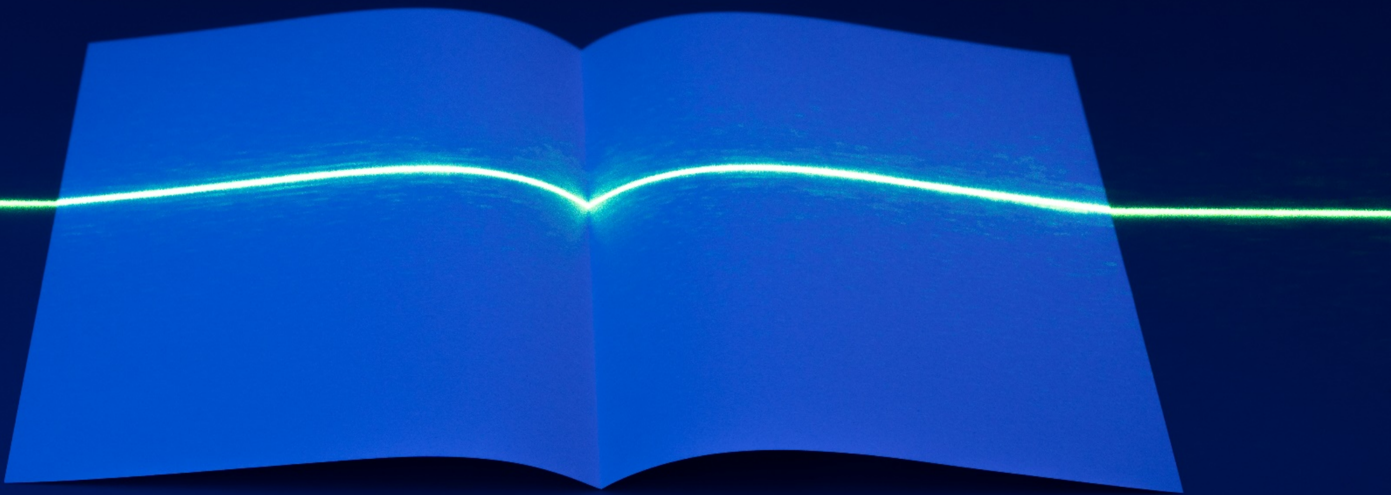
LLOYD'S

Emerging Risks Report 2019

Understanding Risk

Triggering innovation
How smart contracts bring policies to life



Queen Mary University of London

Centre for Commercial Law Studies

Lloyd’s disclaimer

This report has been co-produced by Lloyd's and Centre for Commercial Law Studies for general information purposes only. While care has been taken in gathering the data and preparing the report Lloyd's does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied.

Lloyd's accepts no responsibility or liability for any loss or damage of any nature occasioned to any person as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this report. This report does not constitute advice of any kind.

About Lloyd’s

Lloyd's is the world's specialist insurance and reinsurance market. Under our globally trusted name, we act as the market's custodian. Backed by diverse global capital and excellent financial ratings, Lloyd's works with a global network to grow the insured world –building resilience of local communities and strengthening global economic growth.

With expertise earned over centuries, Lloyd's is the foundation of the insurance industry and the future of it. Led by expert underwriters and brokers who cover more than 200 territories, the Lloyd’s market develops the essential, complex and critical insurance needed to underwrite human progress.

About the Centre for Commercial Law Studies

Centre for Commercial Law Studies (CCLS), Queen Mary University of London (QMUL) has over 30 full-time academic staff and more than 50 practitioners, judges and visiting academics contributing to the teaching, research and life of the centre. The involvement of leading practitioners and business in the delivery of our courses continues to ensure that the teaching and training we deliver is relevant and practical whilst retaining the highest academic rigour.

By bringing academia and practice together, CCLS has become a world leader in commercial law research.

Key contacts

Trevor Maynard
Head of Innovation
trevor.maynard@lloyds.com

For general enquiries about this report and Lloyd’s work on innovation, please contact innovation@lloyds.com

About the authors

Dr Miriam Goldby is Reader in Shipping, Insurance and Commercial Law at CCLS, Deputy Director of the Centre’s Insurance Law Institute, Co-Academic Director of its Institute of Transnational Commercial Law and Director of its LLM in International Shipping Law. She is the deputy editor of the British Insurance Law Association (BILA) Journal. She has published extensively in the fields of shipping, insurance and financial law, including financial regulation.

