International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. X, Issue 6, June 2022

http://ijecm.co.uk/

DIGITAL DISRUPTION OF THE INSURANCE INDUSTRY IN EUROPE: THE INCUMBENTS PERSPECTIVE

Aidan Duane
South East Technological University (SETU), Waterford City, Ireland
Aidan.Duane@setu.ie

Abstract

For years now, academics, researchers, and industry consultants have proclaimed the impending digital disruption of the insurance industry by a raft of start-ups equipped with new and emerging technologies in Analytics, Blockchain, Open APIs, Artificial Intelligence, etc. But what do the incumbent insurance industry business leaders think of these assertions? Is it just hype or is the industry on the brink of monumental change? This paper discusses key insights emerging from a series of interviews with senior business managers in the insurance industry often described as dominated by entrenched traditional incumbents but primed for digital disruption by new entrants. The findings emphasise the increasing threat of cyber-attacks as digitalisation increases, the challenges of digital customer service, the impact of the different national and international regulatory and compliance environments on digitalisation initiatives and indeed new market entrants, and the opportunities for digital disruptors to become digital partners with incumbents.

Keywords: Insurance industry, digital disruption, blockchain, smart contracts, machine learning, artificial intelligence

INTRODUCTION

According to Gartner (2020), digitalization is "the use of digital technologies to transform a business model and create new revenue and value opportunities; it is the process of moving to a digital business". Schmidt (2018) contends that a fourth industrial revolution in technology such as cloud computing, telematics, the Internet of Things (IoT), mobile phones, blockchain technology, artificial intelligence/cognitive computing, and predictive modelling is transforming

the entire insurance business model, enabling new ways of communicating, information sharing, and insuring. Similarly, multiple commercial reports contend that emerging technologies are disrupting the insurance industry and creating new forms of competition including Insurance-as-a-Service models (Cognizant, 2017; Deloitte, 2017; Gartner, 2017; OECD, 2017; PWC, 2018; KPMG, 2019). Digital technology is claimed to be moving up the value chain and increasingly used in risk analysis as insurance CEOs realize greater returns from digital technologies by embedding them in their decision making processes (PWC, 2018). Capiello (2020) describes how digital transformation is "greatly affecting the insurance industry and forcing radical change upon corporate culture, products and processes, customer relationships and relations with the sector's various competitors". Thus, we read grandiose claims that insurers are putting innovation front and centre, taking full advantage of emerging technologies and that those who do will be the winners in an era of constant changing customer demand for even more dynamic digital products (PWC, 2018).

Academics refer to this subdivision of FinTech as InsurTech (OECD, 2017; Nicoletti 2017; Chishti & Barberis 2016; Mackenzie 2015; Baumann, 2018; Chester et al., 2018). The OECD assert that "InsurTech, as compared to FinTech, is more often related to service improvements for individuals, as opposed to businesses". InsurTech has attracted large venture capital investments, and the trend of financing indicates that many start-ups are considered by investors to be commercially viable on a mass-scaled basis (OECD, 2017).

The OECD (2017) catalogues relevant technologies that are being viewed as having the potential to bring innovation to the insurance sector including blockchain technology, robo-advisors and data aggregation while also emphasising the role of start-ups, incumbent engagement with start-ups, the sharing economy, compliance and regulation. Eling and Lehmann (2018) identify three broad categories of how InsurTech is transforming the insurance industry: (1) new technologies change the way insurers and customers interact (e.g. social media, chat-bots and robo-advisors); (2) new technologies can be used to automate, standardise and improve the effectiveness and efficiency of business processes (e.g. online sales and digital claims settlements); (3) new technologies create opportunities to modify existing products (e.g. telemetric insurance) and develop new ones (e.g. cyber insurance). Such is the power of InsurTech, Albrecher et al. (2019) argue that unrestrained digitalisation is sweeping over insurance companies, compelling radical change of culture, products and processes, customer relations and relations with the sector's various competitors.

One technology in particular has been hailed as an industry messiah. For many years now, blockchain has been touted as a force multiplier for organizations seeking to restructure operations and overturn outdated business models across industries. Similarly, blockchain

enabled smart contracts have been advocated for many years as time and money savers with immutable audit trails. By allowing policy holders and insurers to track and manage physical assets digitally, smart contracts codify business rules, automate claims processing, and provide a permanent audit trail offering insurers significant savings in operating costs and lower their operating ratio (Cognizant, 2017). Thus, it has been lauded as a means to streamline how insurance companies operate and interact with the numerous stakeholders across the industry value chain including agents/brokers, third-party administrators, vendors, government agencies, third-party data providers, reinsurers and customers. It has also been claimed that blockchain will enable entirely new disruptive business models, such as peer-to-peer insurance and either eliminate or challenge entrenched intermediaries. It is suggested that insurers will find themselves shifting from a traditional paradigm of data ownership to sharing data in distributed networks with external partners and stakeholders for mutual benefit (Cognizant, 2017). Furthermore, big claims have been made for several years, that for insurers looking to tackle inhouse challenges such as poor customer experience, costly manual administrative processes, and privacy and data security risks, blockchain may well be part of the solution (KPMG, 2019).

While blockchain is often touted as a mechanism for storing all sorts of data, some authors have suggested it is not a viable option for such an activity as it would be prohibitively costly and inefficient (Davies, 2019; Harrison, 2019). Furthermore, some insurance industry experts argue that public blockchains, where all parties have access to every transaction on the ledger, are not feasible for the insurance industry due to privacy and security concerns (Heath, 2019). Hybrid blockchains, that is, a permissioned blockchain integrated with a public blockchain, have been touted as solutions replacing the need for traditional databases (Mearian, 2019), though the technology is considered nascent and at least 5-8 years from any fully secure commercial application. Some experts predict this will never happen (Martin, 2019).

