IRSG

INSURANCE AND REINSURANCE STAKEHOLDER GROUP

Advice on blockchain and smart contracts

IRSG-21/31
29 July 2021

European Insurance and Occupational Pensions Authority

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?

As new technologies in general, blockchain lacks trust (partly because people may not fully understand blockchain technology). However, the insurance industry can offer one of the best environments for developing practical blockchain applications and increase trust towards blockchain when getting fully involved.

Insurers across Europe and beyond are working on developing blockchain initiatives and use cases to explore its potential to serve customers better. Initial feedback is positive and demonstrates its potential as a technology that could benefit both customers and the industry. It is important to ensure that this trend can continue effectively and that insurers are given time to explore the potential use cases and applications of the technology before regulators or policymakers consider any further steps. Any steps taken in the future should be based on a continuous dialogue between insurers and supervisors/regulators.

From a supervisory/customer perspective, DLT could become a true enabler in all those areas where regulators enforce either compulsory or regulated trading. As potential use cases, the following could emerge:

- Dealing with Motor TPL claims clearance & processing at market level (notification, proof of insurance, claims clearing, Bonus Malus certification, etc.)
- Managing the mandatory risks pooling across EEAA states (Terrorism, CAT etc.)
- Providing either a standard or a marketplace for reinsurance / co-insurance agreements and the clearance of the panel positions

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

The Blockchain Insurance Industry Initiative (mentioned in the paper): an important use case with high relevance for the insurance industry.

Streamlined international cross border claims handling: it creates efficient claims administration services across different operating entities/countries.

Challenges:

- Blockchain knowledge across the organization is still rather low so that business leaders don’t easily understand where and how blockchain can fulfil certain business requirements.

- Cross border blockchain projects require extensive alignment among involved entities if simultaneous go-live is involved.

Another domain for relevant DLT implementation is the placement and management of multinational risks for both Corporate Life (Employee's Benefits) and Non-Life (Multinational Programs) businesses, to reduce the friction in exchanging both technical and accounting data across the board and engaging with the network based on a single source of truth. The main challenges so far have been:

- Engagement with the intermediaries: this has proven difficult due to some conflict of interests (perceived disintermediation move of carriers, risk of reduction of service fees etc)

- Lack of a recognized standard to exchange technical and accounting data (Acord not being mature enough) to build interoperability across the network of companies (reinsurance risk transfers).

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.

Development of crypto assets use cases (early stages) in areas such as: (i) Cross border payment settlement for international insurance programs; (ii) Global liquidity netting practices; (iii) Digital securities. (iv) Tokenization of physical assets

Also, the solutions around identity management that has been growing into a large issue over the last couple of years, especially in the crypto space, will be a major change that will have larger reaching effects than just crypto as a trade-able asset. The anti-money laundering laws that exist are currently a bit of a pain point for crypto assets. This has led to solutions in the crypto space to try and simplify user identification. Meaning, that businesses that are dependent on AML rules can now have a fully auditable trail of customer information without having to verify it themselves. They just need to validate that the user they're interacting with has been validated by a trusted oracle of identity. This has the potential to be in effect in traditional banking, decentralized finance, as well as insurance. . https://www.kilt.io/wp-content/uploads/2020/01/KILT-White-Paper-v2020-Jan-15.pdf

A promising use case for insurance is related to the tokenization of Assets, such as in the Art sector or for specialized utilities such as renewable energies etc and the consequent placement on the market of the relative crypto-securitization of such assets. This, joined up with proper

identification/certification oracles and parametric/indexed valuations, could allow to greatly simplify trades and facilitate insurance backed trading markets

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.