Chris Reed is Professor of Electronic Commerce Law at CCLS. He was formerly Director of the Centre and subsequently Academic Dean of the Faculty of Law & Social Science at Queen Mary. Chris has worked exclusively in the computing and technology law field since 1987, and has published widely on many aspects of computer law. From 1997 to 2000 Chris was Joint Chairman of the Society for Computers and Law, of which he is an inaugural Honorary Fellow.

Dr Michaela MacDonald is a Teaching Fellow and a researcher at CCLS, specialising in Information Technology, Interactive Entertainment and Information Security Law. Research projects in recent years focused on the legal and regulatory implications of open source licences, cloud service contracts, data and text mining or the use of intelligent agents in commercial transactions. She also works as a consultant at Moorcrofts LLP.

Dr Katie Richards joined Cardiff School of Law and Politics as a lecturer in September 2015 and teaches in the areas of contract, commercial, insurance and shipping law. Her PhD research was on the topic of ‘Fraud unravels all: A critical examination of the fraud rules in marine insurance and documentary credits’ and she has published several journal articles on the subject of insurance fraud. She is a member of the Insurance Law Institute at CCLS and has participated in the New Voices in Commercial Law series of seminars organised by the Centre.

Lucy Stanbrough MSc, BSc, is an Associate in the Innovation team at Lloyd’s. Subjects covered in recent years include: cyber scenarios; city resilience; synthetic biology, virtual reality and disaster risk finance. Prior to joining Lloyd’s, she worked for over 10 years as a natural hazards and GIS consultant, alongside working at the UCL Hazard Centre. Lucy has contributed to a number of books on the use of technology and online systems pre, during, and post-disaster. She maintains an interest in the integration of scientific knowledge to business applications, and connecting knowledge to people, and people to knowledge.

Acknowledgements

The following people were consulted or commented on earlier drafts of the report, attended workshops and 1:1 meetings, and provided their time and support to the project; we would like to thank them all for their invaluable contributions:

Lloyd's project team

- Dr Trevor Maynard, Head of Innovation
- Dr Keith Smith, Research and Development Manager, Innovation
- Lucy Stanbrough, Associate, Innovation
- Kevin Lazarus, Senior Solicitor
- Flemmich Webb, Speech and Studies
- Linda Miller, Global Marketing

Lloyd's internal consultation

- Paul Brady, Head of Policyholder & Third Party Oversight
- Lindsey Davies, Senior Manager, Customer Consents
- Kevin Clarke, Manager, Salvage Arbitration Branch & Certificate Office
- David Lawrence, Head of Agency
- Anne-Gaelle Leillard, Coverholder Manager
- Xuan Luu, Insights Analytics Specialist, Data Lab
- Mateo Rubio, Research Associate, Class of Business
- Guy Sellers, Senior Manager, Class of Business
- Ian Shelley, Class of Business Manager

Lloyd's market

- Joe Mellen, Antares Underwriting
- John Potter, Antares Underwriting
- Parth Patel, Ascot Group
- Justin Emrich, Atrium
- Samit Shah, Atrium Underwriting
- Dorian Langridge, AXA XL
- Joji Mathew, AXA XL
- Ghanshyam Patil, AXA XL
- Jette Varnals, AXA XL
- Walid AlSaqqaf, Beazley
- Steve Flood, Beazley
- William Skertic, Beazley
- Lee Timms, Beazley
- Emma Whiteacre, Beazley
- David Arthur, Brit
- Daniel Klinger, Brit
- Dana Cullen, Channel 2015
- Will Thorne, Channel 2015
- Tom Graham, Chaucer
- David McKenzie, CNA Hardy
- Filip Wuebbeler, Markel
- Victoria Mills, MIS Intelligence
- Adam Beatty, Nephila
- Gina Butterworth, Nephila
- Karl Stanley, RenaissanceRe
- Jamie Garratt, Talbot
- Hugo Lewis, Talbot

London market consultation

- John Taylor, DXC
- Sreenivas Bandi, LM TOM

Contents

Executive summary

The world is changing. Technology and data analytics are disrupting traditional business models. The industry needs to react to these rapidly evolving business and risk environments so we can continue to provide customers with the support and protection they need to grow and prosper. This means accelerating the development of products and services to meet customers' needs, and creating new business models that support their delivery.

This study analyses one technology – smart contracts, that translate written contracts into computer code – that insurers could use to improve efficiency and add value for customers.