But what do the incumbent insurance industry business leaders think of these assertions and predictions? Do the incumbent business leaders believe that their industry is on the brink of monumental change driven by technological disruption? What is the current state of technology in the ‘traditional’ insurance industry? Are the incumbents investing in the same emerging technologies often touted as the secret toolkit of new entrants, digital start-ups, and digital disruptors, to smash down barriers to market entry. More specifically, which technologies and digital processes do the incumbent business leaders consider to be of merit, warranting attention and perhaps potentially creating opportunities for partnerships and associations rather than direct market competition. According to the OECD (2017), an important development to consider is “how the insurance sector responds to economical and society-wide technological innovations, and provides insurance processes and policies that integrate such changes”.

The following sections discuss key insights emerging from a series of interviews with senior business managers in the European insurance industry often described as dominated by entrenched traditional incumbents but primed for digital disruption by new entrants.

MATERIAL AND METHOD

Qualitative research provides a researcher with an opportunity to gather rich and valuable descriptions of a broader environmental spectrum of interest. Descriptive qualitative studies are used to build rich descriptions of complex circumstances that are under explored in extant literature. Descriptive qualitative research provides first-hand experience of the research environment in action, enabling findings to be interpreted in context (Marshall & Rossman, 1999; Guba & Lincoln, 1994; Duane & Finnegan, 2004).

Over a nine-month period between March and November 2020, fifteen representatives from eight different organisations immersed in the Insurance Industry across Europe were interviewed. Semi-structured in-depth interviews were used to gain an understanding of management perceptions (Duane & Finnegan, 2007) of digital disruption of the insurance industry in Europe. These representatives performed a variety of roles in their organisations including Chief Information Officer, Head of Digital, Chief Underwriting Officer, Claims Manager, Chief Operating Officer, Blockchain Economy Advisor, Cryptocurrency Advisor, Director of Strategic Alliances, Pre-Sales Engineer, Global Head of Industry, and Head of Insurance EMEA. Arising from the literature, the discussion focuses on seven thematic areas:

i. Technology in the Industry
ii. IT Architectures
iii. Data Management
iv. Machine Learning and Artificial Intelligence
v. Open Application Programming Interfaces
vi. Blockchain
vii. Crytpocurrencies

While the original intention was to speak with more individuals, the realities of COVID-19 and the discipline of firms to focus solely on high priority initiatives during this significantly challenging period, meant that engaging more organisations was not possible within the research timeframe.

Technology in the Industry

All respondents agree that technology should have a major role in reducing costs in their business and that they should invest more, and one interviewee went so far as to suggest that a

deeper understanding of how customers engage with their website would lead to even further streamlining and savings. In general, respondents indicated that paper processes were unnecessarily significant in their businesses, although efforts in recent years did reduce the *footprint* of printers within their offices. One of the main sore spots is postage costs, as it is challenging to get customers to opt for email-only delivery of policy documents and related correspondence. Contributing factors to major inefficiencies across the industry include manual keying, the lack of digital self-service capabilities for customers, elongated process chains, duplicative touchpoints with customers, and the fact that digital originations of customer policies are in the minority rather than the majority. One respondent suggests that if they were able to automate the registration and settlement processes up to a certain level, for example, €1,000, that would result in significant efficiencies for their business.

In terms of the kinds of specific technologies mentioned by respondents that will enable disruption and transformation, artificial intelligence, machine learning, deep learning, blockchain, drones and IoT all have significant potential. The increasing usage of these technologies will expectedly reduce the cost of providing insurance, and should, in effect, lower the barriers to entry. What may fuel the increasing adoption of these technologies by incumbents is a new player coming from the outside and disrupting the status quo. Two of the respondents referred specifically to the Lemonade model as a good example of what could work well in the insurance industry. Lemonade is an online insurance company deployed through iOS and Android apps heavily vested in AI bots, trading in the Netherlands, France, Germany and the US[1]. Others to watch out for are Tesla moving up the actuarial curve with their capabilities and Revolut[2] as an insurance broker. However, one respondent noted that technology for technology's sake was not the answer, as the effort should be balanced with priorities, and the priorities will differ based on the view of internal stakeholders. For example, the Head of Marketing will always prioritise UX (User Experience), and the Head of Underwriting will always prioritise AI-themed investments for risk profiling.

Although respondents thought that agile and innovative tech start-ups that could give the customer what they want quicker such as Lemonade, were a competitive threat, existing and pending regulation raised the barrier to entry considerably. One of the key barriers to entry for new insurance players is the high claims cost, especially for motor insurance, which makes it challenging to achieve a sustainable return on investment. One respondent noted that the insurance industry is currently in a cycle where policies are rather inexpensive, and the "*lowest in a decade without many undercut threats*". With the typical model of InsurTechs paying small

[1] https://www.lemonade.com
[2] https://www.revolut.com

claims in seconds, all respondents thought that this was also possible in the near-to-medium term for larger incumbent insurers. It is envisaged that claims below a certain threshold could be paid instantly using new technologies such as AI. However, it is possible that the deployment of such utilities for enhanced claim processing may initially lead to an increase in fraud unless insurers develop new tools to better detect fraud. One respondent noted the 80/20 rule, for example, 80% of the claims is where the least amount of human effort should be, and claims can be paid automatically within seconds/minutes up to a certain threshold.

One area that is open for new players is for those willing to underwrite cyber risks, as players offering these kinds of policies are hard to come by. An olive-branch approach of potential technology white labelling and collaboration opportunities with incumbents also exists for any potential industry digital disruptors. Thus, some understanding of current IT architectures and data management is important.