Ethereum developer community (Etherisc) that develops different insurance-related blockchain applications have shown interest in this kind of application. New applications, as 1) crypto wallet insurance and 2) Collateral protection for crypto-backed loans, have been designed but their further use and marketing to retail or commercial clients is still to be actualized. See: : https://etherisc.com/#products

Moreover, Polkacover is marketing itself as the first DeFI (decentralized finance) insurance marketplace for the global crypto ecosystem. They are working with traditional insurers to create an online platform where insurance can be bought. See https://polkacover.com/index.html#platform

A rather extensive overview describing cases of insuring cryptos is provided by A. Zucherman, Insuring Crypto: The Birth of Digital Asset Insurance, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3756619

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

We expect insurers' investments in crypto assets to increase over the coming years; reasons being:

- The market for crypto assets (still immature today) is growing as new market entrants with a "digitally native" mindset will be open to offering assets (corporate debt, loans) in a "digitally native" manner.
- Access to crypto-assets has been and will further be eased, e.g., via investment vehicles.
- Regulation on markets in crypto assets (underway in many jurisdictions) will provide safeguards for investors.

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?

As it stands, MiCA is not clear enough on how fully decentralized public crypto assets will be regulated. Even if there are certain legal provisions concerning these crypto assets, there is no clarity on how the regulatory measures will be enforced in practice. In the case of Bitcoin, for instance, it is unclear where liability lies, whether with the miners, the people running the nodes (which often coincide with miners), the developers maintaining and updating the Bitcoin code, the wallet providers, or centralized platforms providing onboarding solutions to get into Bitcoin. It would seem that MiCA will only really affect centralized well-identified actors while skipping the issue of diffused liability for all other decentralized actors.

From an insurance standpoint, the EU commission should favor the evolution of insurance and banking investment products (e.g., Unit and Index-Linked) towards MiCa regulated solutions, in order to facilitate comparison, trading and standardization that in turn will lower commissions.

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?

As noted in the discussion paper, there is clear potential for blockchain to be used by supervisors to support their supervisory review process and make it more flexible and responsive. In this respect, the technology can be used to help facilitate both SupTech and RegTech solutions.

One area where the technology could offer great potential is in helping to automate regulatory reporting. This would help to make it more efficient and transparent for both supervisors and insurers while at the same time reducing the overall compliance costs for the industry.

When looking at different use cases in this area, the key focus should be on solutions that can lower the overall costs associated with regulatory compliance and supervision and reduce the burden for both the insurance industry and supervisors.

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.

Beyond the already mentioned use cases, worthwhile exploring the following areas:

- Contract certainty rules (proof of insurance, proof of privacy, proof of payment etc.) and key customer/product data publishing (e.g., unit-linked, index-linked product value assessment)
- international and domestic clearance houses, such as cross border tax payments, levies etc.

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.

The main area for development we have been faced with is related to the insulation and protection of customer data, which should be stored as a specific ledger completely owned by the customer himself, with access/enrichment being delegated to specific actors under the complete control of the customer himself.

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

We do not agree with systemic risk and money laundering risks as presented. When new technology emerges, it is always unsure whether the emerging technology should conform to an outdated system or whether it is the outdated system that needs to adapt to the new technology. Money laundering and systemic risk issues are directly linked to the way money is created under the existing system: via debt. Other monetary systems (such as a monetary system based on the Relative Theory of Money) do not have these problems or risks and can easily handle the emergence of crypto assets all the while addressing problems of money laundering and systemic risk.

10. Are there additional risks?

A new monopoly/oligopoly could be created when potentially disrupting the value chain via DLT (e.g., with oracle data). Therefore, regulatory bodies should endeavor to enforce open standards to maintain free market / lower barrier entrance.

Moreover, legal certainty and reliability in blockchains are strongly connected with the existence of a trustworthy system for digital identity: Individuals and undertakings must have verifiable digital identities. The lack of such a harmonized system is a risk. It is, therefore, crucial to relate to the ongoing work on EU- digital identity regulation.

