakeholder considered that blockchain-based smart contracts such as crop insurance or flight delay insurance where the compensation payment is automatically triggered by a predefined threshold (e.g. amount of rain per square meter or delay of a flight) could be considered as utility-type crypto-assets.

Stakeholders also referred to the so-called Decentralised Finance (DEFI) business models in insurance, which reportedly do not involve entities developing activities similar to those of traditional insurance undertakings and intermediaries. Some of these DEFI business models make

[2] Payment-type often referred to as virtual currencies or 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 typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to shares, bonds or dividends); and utility-type typically enable access to a specific product or service but are not accepted as a means of payment. For example, in the context of cloud services, a token may be issued to facilitate access.

use of crypto-assets / tokens to represent membership rights, and/or tokens can also be used to purchase cover as well as to participate in claims assessment, risk assessment and governance of the DEFI platform.

From a different perspective, stakeholders also acknowledged that some insurance undertakings and DEFI propositions already offer insurance coverage for the loss or theft of crypto-assets. However, these are typically non-mass products and specifically addressed to provide insurance coverage to certain exchange platforms or custodial wallet providers of crypto-assets, or targeted to institutional investors or high net worth individuals. Respondents pointed out the difficulty of insuring risks related to crypto-assets given that the risks are still not well understood by the market. Stakeholders confirmed that existing cyber insurance policies usually exclude the theft or loss of crypto-assets, but they considered that these exclusions could eventually be removed in the future when there is a better understanding of the risk exposure.

4.2. Evolution of investments on crypto-assets

The majority of stakeholders that participated in the consultation considered that investments of crypto-assets by insurance undertakings will increase over the next 3 years. Amongst the drivers of this trend stakeholders referred to new regulations (e.g. MICA) providing greater legal certainty, the fact that crypto-assets are considered by some to be a convenient storage of value (e.g. like gold), a way to hedge against inflation and currency devaluation, or the demand by new digital native consumers. Their low correlation with other assets such as stocks, commodities or fixed income products, the possibility to diversify investment portfolios, and the greater certainty introduced by stablecoins and more particularly Central Banks Digital Currencies (CBDC) were also mentioned as factors that will drive investments upwards.

On the other hand, respondents also noted that certain aspects of crypto-assets could hinder the growth, such as the high volatility of some crypto-assets, their short maturity not necessarily adapted to the long-term vision of insurance, regulatory restrictions to the trading of crypto-assets introduced in some jurisdictions, or their high energy consumption. Some crypto-assets were also labelled by some stakeholders as assets that do not always have a very transparent performance, are subject to anti-money laundering and terrorist financing and cyber security issues. Indeed it was acknowledged that the risks of crypto-assets can be difficult to understand and can be therefore not suitable products for all type of consumers.

4.3. Benefits and risks of crypto-assets

The consultation paper outlined a number of challenges linked to crypto-assets with which respondents generally agreed upon, although it was highlighted the need to differentiate between different crypto-assets, use cases, and contexts in which they are implemented. For example, the case was made on the need to differentiate between marketing unit-linked life insurance products with exposure to crypto-assets to the mass market as opposed to a reduced number of experienced and knowledgeable consumers. It was also mentioned the importance of adequately train staff on IT and digitalization issues to reduce compliance risks and enable them to provide adequate advice to consumers. Operational risks, cyber risks and money laundering and terrorist financing risks were also often singled out as risks that need to be closely monitored.

Stakeholders generally also agreed with the benefits arising from crypto-assets, highlighting their potential to more efficient and cheaper transactions and provide a wider range of investment opportunities to consumers. Nevertheless some stakeholders also emphasized that the benefits are still potential and have not yet materialized, given that they are still at an early stage of development in the insurance industry.

4.4. Impact of MICA and regulation

Stakeholders that participated in the consultation largely believe that MICA will have a positive impact on the market of crypto-assets. They consider that MICA will improve consumer protection, bringing legal clarity and enhance trust in the market. Particularly for the insurance sector, it was mentioned that MICA will particularly favour the evolution of insurance and banking investment products (e.g. Unit and Index-Linked life insurance products). Another stakeholder noted that MICA provides the duty for crypto-services providers to set up own funds or, alternatively, underwrite an insurance policy, and thus leading to the growth of the crypto-insurance market.