IT Architectures

European insurers tend to use a mix of in-house, intra-group and outsourced IT operations, with the size and scale of their IT operations driven by the shape of their business in each country. Native insurers tend to base the majority of their IT operations in their source location but may also outsource strategically due to cost and business continuity drivers, and those outsourcing locations may be in other European countries. Insurers with native international roots tend to rely on intra-group shared services, so they may have their IT operations working together from multiple sites internationally. In terms of data centres, insurers are using a mix of cloud-based and on-premises services, with cloud services primarily provided by Amazon Web Services (AWS) and Microsoft Azure (Azure).

Business-critical systems include their mainframe systems, with one insurer referring to their IBM AS400 mainframe, along with their policy pricing software for personal lines (any kind of insurance that covers individuals against loss that results from death, injury, or loss of property). As a sign of the times with the ongoing COVID-19 pandemic, one insurer referred to how their Virtual Private Network (VPN) and Work-from-Home (WFH) technology frameworks had become business-critical systems.

In terms of software, most are ‘Microsoft Houses’ and use considerable amounts of third-party software, with any proprietary software leveraging Oracle and Java. One insurer specifically mentioned their increasing use of APIs to connect with third parties, so in-house development support is required to connect third-party APIs to their in-house systems. In general, for ‘commodity’ type software, most insurers use third party software but will develop

in-house for some strategic efforts or where it's more efficient or effective to develop and maintain the software internally (i.e.) light system interconnectivity and interfaces.

Network security is managed both in-house and by third parties, some nearshore, with some offshore and further afield, and one insurer specifically refers to their relationship with Accenture and their 'Managed Security' service[3]. Network security is a business-critical process as well, with stringent standards and ISO 27002[4] and/or SOC2[5] requirements for third parties connecting to their systems.

Data Management

For data collection, insurers are using a mix of phone, postal, email and online capture of customer information, depending on the channel. As the collection of customer information is heavily regulated with the General Data Protection Regulation (GDPR)[6] and Know Your Customer (KYC) requirements, insurers tend to use a mix of in-house and third-party Document Management (DM) and Customer Relationship Management (CRM) solutions to track and store customer information. These hybrid solutions are in contrast to the technology solutions of FinTech and RegTech new entrants focused on KYC services, as the insurance industry has been slow to adapt to new technology, according to several respondents.

Most insurers are still in 'early days' mode for leveraging newer data analytics tools within their business, with respondents referring specifically to their use of Google Analytics and Hotjar for tracking web traffic and user experiences, and SaaS (software as a service) tools such as Qlikview and ClixSense for analysing web traffic.

In terms of sourcing third party market data, insurers are doing this, but need to be careful with the amount of customer data they source and track due to regulatory restrictions. For example, one respondent referred to the mandated restriction on offering current customers preferential policy pricing terms compared to those offered to new customers. This means that if an insurer has collected significant amounts of data on a customer over the course of a 5-year relationship with annual renewals, they cannot use this data to put their existing customer in an advantageous position vis-à-vis new customers for whom they have no historical data. Thus, regulations somewhat undermine data potential.

In terms of predictive analytics, this is a key part of policy pricing, as the actuarial engines consider the likelihood of a loss while pricing a policy, which is inherently 'predictive' in nature. However, the usage of newer predictive analytics tools enabled by machine learning and

[3] https://www.accenture.com/us-en/services/security/managed-security
[4] https://www.iso.org/standard/54533.html
[5] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html
[6] https://gdpr-info.eu/

artificial intelligence is not prevalent with insurers. This will be discussed in more detail in the next section.

Overall, there was a general trend towards 'it's not the data, it's how you use it' with respondents suggesting that significant amounts of useful data sets are readily available to insurers today, but if you are not prepared (or allowed) to use that today to form useful insights due to restrictions or regulation, there is no point in sourcing or storing that data.

Machine Learning and Artificial Intelligence

In general, comments such as "*we are at the start of the journey*" and "*it could take 3-5 years to see some traction*" were the norm when it comes to Machine Learning (ML) and Artificial Intelligence (AI). However, there is some leveraging of ML and AI with underwriting and claims processing which drives the majority of the business case. One respondent noted two ongoing efforts – one with pricing policies using ML and another effort using AI to validate customer documents in real-time.

In terms of the potential for AI-enabled bots, all respondents saw this as an area of significant interest. The general view is to focus on AI-enabled customer support first, then document reading and processing, and then switching services. The consensus is that most consumers are underinsured, so developments that make it easier for consumers to access protection will ultimately be a new (or added) source of revenue for insurers. According to one respondent "*the current incantation of bots, however, does leave a bit to be desired by the customer, as they're not usually fuelled by customer data. For example, it is a lot more likely that a support bot will tell you how to contact a customer support representative than share your 5-year claims history with you*". Thus, it's not entirely surprising that most of the respondents acknowledge that overall, customer engagement is low. One respondent remarked, "*I think the first challenge is to engage more with the consumers and listen to them - not just at the time of renewal, or at the time of claims payment*".

However, there was also evidence with some respondents that AI was sometimes conflated with pure automation, as there are significant ongoing efforts across the insurance industry to increase the level of automation and reduce manual processing. One respondent noted that "*it's already there*", but was referring to the reduction in manual processes, pure automation and enhancing the customer experience rather than algorithmically enhanced machine learning and neural networks underlying current confusion in some quarters.

All respondents thought that AI would bring benefit to their businesses, but as the insurance industry was behind the curve of technological advancement vis-à-vis other industries it was still early days. According to one respondent, if "*bots can reach the level of providing*

customers with insight into an over-insured or -under-insured situation, that would be a very positive outcome for incumbents. In addition to driving more frequent and effective customer engagement, such a solution would also remove policy overpricing and lead to risk being priced more appropriately". Combining "*bots with Open Insurance data, however, would be a game-changer*", according to one respondent. The role of AI in Blockchain Smart Contracts is also suggested as a key enabler for settlement automation for low value contracts which could dramatically cut costs according to several respondents.