Smart contracts are pieces of computer code that are designed to start carrying out tasks automatically in response to external 'triggers', such as receiving storm or flood data. They are used to carry out contractual obligations, in whole or in part. A simple contract might be coded in its entirety; a more complex contract would use smart contracts to carry out just some of its obligations.

There is no universally agreed definition of smart contracts yet there are common, agreed features that indicate how they could be developed and put into practice:

- Smart contracts are not written in traditional legal language but are expressed in computer code
- Obligations set out in smart contracts are fully automated and resulting agreements are intended to be self-executing
- Automated, self-executing transactions are cheaper because they are self-contained and do not require legal enforcement
- Smart contracts can be linked to trusted third-party data sources

Given these features, smart contracts could have two main functions:

- To enhance existing processes within the insurance sector, including risk placement and premium payments, warranty enforcement, and claims assessment and settlement
- To enable new ways of doing business by facilitating new product development and other factors that help achieve this

The Future at Lloyd's

These two aspects – enhancing existing process and enabling new ways of doing business – sit at the heart of The Future at Lloyd's process, which looks at how we could evolve Lloyd's so it continues to be successful in the future.

The new Lloyd's will be nimbler and faster, offering our customers outstanding products, services and insight, supported by technology, innovation and flexible, responsive capital.

The Future at Lloyd's document sets out six possible ways we could achieve this. One of these options focuses on building a next generation claims service that pays a claim before the customer realises they have experienced a loss. Smart contracts could help make this happen.

Parametric progress

There is already a lot of change underway at Lloyd's. We are ensuring the market's underwriting, and the way in which we asses and price risk, is world-class through rigorous performance management and adherence to best-practice standards.

We are also continuing to modernise the market, and embrace new technology and new ways of doing business. Our ambition is to ensure we have the appetite and expertise to protect customers from their most challenging risks, and that they will continue to find solutions for those risks at Lloyd's.

Parametric insurance, which pays out a pre-determined value once the triggering of a parameterised loss has been verified, constitutes one of the cornerstones of smart contracts from a product-design perspective.

Several Lloyd's market participants already sell parametric insurance covers, positioning Lloyd's at the forefront of the parametric insurance industry and successfully demonstrating that:

- With appropriate data management, risk modelling, product design, accompanied by robust legal advice and consumer education, parametric insurance and subsequently smart contracts, can be designed to provide timely and adequate covers for a wide range of risks, whilst building important cost-efficiencies for carriers.
- The Lloyd's market is a unique ecosystem, which facilitates the development and sale of parametric products to the highest underwriting standards.
- There is a plenty of scope for the Lloyd's market to write more parametric insurance and become the sector leader in this field.

New challenges and opportunities for the insurance industry: smart contracts

Smart contracts have the potential to be used beyond parametric products to automate aspects of traditional insurance contracts and to facilitate innovative product development.

Aligning products and services to customer needs, smart contracts could automate a number of insurance functions, including:

- Initiating workflow actions
- Initiating claims-agreement processes
- Notifying follower insurers that claims payments have been approved
- Updating adjustable contract premiums
- Paying claims based on trusted information sources

This report provides information on smart contracts and their use in insurance to make risk transfer more efficient *(Section 2)*. It also sets out how smart contracts could help create new insurance products for different customers, including individuals, binder business, and regional and national governments *(Section 3)*.

The report does not go into detail about different smart contract technologies nor give legal advice, but does suggest feasible models and how to build them *(Section 4)*. This includes design considerations for insurers looking to create smart contracts.

The study also:

- Outlines the range of development options within smart contracts and how they can be applied
- Analyses the potential risks and opportunities associated with smart contracts
- Assesses the technology available today and how it might develop in the future
- Considers the role of indices, distributed ledgers and other sources of objective information in the contract process
- Looks at the legal frameworks and standards associated with putting smart contracts in place

Key findings

1. Insurers using smart contracts will need to design them carefully, so they are flexible enough to be practical. Current smart contract technology only supports the coding of logical clauses ("if X, then do Y"). This means that, except for very simple products, in the short-term, smart contracts will likely exist alongside traditional contracts.
2. Smart contracts could be used to redesign the existing contractual framework to allow automatic claims payments as part of low-value, low-complexity, high-volume insurance products, where in-depth scrutiny of claims is not normally required and where the costs of processing the claim manually may exceed the benefits of paying out. The four case studies in this report demonstrate the possibilities in this area.
3. Automated pay-outs via smart contracts may be completely unsuitable for high-value, complex insurance cover, where human decision-making remains key to managing the claims process and the insurer-customer relationship more generally. In this scenario, smart contract code could still be used to make processes more efficient - by alerting claims handlers that action needs to be taken, for example.
4. Insurers should consider the classes and geography of their policies when thinking about smart contracts as there may be jurisdictional restrictions in place, or regulatory programmes that allow testing and development.
5. Although the original conception of smart contracts was that their code would include all parts of a legally binding contract between parties, this is not how the majority of smart contracts will be seen in law. Instead, the law defines the contract as it appears in documents, correspondence and statements, and will see the code as a means of performing the resulting contractual obligations.