Some stakeholders also had reservations and considered that it would depend on the final text of the Regulation, warning that too burdensome requirements could risk eliminating crypto-assets operators in Europe. With regards to the scope of MICA, it was pointed out that it was unclear how the Regulation would impact (if any) fully decentralized business model (DEFI), and also it was reportedly unclear which crypto-assets assets should be deemed a security/financial instrument. Two stakeholders considered that the insurance sector should be included in the scope of MICA.

Insurance undertakings nevertheless need to comply with the Solvency II Directive, which stakeholders noted that it has comprehensive asset-allocation prudential requirements, which would also cover investments on crypto-assets. Indeed some stakeholders considered that the Solvency II framework does not encourage diversification strategies involving crypto-assets, or even it was considered to be “very punitive” framework for these types of investments. Some

stakeholders also mentioned that the lack of clarity of the accounting and prudential treatment of crypto-assets could act as a barrier to the development of crypto-assets offerings in insurance.

Some respondents considered that it would be useful to clarify the accounting and prudential treatment of crypto-assets, in accordance with the other initiatives undertaken at European and international level, and highlighting the importance to distinguish between the different types crypto-assets and not to rely on a one-size-fit-all approach. The accounting definition of crypto-assets, the applicable accounting standards, the fair value of the asset in case it is not traded in deep and liquid market, how to calculate the 1-in-200 scenario for this kind of assets, and whether or not insurers should perform an overall assessment of the relevant risks developing new type of stress scenarios were mentioned as aspect that would benefit from greater regulatory clarity and convergence across Europe.

BARRIERS, CHALLENGES AND NEXT STEPS

EIOPA asked in its consultation about regulatory barriers in insurance and non-insurance regulation and adequacy of the current framework on addressing new risks, while also proposing possible follow-up actions. Most of the stakeholders agreed on barriers already highlighted by EIOPA, however some also stating that the barriers are not insurmountable.[3] Stakeholders also generally agreed on possible next steps, including the need for a coherent European approach to blockchain and smart contracts in insurance and common understanding of how existing rules should be applied in order to develop a more integrated and efficient European insurance market. This would help to facilitate cross-border business and guarantee a level playing field across different jurisdictions. Some stakeholders noted a coherent approach is not only needed for the insurance sector but for financial and other sectors. This could increase "digital trust" in general.

Stakeholders considered that the existing regulations like IDD, Solvency II Directive or GDPR, in combination with recently launched legislative initiatives such as MICA, DORA, AMLD 5, or the AI Act, would address most of the risks posed by the use of blockchain technology and smart contracts in insurance. However, stakeholders highlighted the importance of ensuring that the new legislative initiates are sufficiently "future proof" and do not create excessive burdens to business, especially SMEs (e.g. start-ups), when they bring added value to consumers. Overregulation should be avoided keeping in mind among others broader European competitiveness vis-à-vis other jurisdictions. In this regard, regulatory sandboxes were seen as a positive development by some stakeholders. One stakeholder did not agree with the proposal of amending the EIOPA Guidelines on ICT security and governance with the aim of taking into account the development in the use of blockchain and smart contracts stating that Guidelines should maintain their technological neutrality and principle-based nature to keep pace with the technological evolution.

Notwithstanding the above, certain refinements to the rules or guidance on how they would apply on certain contexts were also seen as potentially beneficial. For example, in addition to clarifying prudential and accounting treatment of crypto-assets (see section about crypto-assets), it was also suggested to develop guidance about the application of the GDPR in finance (e.g. application of GDPR's "right to be forgotten"). Stakeholder also pointed to other GDPR provisions where uncertain interpretation could hinder the implementation of blockchain systems. More specifically it was referred to (i) the anonymisation and encryption techniques to be adopted (e.g., if anonymisation

[3] Interestingly, some stakeholders noted that barriers highlighted in EIOPA paper only concern the use of smart contracts by incumbent/regulated insurance players and there are hardly any barriers when it comes to the use of smart contracts of decentralized public blockchains by consumers directly.

can fulfil the "erasure" of data for the purposes of Article 17 GDPR); (ii) the qualification of data controller (e.g., what kind of influence over the purposes and means of processing does qualify a subject as data controller); (iii) data minimisation and purpose limitation (e.g., whether storing the personal data off the chain does comply with the provision of data minimisation). Stakeholders also noted there is a lack of definitive guidance on whether nodes and miners are to be considered controllers or processors, which is why the accountability obligations under the GDPR cannot be clearly allocated. This in turn determines whether the participant needs a legal basis pursuant to Article 6 GDPR or an agreement pursuant to Art. 28(f) GDPR. Similarly, only controllers are responsible for fulfilling data subjects' rights.