Open Application Programming Interfaces (APIs)

The respondents had differing thoughts on Open Application Programming Interfaces (APIs), with the split driven by insurers' use of APIs within their business currently. Respondents think that the integration of APIs should be done with careful consideration of the overall IT architecture, or else insurers would only add to their own technical debt. One respondent comments that "*the pace of technological change in insurance mimics that of the customer needs*".

One respondent thought that the openness of insurers to integrate Open APIs would be driven by the point of origin of the API. For example, was an insurance company integrating with an Open Banking API, or was a bank integrating with an Open Insurance API? The respondent thought that this would make a difference as to how widespread Open API usage would become across the financial sector, as both the customer benefit and the insurer benefit need to be weighed up. Thus, it is possible that the emergence of an Open Insurance initiative modelled after Open Banking will increase competition within the insurance industry. In the same way that new banking players are leveraging customers' Open Banking data across their multiple bank accounts to propose financial products, new insurance players would be able to do the same by accessing customers' Open Insurance data. Also, new technology only players such as Alternative Information Service Providers (AISP) under the PSD2 initiative for Open Banking, may result from an Open Insurance initiative.

However, while many potential disruptors view Open Banking and Open Insurance negatively for incumbents, such an outcome is deemed positive by respondents. The respondents assert that the access they have to their customers' data across insurance providers under Open Insurance would be significantly beneficial to their underwriting and claims processes. One of the main insights on Open Insurance provided by one respondent, "*is the opportunity to fuel bots with the context of standardised customer data flows, in the same way some players have done with Open Banking*". However, Open Insurance data flows are not expected to be a reality in the short-term.

Blockchain

One respondent captures the general consensus that with the exception of blockchain in commercial insurance for cargo and marine insurance, for blockchain technologies to "*be implemented in insurance in a way that takes advantage of the core benefits of distributed ledger technology, the market requires a tipping point of acceptance first*". However, there is also a concrete consensus that two of the most relevant use cases for blockchain technology in the insurance industry is with digital identity and the related data sharing context, and AI enabled smart contracts built on blockchain technology to automate verification of the transactional process elements.

If a consumer owns all of their identity data and grants access to it to other parties, including insurance companies, banks, social services and government through APIs, insurers get a complete view of the individual. Blockchain can enable a framework where data usually stored by these entities can be shared with the individual's consent, without revealing the identity of the individual, and this is a powerful proposition. In essence, AI could value, interpret, recognise and make decisions while blockchain can verify, execute and register. However, these kinds of data exchanges need to be regulated, and while we have GDPR, it is not yet sufficient to enable the full deployment of blockchain-enabled digital identity solutions for individuals.

Identity Management on the Blockchain

All of the respondents had interesting contributions on using blockchain for identity management, and the resulting themes largely pointed to a consensus that it's technically possible, although possibly a bit early and likely not advisable with the current maturity of digital identity frameworks in the blockchain 'arms race'. Thoughts expressed included:

i. Onboarding customers today using KYC data from a decentralised database shared across competitors is not likely possible from a regulatory perspective – the service provider may still need to replicate the independent verification of identity documents in most regulated financial services sectors in most countries.
ii. Digital identity enables far easier switching for consumers, and insurers may prefer not to enable easy switching.
iii. There have been some early steps with digital identity frameworks with the leading blockchain protocols such as Hyperledger Indy, but most of the projects are focusing on B2B solutions rather than B2C.

iv. Furthermore, most respondents thought that more basic solutions were available rather than a DAPP, and one respondent felt that putting any identity information, even as just a hash corresponding to an off-chain database, was a bad idea.

Smart Contracts and Trusted Oracles

In terms of commercial examples of smart contract frameworks, respondents point to cryptocurrencies such as USDC and USDT/Tether, and any other deployment of ERC20 token-linked smart contracts in cryptocurrency exchanges and decentralised finance (DeFi) protocols, Insurwave[7] and the ClydeCode[8] initiative. However, with regards to the legal view of smart contracts, the consensus is that "*the code is not the law*", and that an overarching legal agreement is necessary to back the smart contracts. There is a significant difference between smart contracts, which one respondent refers to as "*dumb programs*", and smart legal contracts. According to one in-house legal expert, "*the idea is that there needs to be an overarching legal agreement that governs the transaction. This can come in the two following ways: 1. A smart legal contract that specifically incorporates the code, and/or 2. A platform level agreement. However, we do not have anything specific with regards to an analysis of legally binding contracts*".

On how potential digital disruptors are dealing with these issues, respondents provided examples such as Colony[9], Nexus Mutual, cryptocurrency exchanges, and a recent effort to pull together some thoughts on this by Clifford Chance (2017), R3[10], the Singapore Academy of Law (2020), and ISDA (2019). However, there was no clear strategy common to digital disruptors for navigating smart contract enforcement from a legal perspective.

Regardless of the current level of maturity of smart contracts from a legal perspective, all respondents felt that lawyers would be needed to program smart contracts if they were to become legally enforceable without the safety net of an overarching legal agreement and that start-ups were going in this direction (hiring legal experts).

For commercial implementations of smart contract linked payments, some of the respondents are taking a deeper look at Lemonade's framework using smart contracts, Nexus Mutual and the integration of Corda Settler with Corda-based networks which will eventually be surpassed by a Corda Payments SDK that is currently in development at R3 to integrate with existing payment rails.