   This means that a combination of computer and legal skills are needed to create a smart contract as it involves coding legal obligations. One challenge is to ensure the nature of the contracted relationship is not lost in translation.

6. Accurately representing and interpreting contractual semantics in code will require hiring employees with relevant skills, making recruitment and training an important part of the smart contract process.
7. Testing smart contracts will be crucial, as even correctly written code may produce unexpected results in unusual circumstances. Smart contract code needs to be assessed against historic, synthetic and extreme scenarios before it is put into commercial use.

Case studies

The four models in this report (Section 3) show some of the innovative ways smart contracts could be included as part of insurance products, particularly for risks where independent data sources are available, as these would allow automatic triggers for claims payments to be used.

These models are intended to stimulate ideas in other insurance classes in which full claims and/or workflow automation could be used today, and to harness wider initiatives in the Lloyd's market in the future.

The case studies cover the following business classes:

– Cargo: this is a class in which the prospect of switching to products featuring smart contracts triggered by data from independent sources is looking increasingly realistic.

  The use of internet of things (IoT) sensors could improve claims services, by helping establish workflows that appoint the closest approved surveyor (using geolocation) to inspect cargo immediately after its discharge from a vessel. IoT sensors could also be used to provide risk mitigation information for customers to take corrective action to prevent or reduce losses if they opt-in to alerts.

– Contingency/Aviation: smart contracts for automated pay-outs in aviation could be applied to add-ons or as replacements for parts of existing insurance contracts. Automatic pay-out pursuant to the triggering of a smart contract may be suitable for two add-on products: business interruption related to adverse weather conditions or technical defects.

  For adverse weather resulting in flight delays or cancellations, verifiable third-party data could be collected from airfields and weather services to identify and confirm 'non-flying' weather. For technical defects, independent data could be taken from an approved engineer certificate or outputs of sensors from an aircraft confirming a fault.

– Agriculture: Smart contracts as part of parametric insurance covers might work for crop failure in the agricultural sector. An insurance product that operates as a smart contract would have to cover against the causes of crop failure, with an automated pay-out occurring when agreed damage thresholds are reached, that would indicate damage or failure – this could be tiered.

  A range of indices are available to provide objective sources of data, but where there might not be coverage from national weather offices, products may need validation from multiple sources.

  Smart contracts could also be used at the portfolio level to support underwriting a risk decision. For example, factors affecting known disease vectors might be detected, and trigger an underwriting decision or risk control to support closing the protection gap.

– Property catastrophe: Parametric products are already available in the Lloyd's market for areas prone to natural disasters, and could feature smart contracts that execute automated claims pay-outs when these events occur.

  This would help insurers respond to disasters quickly and efficiently. The pay-outs would be made on the intensity of an event occurring in a particular location rather than on the basis of assessed losses.

  Parametric products are already being used for reinsurance in this class, including through the issuance of catastrophe bonds. Smart contracts could be used to develop retail parametric insurance products on the same terms as the reinsurance arrangements.

  Besides enabling efficient responses to disasters, these products would have the added advantage of improving the alignment between insurers' exposure and their protection through reinsurance, as the recovery from reinsurers would match more closely the pay-out made by the insurer to the insured. Smart contracts could also be used to trigger reinsurance layer notifications.

Making it happen

There are many studies outlining the potential application of smart contracts and the various technologies currently under development used to build them, but there is limited information on how they can be used to address specific insurance industry challenges such as parametric covers.

This study outlines three elements that will help insurers consider how smart contracts could work for them *(Section 4).*

1. Technology

The concept of smart contracts is independent of the specific technology used to build them and could be implemented on any computer system that keeps records and is capable of input from and output to external devices.