Since identity is a very sensitive issue, any digital identity should replicate the attributes of “physical” identity documents, especially making sure that no authority can arbitrarily alter or delete a proof of identity, which is a fundamental right. Furthermore, to avoid any abuse, data theft or identity theft, any identity verification should be limited to YES/NO condition checks, with no data being shared with the third party. For instance, it is possible to create a smart contract that can only query a digital identity by checking for certain conditions like proof of residence (Is the person residing in a specific country? YES/NO) and age (Is the person above 18? YES/NO). This guarantees that no data is leaked to third parties while still guaranteeing that a user fulfils the conditions to access a service. The de-anonymisation of a user would require an official query from a judiciary authority.

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?

The regulatory and supervisory framework should be innovation- and digital-friendly, technologically neutral, and sufficiently future-proof to fit the digital age and encourage digital innovation. Therefore, an important starting point is to look at the existing framework and see where the rules may need to be adapted to meet these objectives and respond to digital developments.

Existing rules such as the GDPR, for example, can address many of the issues that may arise from the use of blockchain technologies, e.g., protection of personal data, ensuring accountability of companies, etc. However, certain well-established requirements of the GDPR create challenges and legal uncertainty (e.g., applying the right to be forgotten) in a blockchain context. They may limit the potential use of blockchain technology where companies fear falling foul of the rules. Therefore, it would be worth looking at areas such as this to see if further guidance may be necessary regarding the application of the GDPR to the use of new technologies in financial services.

In the context of smart contracts, the current regulatory and supervisory framework for the insurance sector should continue to be sufficient. Existing conduct of business requirements, for example, would continue to apply as they are intended to be technology-neutral and should therefore be equally fit for smart contracts.

Regarding private blockchains, there are many ways to mitigate risks that can be addressed with current regulation or new regulation. However, it is implausible that any regulation will address risks emerging from public blockchains since there is no clear way to enforce these regulations. Furthermore, there is no example, at present, of a country having successfully influenced the protocols or governance of public blockchains via regulation. Thus, the only impact of regulation so far is to restrict or ban the emergence of centralized public intermediaries (such as exchanges), facilitating the interaction and engagement of citizens with public blockchains.

New risks emerging from public blockchains should be addressed by developing a common open-source body of resources and know-how for public blockchain developers to have all the tools at their disposal to address the risks identified and avoid making common mistakes in their programming. In addition, supervisory authorities should set up special working groups which include public blockchain developers from prominent existing public blockchains which might be used for insurance and/or financial products (Ethereum, Cardano, Solana, etc.), organizations engaged in developing standards such as Consensys, and key stakeholders representing the interests of consumers and incumbent business players to facilitate interoperability and take-up of these new solutions by incumbents, and interface directly with consumer organizations to prevent certain risks. Up until now, there has been no cooperation or engagement between regulators and public blockchain developers.

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

The benefits have been well identified. The use of blockchain technologies offers advantages in terms of more secure and faster transactions, low operational costs, greater transparency and reliability of the data and improved traceability. This carries great potential to make a significant different for insurers in terms of increasing trust, reducing costs, detecting fraud, making payments more efficient, and managing and storing customer data.

13. Are there additional benefits?

Public blockchain solutions might help blur the line between "consumer" and "service provider" since consumers can engage in various ways in public blockchain products and public governance. For instance, consumers can help secure the network (via staking a token, for instance, as in Ethereum, thereby supporting smart contract execution), or become decentralized oracles (like Augur), decentralized escrow service providers, or decentralized mediators in case of conflict between a consumer and a public blockchain protocol or another intermediary. In the future, consumers can at the same time be users of a public blockchain and service providers of that same service by helping maintain the protocol or engaging directly with the protocol.

The smarter and more open while protected use of data will potentially disclose the access to new products and services beyond the pure insurance coverage, as the customer could be offered advice in stronger relation to their unexpressed needs, simply by showing them the risk context to which they are exposed based on the ledger data they are making available. In addition, data enrichment and data augmentation on top of native customer data could be used to counsel customers on various add-on solutions to improve their risk position and better decide on how to deal with external factors.