[7] https://insurwave.com/
[8] https://www.clydeco.com/en
[9] https://colony.io/
[10] https://www.r3.com/

On the topic of using Oracles, such as Chainlink[11], as trusted data sources for smart contracts, the consensus among respondents is that trust is the key word. For example, in the financial markets, Thomson Reuters[12] is a trusted name and financial market participants will likely trust an Oracle operated by Thomson Reuters to provide data to smart contracts. In any financial services geared proposal leveraging Oracles, when assessing the viability of different Oracles, trust in the name behind the Oracle will likely outweigh the confidence that a blockchain-powered network might have in the manner in which the Oracle collects its data. Overall, the respondents expressed a common view that while some initial work in the Oracle space has been impressive, especially the frameworks of Chainlink (as used by Nexus Mutual[13]), it is still early days for wider commercial acceptance. Furthermore, use of Oracles or indeed any other form of trusted third parties is largely dependent on choices regarding Public, Private, Consortium and Hybrid Blockchain Models.

Public, Private, Hybrid and Consortium Blockchain Models

Looking at the insurance industry specifically, although Ethereum had been leveraged historically for financial services proofs-of-concept, Hyperledger Fabric was more popular initially for the blockchain pioneers of the insurance industry. More recently, however, R3's Corda seems to have taken the lead not only in the insurance industry but also in the capital markets overall.

The consensus amongst respondents is that private or consortium blockchains are more suitable for the insurance industry than public blockchains for the following reasons:

i. Pseudo-anonymity of public blockchains mean that some data may still be able to be traced back to an individual (i.e.) potential privacy issues.
ii. Increased latency and cost of public blockchains.
iii. Challenges with scalability of public blockchains.

Overall, the respondents saw a place for public blockchains in insurance in the future, but more for payments and data sources/oracles. One respondent pointed out Nexus Mutual as an early indicator of what's to come, as they operate on a public blockchain, although the products are currently dedicated to the crypto space. One respondent suggests that if he were to build a consumer facing insurance product, he would do so using a completely private blockchain rather than a public or consortium blockchain. The rationale for this view was that a

[11] https://chain.link/
[12] https://www.thomsonreuters.com/en.html
[13] https://nexusmutual.io/

public or consortium blockchain lowers the barrier to entry for a potential competitor to copy the product and entice customers to switch over to their product.

The consensus on hybrid blockchains is that while they are technically possible, it's necessary to take a "*horses for courses*" approach according to one respondent. It's important to determine "*what is the true problem that the proposed product is looking to solve, for whom, and how painful is that problem for the user vis-à-vis the experience of using the product*". One respondent pointed out that XinFin is an interesting example, given their aim of "*combining the power of public and private blockchains with interoperable smart contracts*". Several other players are working on high-volume and scalable blockchain solutions leveraging sharding (a type of database partitioning that separates large databases into smaller, faster, more easily managed parts) and the Casper proof of stake frameworks. However, respondents agree that while the integration of public and private blockchains are possible for the insurance industry, there is some doubt as to the pragmatism of such an integration today, as one respondent suggests "*we are still in the 'arms race' stage of blockchain*".

On the topic of the possibility of a consortium blockchain developed by underwriters, being interconnected to a private blockchain developed by a third party for insurers, which is itself interconnected with a public blockchain populated by the public, the respondents all thought that this was feasible, and had some interesting if not mixed viewpoints:

i. The mix of permissioned and permissionless frameworks in one ecosystem can make access points very difficult to manage, especially in the case of disputes between public and private blockchains that form part of that ecosystem.
ii. The element of trust between parties in an insurance ecosystem is much stronger than that of a cryptocurrency ecosystem, so segregation of ecosystem functions into multiple blockchains may not be necessary.
iii. Although such a solution is possible, complicated frameworks pale in comparison to the simple solutions generally preferred by the end customer.
iv. Interoperability between blockchains is viewed as a fast-moving yet largely unsolved space, and with the ongoing 'arms race', interoperability between blockchains will become far more important than the features of any single blockchain, i.e., there will be no winner.
v. Rather than maintaining multiple transactional blockchains, consider how one of the proposed blockchains could just be replaced by an oracle, especially with common 'Roots of Trust' across the ecosystem.

vi. Moving between an Ethereum-based blockchain and a Hyperledger Fabric-based blockchain should be relatively straightforward with “2-way pegs”, as Ethereum and Hyperledger Fabric are very similar protocols.

Thus, it is clear that there is still much debate on blockchains and their application. The consensus is that public blockchains will eventually become scalable and suitable for wider financial services products, as there is a great deal of intellectual energy dedicated to this space. However, the expectation is that we are at least five years away from this becoming a reality.

Blockchain Interoperability with Legacy Infrastructure

With regards to successful integrations of blockchain with legacy infrastructure, the following examples were provided, as it was deemed common with private and consortium blockchains:

i. The IBM and Maersk shipping blockchain, TradeLens
ii. Ripple/XRP, especially their Ripplenet interbank network
iii. Any project using R3’s Corda, as each node has a SQL database sitting behind a firewall, such as B3i and Insurwave
iv. Most cryptocurrency exchanges, as this is the prime example of blockchains being integrated with centralised (if not legacy) technology.
v. Any off-chain database linked to a blockchain, using SQL, Java, Oracle, or even an Excel spreadsheet

All respondents had thoughts on the decisions that software engineers now face when deciding between centralised and decentralised databases. Integrating blockchain with traditional databases using services such as IBM with Multichain, Chainpoint, and Immu dB from Code Notary are also possible according to respondents. One respondent suggested that starting with a decentralised framework could be of longer-term benefit if what was initially going to be a private network could eventually become public. For example, where a private network was the foundation of a digital identity solution, those governing the project may eventually propose to transform it into a public network when it reaches the level of scale where a government agency, for example, may wish to run a node to validate/notarize changes.