This could be a variety of distributed ledger technologies or existing databases. The precise technological implementation is less important than understanding the concept of smart contracts and how they might be used in the insurance sector. For individual insurers this is an internal decision. Use in any wider network will require collaboration with stakeholders on standards, platforms, etc.

2. Design choices

The customer needs to be sure their insurer is authorised and that they themselves have been verified so they can receive premiums and claims payments, in accordance with Know Your Customer regulation.

A smart contract needs to be built on either a "permissioned" distributed ledger system (in which users are identified) or a centralised database system (or some equivalent) to provide the transparency needed to comply with regulation.

In either case, the system will need to be controlled by some entity, the system "owner". That owner will need to make a number of design choices, all of which have legal and regulatory consequences:

- Revocation: there may be some circumstances in which the smart contract needs to be revoked, which will usually require cooperation, agreement and some technical action by both parties.
- Rectification: if unilateral revocation is not allowed there will need to be some mechanism through which errors can be rectified. This might include a code defect being corrected or the contract being cancelled.
- Payment of claims: as well as mechanisms for payment, provision for compliance requirements such as money laundering will need to be built in.
- Closed or open code: open code could assist courts to interpret conflict between code and human interpretation; closed code preserves intellectual property and security. There is no right answer on which is the most suitable but the issue needs to be considered.
- Code testing: there should be a testing regime for code before it is used in smart contracts, and records should be kept to determine compliance.
- Certification and standards: for smart contracts to realise their full potential, certification and standards will be needed to demonstrate regulatory compliance and give confidence that code will perform as intended.
- Bespoke code: bespoke changes for particular customers or risks might invalidate any testing, so a sensible choice at this stage would be to develop modular smart contracts so only the input parameters are changed and not the code. Customers would be given a menu of choices, all of which would produce known, tested outcomes.
- Market alignment: where the terms of the primary contract allow the lead insurer to choose different information sources as smart contract triggers, follower insurers would need to consider whether they will accept the same sources or demand different triggers. There are key considerations around risk understanding and consistency of claims payments that will need to be thought through.

3. Legal and regulatory considerations

Smart contracts are in the early stages of development and while there is progress, currently there are no international standards applicable to them nor is there a uniform legal regime governing their use. Each jurisdiction will raise its own legal and regulatory issues that will need to be considered.

There are also considerations around:

- Indemnity and insurable interest: ensuring there is a mechanism for verifying insurable interest at policy inception and loss will be a key aspect to build in.

  For example, in the cargo class, a smart contract would need to be linked up with an information source that records the insurance cover as it moves from the cargo's sellers to the cargo's buyers, so that the ultimate owner may be verified at the time of the claims pay-out.
- Conduct of business regulation: there are a number of areas to watch here, including the obligation to identify client needs and advise accordingly, speed of payment of claims and treating customers fairly. For example, ensuring that the code functions properly and in line with the insurer's conduct of business obligations towards its customer. Quality control needs to be undertaken.

  These design features need to be built in so they are compliant with regulatory requirements, ensuring that customer expectations are properly managed.
- Data protection: should the use of smart contracts become more widespread, insurers will be managing much larger volumes of personal data from interconnected sources.

  A full data protection assessment will need to be carried out for any activities or products which change because smart contracts have been introduced.

Conclusions

Smart contracts could be a promising solution to improve efficiency in the insurance sector. Other product innovation such as parametric insurance is helping drive this technology forwards and there are likely to be more examples of innovation in this area as awareness of smart contracts grows.

It is important for anyone thinking about using smart contracts or parametric insurance to seek legal advice to ensure regulatory compliance.

Any new product is subject to Lloyd's normal guidelines around planning and class specific requirements, and managing agents should refer to their syndicate business performance manager for questions.

The Lloyd's class of business team is available to accompany and assess managing agents in all stages of parametric product development, and expects to analyse the viability and legality of new products individually.

1. Introduction

Disruptive forces are changing the insurance sector with challenges such as an abundance of capital, demographic changes, changing risk profiles, cognitive computing and data analytics, and new customer needs forcing insurers to come up with collaborative solutions.

Furthermore, new technology and the need to futureproof systems and processes has made it more important than ever to modernise insurance and make it easier to do business, whether through face-to-face or electronic trading.

This report examines one development that could be used to support and facilitate innovation – smart contracts. At their core, smart contracts are neither "smart" nor "contracts" but a "a set of promises, specified in digital form, including the protocols within which the parties perform on these promises" (Szabo, 1996) or "if X occurs, do Y" (Savelyev, 2017).