Moreover, stakeholders also highlighted that regulations should always respect key supervisory principles such as technological neutrality and activity-based approach, bringing relevant actors in the insurance value chain inside the scope of the regulatory perimeter. Stakeholders also emphasized the need to prevent the creation of data oligopolies, for instance those arising from non-insurance providers in the context of the increasing use of sensors and the Internet of Things.

Several stakeholders considered that supervisors could engage in a dialogue with stakeholders in order to define open-source standards and protocols, for example in order to ensure more consistency at the data layer, and at the same time allowing differentiating innovation at the products layer. This would support the adoption of this technology by addressing several of the security and governance problems (e.g. common mistakes when programming) and remove existing obstacles. More concretely, it was proposed to follow the example of the legislative proposal for a pilot regime for market infrastructures based on distributed ledger technology[4], and develop a blueprint for a regulation of smart contracts and blockchain use cases in insurance. One stakeholder noted EIOPA should set up open-source standards and good practices in smart contract development and use, facilitating the identification of "approved" smart contracts by consumers and service providers and help integrate smart contracts within the current legal framework. Some stakeholders recommended to set up dedicated EIOPA expert group which would bring together supervisors, consumers, industry and public blockchain developers. The establishment of a working group could allow actors in the field to share their experiences, operations and bottlenecks as well as to understand risks and benefits better.

Moreover, stakeholders considered that potential regulatory initiatives should promote legal certainty and transparency and follow a technology neutral approach. It should also be innovation-friendly, learn from best practices adopted in other jurisdictions, and avoid establishing onerous requirements and new entry barriers. On the contrary, stakeholders considered that a flexible

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN

approach should be adopted, laying down principles and guidelines. It was also suggested to develop a standardised and dedicated Key Investor Information Document for smart contracts.

It was also suggested to promote supervisory and regulatory convergence at European and international level to avoid the creation of "offshore technology havens".

Many stakeholders mentioned possible barriers related to the insurance distribution rules (e.g. legal norms requiring paper records of transactions). Some stakeholders felt 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 (e.g. less complex or low monetary value products). Some stakeholders noted more generally the need of rethinking the whole transparency discipline, which should be more proportionate (taking into account the value and complexity of the products) and fit for the distribution in the digital age. With specific reference to Insurance Based Investment Products (IBIPs) that include crypto-assets, one stakeholder noted it should be considered also in the PRIIPs KID regulation in relation particularly to the performance scenarios and to the representation of the Reduction in Yield (RIY).

Stakeholders also referred to sustainability angle, given the massive energy consumption that some blockchain solutions could invoke.[5] Hence wider use of blockchain could counteract climate change mitigation effort and lead to conflicting regulatory imperatives. Some stakeholder also referred to EIOPA recent work on value for money, stated it would be interesting to consider the recently proposed ´value for money´ methodology and how it would interact with the analysis of this paper, in the context of POG and target market requirements.

Stakeholders also agreed there are still many compatibility issues with national civil law provisions. In particular, stakeholders referred to the smart contract interpretation in court, the algorithmic implementation of concept such as "best endeavours" and "bona fide", the possibility to withdraw a contract, the liability of the smart contract developer, and the possibility to amend the contractual conditions. Finally it was referred that in case that technology is provided, developed and/or hosted outside of the EU, the responsibility and liability must be clarified and there must be a right of access for relevant regulatory bodies.

Barriers that cannot be seen as directly related to regulation were also mentioned, including lack of knowledge and skills (both in the industry and in supervisory authorities) to understand blockchain opportunities and risks, organization culture, change management (perception and education), large investment needs and challenges related to cooperation when multiple parties are involved (especially in cross-border blockchain projects). Lack of a recognized standard to exchange technical

[5] The current standard process of transaction verification, based on the proof-of-work algorithm requires a huge amount of processing power, and, therefore, electricity, to run associated computer calculations.

and accounting data (e.g. in reinsurance) was also mentioned. Similarly, some stakeholders highlighted the importance of modern, high-speed communication infrastructure (high-speed interned and 5G networks) to ensure that data in blockchain applications can be synchronised without any delay.