Respondents also challenged the notion that the emerging and much lauded private blockchains are tamper-proof, pointing out that they are only “*tamper-resistant*” or “*tamper-evident*”, and adding that centralised databases can also be cryptographically secured,

mentioning solutions such as Amazon's QLDB[14] and Git[15]. One respondent asserts that what this really comes down to is a matter of trust, and the question to ask is this – "*does the level of trust that the targeted network participants typically have in the proposed database necessitate an alternative database structure to either establish the trust differently with a centralised database, or go decentralised, and what are the options*"? Accordingly, to find the answer, one must assess all of the options to address the trust issue across centralised and decentralised frameworks, rather than just assuming that the decentralised option is the strongest.

A further consideration is that centralised and decentralised databases can indeed be complementary, and respondents again gave examples of cryptocurrency exchanges and R3's Corda[16]. All respondents felt strongly that start-ups aiming to challenge incumbents should not just focus solely on decentralised databases. Examples of migrating data from legacy relational databases and onto a decentralised database are hard to come by in commercial projects outside of those run on Corda, as data migration from legacy databases is an option with Corda implementation.

With regards to the overall 'best-fit' solution set available for achieving the benefits of decentralised databases in the financial services markets, the consensus is to look at R3's Corda because of the market acceptance of R3 as a serious player and the fact that Corda was designed for the capital markets. While a respondent is an employee of R3 and thus may be biased, each of the other independent respondents' overall thoughts pointed in this direction, although Hyperledger was not too far behind. While Corda has been B2B focused rather than B2C focused, they are well-positioned to integrate with 'fiat onramps' into the digital asset space.

On the use of blockchain as a framework for a scalable solution with high transaction volumes, the consensus is that blockchain solutions are not suitable for this today, especially in the context of public blockchains. To quote one respondent, "*if throughput is your main concern, blockchain is not the place for you. If your main concern is scaling and growing and interacting with things that require very little upheaval to get there, I think you'll probably find that there are cheaper, easier, better ways to service your end goal, and those won't need a blockchain.*"

Cryptocurrencies

In respect of an overall view of the broader transformation of financial services infrastructure into that of blockchain and cryptocurrencies, the consensus is that this

[14] https://aws.amazon.com/qldb/
[15] https://git-scm.com/
[16] https://www.corda.net/

transformation has already started. However, exposing individuals that are less technology-savvy to the relative nascency of many crypto and blockchain frameworks today was akin to "*asking someone to watch a cow being slaughtered before your steak is served*", according to one respondent. Another respondent had a personal view that waiting for a Central Bank Digital Currency (CBDC) was sensible before trying to progress blockchain technologies for consumer-geared policies in the Insurance Industry.

With regards to cryptocurrencies and blockchain wallets being used to enable overall product propositions for the insurance industry, while the respondents saw this as an option, most suggested that exposing consumers to this level of complexity today was not a good idea. In the context of hardware wallets, key management and account recovery, the consensus is that while the security space was moving quickly, subjecting unsophisticated users to the current options available was not advisable. Examples provided by respondents of crypto players that are simplifying the user experience for individuals include Coinbase, Simplex, Argent, Mode Banking and the Ivno stablecoin project (although designed for institutional use)[17].

Largely, the consensus is however, that a Central Bank Digital Currency (CBDC) would be the best solution. However, several players have gotten around the need to buy Ether (ETH) to get fiat onto the Ethereum network[18], which could take away some complexity for less sophisticated users. In general, it is expected that CBDC will become a reality before Bitcoin (BTC) or ETH become mainstream, although players such as PayPal and Square are making considerable progress with BTC enablement through building up their own reserves. One respondent advises that digital disruptors "*explore payment solutions that protect the end user from cryptocurrency frameworks. These are available today, and pending regulations. CBDC developments are 3-5 years away. So the objective should be to engineer the product so that it is easy to use for the end customer*".

With regards to the regulation enabling stablecoins being used as a means of payment, this is now in progress in the EU with the Market in Crypto Assets (MiCA)[19] proposed regulation released in Q3 2020 as part of a wider EU Commission Digital Finance Package. A large part of the proposed regulation focuses on the interplay between stablecoins and electronic money, and the electronic money institutions are already regulated in the EU and the UK. Crypto players such as Coinbase and Gemini already have their Electronic Money Institution (EMI) licenses governing how they hold fiat on behalf of their customers, and both of these players already enable Visa debit card linked payments in stablecoins or other cryptocurrencies. So, in

[17] https://www.ivno.io/
[18] https://ethereum.org
[19] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-crypto-assets-1

short, the regulation is coming to make such a framework available to non-EMIs, and the large crypto players are well-positioned to adapt to MiCA. Outside of EMIs, the use of stablecoins to pay for private transactions is legal on a peer-to-peer basis. Those crypto players/wallets enabling these transactions do need to register as Virtual Asset Service however.

CONCLUSION

The general view is that digitalisation, the search for talent, the needs of the customer and the weight of regulatory and compliance requirements will all define the next five to ten years of the insurance industry. Each one of these factors are key drivers of change and have wider impacts as well:

i. Digitalisation: the more digital we become, the greater the cyber threat for all insurers.
ii. Search for talent: the post-Brexit future is uncertain in terms of how insurers attract and retain talent.
iii. Customers generally only engage with their insurers once a year, but they're expecting the same levels of digital self-service they enjoy elsewhere
iv. Regulatory and compliance: not only country-specific requirements, but also an increasing level of EU requirements.

Each of these factors can also present threats, as with digitalisation and cyber risks, and there are some threats external to the industry as well. For example, if those insurers with the best grasp of technological acumen and information/network security are those that can succeed in the future, would the industry overall be threatened by those that already have those capabilities in spades? Amazon and Tesla have commonly been referred to as the most capable of those that can threaten the status quo of insurers from the outside, but they have yet to make a move on this side of the world (Telsa and Axa collaborated in Hong Kong from 2015-2018).