This broad definition allows for a variety of operational models and variations between two ends of a spectrum:

1. The contract is the code: the entire insurance policy is digitised as smart contract code, translating legal contract terms into computer code;
2. Digitising the performance of business logic: i.e. smart contracts that pay the insured and trigger a workflow.

Within the insurance sector, smart contracts could perform a number of different functions, such as instigate workflow actions, initiate a claims agreement process on notification, notify followers of approval to pay, update an adjustable contract premium based on objective data, or pay a claim following a trigger.

There are also areas where smart contracts may not be the correct solution. For example, while reinsurance treaties can largely be standardised, and smart contracts could add security and efficiency, facultative reinsurance is more variable and triggering workflows is likely to be a more practical application rather than full coding, due to costs involved (Long Insurance, 2017).

There are many studies available that outline the potential applicability of smart contracts and the various technologies currently under development. These are mentioned throughout this study and in further detail in Section 3.

However, there is limited information available on how smart contracts can be practically implemented to specific industry challenges and this study aims to answer some of those questions.

While this report is not meant to explain the internal workings of different technologies nor give legal advice, it does suggest some feasible smart contract models and the main steps towards achieving them.

Section 2 discusses the core concepts of smart contracts and the development streams of supporting technologies that could enable their implementation, including what the existing literature says about potential uses of smart contracts in the London insurance market.

Section 3 outlines some potential uses of smart contracts and sets out four business models that demonstrate how smart contracts could:

- Enhance existing processes within the market: including placement, premium and assessment, and the settlement of claims
- Enable new ways of doing business, including the development of new products and the enabling factors that will need to be in place to do so.

1.1 Common terminology

To help build understanding the following key terms are used:

Box 1: Key terms

Smart contract: a smart contract is a computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.

Smart contracts are pieces of computer code that are designed to carry out tasks automatically in response to external triggers, such as receiving storm or flood data. They are used to carry out contractual obligations in whole or in part. A simple contract might be coded in its entirety; a more complex contract would use smart contracts to carry out only some of its obligations.

Smart contract triggers: the trigger for a smart contract can be as simple or as complex as is needed, provided it can be coded.

Distributed ledger: a record or ‘ledger’ of transactions which is distributed among a number of nodes each of which holds an identical copy of the record and in which the transactions are stored in a permanent and near inalterable way using cryptographic techniques. At heart, the main function of any distributed ledger system is to provide evidence about assets, participants and transactions between participants.

Blockchain: a distributed ledger technology that records transactions between two or more counterparties in a tamperproof way that ensures records can be completely relied upon. Transactions are grouped in ‘blocks’ and each block is linked to prior and succeeding blocks, using the same cryptographic techniques.

A blockchain-based system needs no central platform or run ‘authority’. Each participating organisation runs the application on its own ‘node’ and each has exactly the same view of the data that is relevant to them (but not of anyone else’s data) at all times. Participants share the process of authenticating the validity of transactions.

2. What are smart contracts?

The concept of a 'smart contract' first emerged in the literature in the mid-1990s and is attributed to the computer scientist and cryptographer Nick Szabo (1996, p. 120). At that stage, the smart contract was defined as:

> *"A set of promises specified in digital form, including protocols within which the parties perform on these promises." (Szabo, 1996)*

Szabo illustrated this concept with the example of a vending machine (1996); an "autonomous transfer of property" (in, for example, a drink) was triggered following "a predetermined input" by the consumer (the insertion of money) (Giancaspro, 2017). This was a smart contract in that it minimised human interaction by wholly automating the "seller's" role in the transaction and because the transaction could not be revoked, once the consumer had inserted the money.

Szabo believed that the "cyberspace era" and the growth of computer networks and algorithms would revolutionise the way in which contracts were made (Szabo, 1996). Recent advances in Internet-based technologies, such as blockchain and artificial intelligence, have re-ignited interest in the concept (Harley, 2017). These capabilities are here and unfolding, making it the perfect time to consider how they might be used to solve industry challenges and open new opportunities.

These technologies are widely regarded as the means by which Szabo's smart contract theory can be fully realised. As a result, there is an emerging, but still relatively small, body (Giancaspro, 2017) of literature in this field. This literature is comprised of both academic papers (Eidenmüller & Aggarwal, 2018) and industry publications, including those issued by law firms[a], and can be found in the references at the back of this study for anyone looking to delve deeper.