14. What can be done to maximise these benefits?

Make sure public authorities and supervisors come to terms with the unique nature of public blockchains and the limits of traditional regulatory approaches to addressing certain risks, which should lead to the emergence of a more open approach, with the set-up of systematic dialogue and exchange with developers of public blockchains to help bring about common standards and approaches in coding and launching public blockchains, with most security and public governance problems addressed immediately. Foster the development of a healthy eco-system of public

blockchains, with all the necessary resources and tools to help emerging projects develop, for instance, by providing free auditing services and technical advice.

Promote and maintain a very open data exchange standard for the industry value chain (mirroring what has happened with the GSM standards in the mobile space) so that more and more players could access the DLT and contribute to its development.

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

Yes, but these barriers only concern the use of smart contracts by incumbent insurance players. There are hardly any barriers when it comes to the use of smart contracts of decentralized public blockchains by consumers directly. For instance, any consumer can freely install non-custodial wallets such as Argent on their smartphone and interact with various smart contracts with no KYC process. There is no way to stop this from a regulatory perspective, just like there is no way to stop distributing open-source software like Tor (which helps keep your Internet connection private and anonymous).

Furthermore, even if RegT and SupT should embrace and improve the guidance brought forward by mass adoption of technology (e.g., Bitcoin), that typically contribute to set the global standards. Incremental compliance should be adopted instead of complex, comprehensive issuance of large bodies of supervision.

16. What additional regulatory barriers do you see?

a) in EU insurance legislation.

b) in EU non-insurance legislation.

It will be crucial to ensure that the application of EU privacy and data protection rules does not create unnecessary barriers to the deployment of blockchain technology solutions in the financial sector. The underlying principles of blockchain technology already raise certain questions regarding compatibility with existing legislation. The GDPR, for example, sets out numerous rights for the data subject, such as the right to be forgotten and the right to rectification, as well as requiring data to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. This needs to be reconciled with the fact that blockchain technology is designed to be an immutable and permanent record of all transactions.

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

Regulatory uncertainty on which digital assets should be deemed a security/financial instrument could prevent insurers from using crypto assets. On the other hand, a non-regulatory barrier is perhaps the lack of loss history of insured crypto assets.

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?

There would seem to be a need for a coherent European approach to blockchain and smart contracts and a common understanding of how existing rules should be applied.

One of the crucial factors for the successful deployment of blockchain solutions will be to have continued cooperation between all the different stakeholders to avoid obstacles arising from standardisation or interoperability issues. It will also be crucial to ensure that the application of EU privacy and data protection rules does not create unnecessary barriers to deploying blockchain technology solutions in the financial sector. Furthermore, insurers also need legal certainty regarding implementing their own use cases without facing any unnecessary obstacles. Therefore, it would be important that that data protection authorities help facilitate the uptake of blockchain solutions by developing opinions or clarifications that provide companies with reasonable legal certainty regarding the use of such technologies.

Any approach must uphold neutrality in relation to different technologies. It is also key to ensure a balance between innovation and the proper protection of consumers. Legislation on consumer protection should probably create sufficient safety for consumers in blockchain/smart contracts contexts. However, this needs to be further monitored. A coherent approach could also be necessary to guarantee a level playing field across different countries and jurisdictions. This approach could consist of harmonizing the rules on regulatory sandboxes to avoid differences between the Member States. However, the harmonization must be consistent with the primary objective of European insurance regulation, which is the protection of customers.

Furthermore, EIOPA and other public authorities need to set out the conditions for official legal recognition of smart contract effects. For instance, under which conditions should a smart contract executing the transfer of ownership of a car be recognized by public authorities? In addition, 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. Finally, some standards are also needed to address how the legal system can “reverse” a smart contract execution, for instance, by

making two or more parties set up a new smart contract that restores the original situation to the extent possible.

Lastly, specific areas where EIOPA could introduce and nurture the development of BCH are the creation of Industry standards (e.g. for risk exchange) and the institution of key oracles (KYC, AML…).

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?

These follow up actions do not mention the set-up of a dedicated working group at EIOPA which would bring together consumers, business representatives and public blockchain developers.