Looking at the insurance industry today, there is an opportunity to simplify how consumers interact with insurers to protect against loss. The industry is lagging behind other industries in terms of technological advancement, where consumers don't have to spend that much time talking to the business from whom they are purchasing a product or service. There are ready-made software components that are available to insurers today that are used well in other industries, so the solutions don't need to be developed in-house. However, the prioritisation, budget allocation and selection of technology to solve a problem are obviously followed by implementation, integration and usage optimisation at the insurer level, which are challenges for all industries to get right.

Insurers are also dealing with the cost of legacy systems, alongside the streamlining and automation of operational processes and digitalisation of customer engagement. What this presents is the fallacy of pointing to technology as the cure-all, as it takes a concerted effort across all stakeholders to implement transformational technology, and digital transformation is just as much about people change as it is about technology change. In addition, new regulatory challenges can result in insurers pausing transformational projects. For example, some new regulations result in insurers changing their back-office systems to support new requirements, and regulatory projects always take precedence over digitalisation projects. The two can be done simultaneously with a creative approach, but this requires walking a fine line and can be risky, which is what insurers seek to be the opposite of.

Overall, the baked-in inefficiencies of the insurance industry are significantly influenced by the typical model of engagement with customers (i.e.) once a year. Many insurers are working on new ways to engage more regularly with customers through mobile apps linked to their health data for health insurance purposes, for example, but the general insurance lines have different requirements. The shared view on how insurers can reduce costs while creating the environment for more frequent engagement with customers centres on:

i. Sharing of customer data across the insurance industry to significantly improve how insurers underwrite policies and settle claims, assuming the right regulatory and competition frameworks are in place to enable data sharing.
ii. Building a new level of trust with customers as a more effective underwriting experience and claims process as data shared between insurers can positively impact how customers perceive their insurers, creating a context where customers are more open to sharing additional data with their insurers.
iii. Better user experience as customer engagement with insurers becomes far more personalised through the use of their own data, the ability of insurers to create more comprehensive app-based customer journeys leading to an increased digitalisation of operational processes within insurers, in turn, reducing costs.

For digital disruptors intent on bringing to market a Minimum Viable Product (MVP) to generate revenue while the market develops over 3-5 years, thoughts should turn to products that smartly nudge uninsured consumers to get insurance and the underinsured to buy more. There appears to be enough inefficiencies in the underwriting process to merit a solution. One respondent advises digital disruptors to "*keep it simple – most consumer-market geared insurers are focused on improvements around the edges – implementing cloud services and data analytics tools, UX improvements, APIs, mobile apps - not wholescale changes to the business model for a small part of their business*".

In the context of digital disruptors focused on blockchain and distributed ledger technologies, one respondent advises, "*If you use blockchain, I hope that you use it wisely. It's useful if you have a requirement for one party to keep their data and the other party to also keep their own data, and the two parties cannot trust one another with it. If that requirement does not exist, it doesn't make sense to use blockchain, because then you can just use one database and update it together and set up also some sort of scheme to govern who can do what*." However, the most important blockchain takeaway from all of the interviews seems to be the following proffered by one respondent: "*Don't say 'blockchain' - the eyes of 90% of insurance executives gloss over when you talk to them about blockchain – see if you can construct your value proposition without using the terms 'blockchain', 'distributed ledger technologies', 'decentralised databases' to force the focus on the product, not the infrastructure*".

In recalling one of the closing thoughts from one of the insurance executive, "*the pace of technological change in insurance mimics that of the customer needs*," the onus is on the digital disruptor to design a product that the customer needs, and then becomes so enamoured with it that they can't live without it. This is true at the B2B and B2C level.

Finally, digital disruptors are advised to avoid the handcuffs - this space requires the proposal of frameworks to regulators rather than waiting for them to make a call and do not let it stop progress if there's no clear regulatory answer in the market.

FUTURE RESEARCH

This research provides valuable insights into the thoughts and perspectives of incumbent business leaders of the insurance industry in Europe. Future research could pursue further exploration of incumbent and new entrant partnership opportunities and success stories; the role of regulation and compliance as a barrier to market entry for new digital disruptors; the increasing threat of cyber security to digitalisation of the insurance industry; the application of DLT's by the insurance industry in a business to consumer facing context; and the role of ML and AI in improving and driving customer service and moving from fraud detection to fraud prevention. Furthermore, the role that drones will play in risk assessment, insurance investigations, and policy settlements is a future topic worthy of research.

ACKNOWLEDGEMENTS AND DECLARATIONS

This research paper was funded under the South East Technological University (SETU) Waterford Research Connexions Fund 2020-2021. The author declares that they have no conflict of interest professionally or materially with respect to the subject matter or insurance industry.

REFERENCES

Albrecher, H., Filipović, D., Koch-Medina P., Schmeiser H., Loisel, S. (2019). Insurance: Models, Digitalization and Data Science. Swiss Finance Institute. Research Paper Series, 19-26, June.

Arner, D.W., Barberis, J., Buckley, R.P. (2015) The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong Faculty of Law Research Paper No. 2015/047, UNSW Law Research Paper No. 2016-62. Retrieved June 2nd, 2022 from SSRN: https://ssrn.com/abstract=2676553

Baumann, N., (2018). A Catalyst for Change - How Fintech has Sparked a Revolution in Insurance. Retrieved June 2nd, 2022 from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-catalyst-for-change

Capiello, A. (2020). The Technological Disruption of Insurance Industry: A Review. International Journal of Business and Social Science 11(1)1, January, doi:10.30845/ijbss.v11n1p1

Chester A., Hoffman N., Johansson S. and Braad Olesen P. (2018). Digital Insurance in 2018 - Commercial Lines InsurTech: A Pathway to Digital, Retrieved June 2nd, 2022 from https://www.mckinsey.com/industries/financial-services/our-insights/html

Chishti, S., and Barberis, J. (2016). The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries. Chichester, UK: John Wiley & Sons Ltd.