2.1 Core concepts

The purpose of smart contracts is "to create a series of actionable, computer-processable instructions that approximate what it is that the parties are intending to do in their contractual arrangement" (Surden, 2012).

This last point is important. Although the technologists who devised the concept of smart contracts envisaged their code as embodying the whole of the legally binding contract between the transacting parties, this is not how the vast majority[b] of smart contracts will be perceived as a matter of law. Rather, the law will conceptualise them as follows:

- The parties enter into a contract on whatever terms can be identified from the relevant documents, representations and context.

  In the insurance contract this would typically be a set of written terms, either in hard copy form or presented via a website and agreed to by clicking a button or ticking a box. For the purposes of discussion, we will describe that contract as the "primary contract"; and
- The smart contract will be the parties' agreed method of performing some, but not necessarily all, of their obligations under the primary contract.

[a] See the references at the back of this report for sources.

[b] It is possible for a minority of transactions to code a smart contract which does embody all the express contractual terms at least – the analogy would be sale of a physical product such as a bar of chocolate via a vending machine. The clearest example might be a smart contract for the future purchase of a Bitcoin; once the triggering event (the date) occurs, the smart contract code automatically transfers entitlement to that Bitcoin to the purchaser by issuing a payment instruction to a credit card provider and, once notice of payment is received by the code, recording the purchaser as the person now entitled to dispose of the Bitcoin. But we should note that a court might still imply terms outside the code – for example, the sale of the chocolate will contain an implied term that it is of satisfactory quality, and the Bitcoin contract might be found to contain an implied term that the purchaser will not seek to reverse the payment under the purchaser's contract with the credit card provider.

Insight

This conceptualisation has the potential to lead to problems of interpretation if the terms of the primary contract do not exactly match the actions which are coded into the smart contract.

A mismatch of this kind can have costly repercussions, as while the insurer remains bound by the primary contract, the actions taken in execution of the agreement would not constitute performance. As discussed in more detail in the following sections, in view of this, testing and validation of the smart contract code is going to be key to their deployment.

2.2 Common features

There is "no universally agreed definition of 'Smart' contracts, which is not a surprise, both in view of the very novel nature of this phenomena [sic], and of its complex technological basis" (Savelyev, 2017; Werbach & Cornell, 2017; Clack, et al., 2017).

However, it is possible to identify some common features which emerge from the current discussions around smart contracts:

1. The smart contract is not written in traditional language but is expressed in computer code

This ensures that the process of execution or performance can be automated (Werbach & Cornell, 2017). This is reflected in the literature as 'if X occurs, do Y' (Savelyev, 2017; Hingley, 2018). Importantly, the trigger (the X) for the execution of contractual obligations (the Y) is defined in objective terms.

For example, the automatic payment of money (the Y) on a given date (the X) (e.g. a direct debit), the transfer of assets (the Y) on receipt of cleared funds (the X) and the adjustment of an interest rate applied to a loan (the Y) following a change in the published interest rate (the X) (Hingley, 2018).

2. The obligations set out in the smart contract are fully automated

However, entering into the primary contract (and thus agreeing that the smart contract will execute according to its terms) will still require the interaction of a human participant in most cases.

This moves the debate on from Szabo's vending machine example that still required the interaction of one human participant, i.e. to insert the money and select the product (Savelyev, 2017).

3. The resulting contract is intended to be self-executing[c]

This means that transactions, once agreed to by means of a smart contract, cannot be stopped or reversed (Bacon, et al., 2017; Clack, et al., 2017; Harley, 2017). This statement will be true for permission-less, distributed systems like Bitcoin – once the smart contract code has been digitally signed by both parties and recorded on the blockchain, the technology provides no way to prevent it executing unless the smart contract code allows the parties to agree to cancel it, by means of a digitally signed record on the blockchain.

It may not be true for blockchain systems which use a single, trusted entity (or a group of such entities) to approve blocks, as those approvers could effectively cancel a pending smart contract or other transaction (Reed, 2013).

It is unlikely to be true for non-blockchain systems which incorporate smart contracts, as here the system design will almost certainly allow the 'owner' of the system to make changes which prevent the smart contract code from executing, but it is still possible that the rules for participating in the system might provide that smart contracts are irrevocable.

In systems where there is no smart contract revocation mechanism (*see Section 4.1, 'Design choices', p36)*, performance of that element of the transaction is not dependent on legal structures (Savelyev, 2017) or other third-party human intermediaries, i.e. banks or brokers for enforcement (Wheeler, 2017; Norton Rose Fulbright, 2015).