On concrete PoCs (see previous chapter), stakeholders noted that in some cases market did not seem ready for specific solution, especially for solutions including crypto-assets (e.g. for payment). Often the economic cost of implementation was high which required a lot of volume[6] to make the PoC profitable. Sometimes the technology of blockchain as such was successfully implemented but it did not provide significant advantages over existing technology alternatives. Governance challenges were also highlighted. Finally, some solutions never went beyond the stage of a PoC, as it faced significant legal uncertainty regarding data protection legislation or insurance distribution rules. This highlights overall the importance of addressing barriers mentioned in this chapter.

One stakeholder recommended to repeat similar market monitoring exercise after some time, e.g after one or two years, as the blockchain and its practical application in the insurance sector is still in early stage. Related to that some stakeholders would welcome a broader definition of smart contracts and blockchain in future work, with important distinctions that can be drawn between the varied and nuanced implementations of this technology.

EIOPA'S FEEDBACK STATEMENT

- EIOPA notes that blockchain and smart contract use cases in insurance are still at an early stage.

- EIOPA noted in its Discussion Paper that there are a wide range of opportunities and challenges arising from the use of blockchain and smart contracts in insurance, which can vary depending on the concrete use case and context in which they are implemented, and hence they need to be assessed on a case-by-case basis. EIOPA will further consider additional opportunities and challenges highlighted by stakeholders during the consultation. EIOPA shares the concern on sustainability, given the massive energy consumption that some blockchain solutions could invoke.

[6] The benefits are often recognised only once volume and integration are achieved. Similarly, long sales cycle related enterprise software were mentioned.

- EIOPA will consider highlighted barriers in its different work streams as appropriate. EIOPA will also aim to share highlighted barriers and challenges with the European Commission and European Data Protection Supervisor.

- EIOPA will continue monitoring blockchain and smart contract use cases in insurance, barriers and related risks and benefits, including in its InsurTech Task Force. EIOPA will also continue to assess blockchain use in RegTech and SupTech as necessary. Potential area for further focus is Decentralised Finance (DeFi) and its extensions in insurance (DeIn).

- EIOPA notes that proportionality issues related to the POG and IPID could be considered further in the upcoming IDD review.

- EIOPA notes that in light of blockchain and smart contract developments closer cooperation is needed with supervisory authorities outside of insurance. EIOPA highlights that in response to the European Commission Call for Advice on Digital Finance the ESAs recommended for the Commission to consider possible ways to enhance cooperation between financial and other relevant authorities, building on existing cooperation models.

- EIOPA notes that there are different types of crypto-assets use cases in the insurance industry, although their level of adoption is still at an early stage. EIOPA would like to warn consumers that many crypto-assets are highly risky and speculative and are not suited for most retail consumers, as stated by recent warnings concerning crypto-assets of the European Supervisory Authorities (ESAs).[7][8][9] Consumers should be aware of the lack of protection available to them, especially insofar the upcoming MICA legislative proposal has still not entered into force. The environmental impact of some crypto-assets (namely those leveraging on Proof of Work consensus mechanism) is also a source of concern. Moreover, EIOPA also acknowledges that there are a number of initiatives from international standard-setting bodies such as the European Financial Reporting Advisory Group (EFRAG) or the Basel Committee on Banking Supervision (BCBS) assessing respectively the accounting and prudential treatment of crypto-assets. In cooperation with the European Commission and the other ESAs, EIOPA will continue monitoring market and regulatory developments and, where necessary, leverage on them to adopt any

[7] https://www.eiopa.europa.eu/document-library/consumer-warnings/warning-consumers-risks-of-crypto-assets_en

[8] https://www.eiopa.europa.eu/media/news/esas-warn-consumers-of-risks-buying-virtual-currencies_en

[9] https://www.eiopa.europa.eu/sites/default/files/publications/crypto-asset-risks-esa-update.pdf

measure on this area. The new Solvency II reporting framework that will enter into force in 2023 will also better capture crypto-assets related investments.

EIOPA

Westhafen Tower, Westhafenplatz 1
60327 Frankfurt – Germany
Tel. + 49 69-951119-20
info@eiopa.europa.eu
https://www.eiopa.europa.eu