Clifford-Chance (2017). Are Smart Contracts? Clifford Chance. Retrieved June 2nd, 2022 from https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2017/08/are-smart-contracts-contracts.pdf

Cognizant (2017) Blockchain in Insurance. Retrieved June 2nd, 2022 from https://www.cognizant.com/whitepapers/blockchain-in-insurance-risk-not-reap-not-codex3136.pdf

Davies, A. (2019). How to Use Blockchain to Build a Scalable Database? Retrieved June 2nd, 2022 from https://www.devteam.space/blog/how-to-use-blockchain-to-build-a-scalable-database/

Deloitte (2017) White Paper: The Blockchain (R)evolution – The Swiss Perspective. Retrieved June 2nd, 2022 from https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-blockchain-revolution.pdf

Duane, A. and Finnegan, P. (2004). Managing Email Usage: A Cross Case Analysis of Experiences with Electronic Monitoring and Control. In M. Janssen, H. G. Sol, & R. W. Wagenaar (Eds.), ICEC'04: Proceedings of the Sixth International Conference on Electronic Commerce (229–238). New York: ACM Press.

Duane, A. and Finnegan, P. (2007). Dissent, Protest and Transformative Action: An Exploratory Study of Staff Reactions to Electronic Monitoring and Control of E-mail Systems in One Company Based in Ireland. Information Resources Management Journal, 20(1), 1-13.

Eling M. and Lehmann M. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. The Geneva Papers. 43, 359–396.

Gartner (2017). Insurance as a Service? Retrieved June 2nd, 2022 from https://blogs.gartner.com/andrew_white/2017/09/25/insurance-as-a-service/

Gartner (2020). Gartner Information Technology Glossary Digitalization. Retrieved June 2nd, 2022 from https://www.gartner.com/en/information-technology/glossary/digitalization

Guba, E.G. and Lincoln, Y.S. (1994) Competing Paradigms in Qualitative Research. In Handbook of Qualitative Research, (Denzin, and Lincoln, Eds.), C.A., Sage.

Harrison, G. (2019). Leveraging the power of blockchain in databases. Retrieved June 2nd, 2022 from https://jaxenter.com/blockchain-databases-160855.html

Heath, M. (2019). Making a Blockchain Powered Insurance Industry Reality. Retrieved June 2nd, 2022 from https://medium.com/@ontheheath/making-a-blockchain-powered-insurance-industry-reality-4588a6ec6aee

ISDA (2019) Legal Guidelines for Smart Derivatives Contracts. Retrieved June 2nd, 2022 from https://www.isda.org/2019/10/16/isda-smart-contracts/#legal-guidelines

KPMG (2019) How Blockchain is Tackling Insurance Industry Challenges. Retrieved June 2nd, 2022 from https://home.kpmg/xx/en/home/insights/2018/09/blockchain-in-insurance-fs.html

Mackenzie, A., 2015. The Fintech Revolution. London Business School Review, 26(3), 50-53.

Martin, L. (2019). Blockchain vs. Relational Database: Which is Right for Your Application? Retrieved June 2nd, 2022 from https://techbeacon.com/security/blockchain-vs-relational-database-which-right-your-application

Marshall, C. and Rossman, B.G. (1999) Designing Qualitative Research. 3rd Edition, Sage, C.A.

Mearian, L. (2019). Why Hybrid Blockchains will Dominate eCommerce. Retrieved June 2nd, 2022 from https://www.computerworld.com/article/3435770/why-hybrid-blockchains-will-dominate-ecommerce.html

Nicoletti B., 2017. The Future of FinTech: Integrating Finance and Financial Technology in Financial Services. Palgrave Studies in Financial Services Technology. Palgrave and MacMillan. DOI 10.1007/978-3-319-51415-4. Retrieved June 2nd, 2022 from https://fintech.neu.edu.vn/Resources/Docs/SubDomain/fintech/(Palgrave%20Studies%20in%20Financial%20Services%20Technology)%20Bernardo%20Nicoletti%20(auth.)-The%20Future%20of%20FinTech_%20Integrating%20Finance%20and%20Technology%20in%20Financial%20Services-Palgrave%20Macmillan%20(2017).pdf

OECD (2017). Technology and Innovation in the Insurance Sector. Retrieved June 2nd, 2022 from https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf

PWC (2018) The Insurance Industry is Rife with Opportunity and Growing Threats, Reveals Insurance Ireland'. Retrieved June 2nd, 2022 from https://www.pwc.ie/media-centre/press-release/2018/insurance-industry-rife-with-opportunity-and-growing-threats-reveal-insurance-ireland-pwc-ceo-pulse-survey.html

Schmidt, J., Drews, P. and Schirmer, I. (2017). Digitalization of the Banking Industry: A Multiple Stakeholder Analysis on Strategic Alignment. Presented at Americas Conference on Information Systems (AMCIS), Boston. Retrieved June 2nd, 2022 from https://aisel.aisnet.org/amcis2017/StrategicIT/Presentations/27/

Singapore Academy of Law (2020) Private International Law Aspects of Smart Derivatives

Contracts Utilizing Distributed Ledger Technology, Retrieved June 2nd, 2022 from https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-08/2020-Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf

Singh, N. (2018). Hybrid Blockchain- The Best of Both Worlds. Retrieved June 2nd, 2022 from https://101blockchains.com/hybrid-blockchain/.