In these systems, smart contracts can be used to overcome the natural absence of trust in transactions between anonymous parties that might otherwise be prohibitively costly in terms of mitigating the risk of non-performance (Werbach & Cornell, 2017).

[c] i.e. once the precondition has been met (the 'X' function) the next phase in performance is triggered (*event-condition-action* rule, or 'if this, then that')

Insight: blockchain permissions

Some blockchains (Bitcoin is the best-known) allow anyone in the world to participate. The participant downloads client software, which is what identifies the participant to the blockchain, and generates the signature keys necessary to undertake transactions. This is known as a permissionless blockchain.

Other blockchains have an 'owner' who grants permission to participate, usually requiring the participant to register and taking some evidence of their real-world identity. The perrmissions granted control how the participant can interact with the blockchain, which is therefore described as permissioned.

Different functionalities can be permissioned or permissionless – for example, a blockchain might be unpermissioned for reading, so that anyone can access its information, but require permission to undertake a transaction.

4. Automated, self-executing transactions are cheaper.

This is because they are self-contained and do not require parties to resort to the legal system for enforcement. Nevertheless, the self-executing nature of smart contracts may result in unintended consequences (Werbach & Cornell, 2017). As such, a proportion of smart contracts will inevitably generate disputes arising from their performance.

5. A smart contract can be linked with trusted third-party sources

These are described in the literature as 'oracles', and include asset registries, weather databases, stock market indices and physical sensors (Gatteschi, et al., 2018; Surden, 2012). They provide the relevant data which the smart contract code uses to determine if the precondition – the 'X' function – has been satisfied, which then triggers the remaining obligations under the contract, the 'Y' function (Gatteschi, et al., 2018; Surden, 2012).

This further automates the process as the contract is triggered when an objective condition has been met and communication of this is not dependent on human intervention.

There are two categories of trusted source recognised in the literature:

1. Software oracles: These extract information from online sources and databases, i.e. weather data, death registry.
2. Hardware oracles: These extract data from the real world via physical sensors (such as sensors located on the insured property) (Gatteschi, et al., 2018).

For example, a smart contract for home flood insurance may automatically process a payment to the customer when an oracle verifies that flooding has occurred. This verification may be through access to official meteorological data (a 'software oracle'), or a flood detection device installed at the home (a 'hardware oracle') or, if required by the coding, both (Roughton, 2017).

These oracles could also be linked to workflow processes for occasions when thresholds of uncertainty are reached where action could be forwarded to an expert for a decision.

Insight: smart contract triggers

The trigger for a smart contract can be as simple or as complex as is needed, so long as it can be coded. For example, suppose the insurance is to pay out in the event of a hurricane. The smart contract code needs to determine, using data from defined trusted sources, whether there has been a hurricane.

At the simplest level, this might be determined using wind speed readings from automated weather stations. If all (or more likely a specified majority) of the defined weather stations report a wind speed in excess of X kph then a payment is made.

At a more complex level, a hurricane might be defined as sustained wind speeds in excess of X kph over a defined area, lasting for at least Y minutes. The smart contract would contain a complex algorithm, using multiple data inputs over time, to determine this.

At the most complex level, the insured event might be a 'damaging' hurricane, whose calculation integrates both wind speed and sea levels (to include the risk of flooding). The code here would take a range of inputs and perform its calculation, perhaps using fuzzy or probabilistic logic to trade off wind speed against flooding risk.

2.3 Limitations of smart contracts

Smart contracts represent a shift from natural language to computer code, which inevitably determines the content of digital relationships. These areas include:

- Understanding: clarity and agreement between parties;
- Fixed logic: can discretion and flexibility be dispensed with?
- Legality: don't get lost in translation;
- Terminology: the importance of context.

Understanding: clarity and agreement between parties

One clear difficulty is in ensuring that both the insurer and the insured understand the obligations which are now expressed in code form. This raises two issues:

- Will the code execute as it is intended to do in all circumstances? Proving this is difficult for complex code, though research is constantly improving tools for software verification (D'Silva, et al., 2008).
- Even if the insurer understands the workings of the code, can that be explained adequately to the insured?

See Section 4.1, 'Design choices' (*p36*) for further details.

Fixed logic: can discretion and flexibility be dispensed with?

A second difficulty is that typically, commercial contracts are a combination of logic clauses, scenarios such as 'if X occurs, do Y' which are readily computable (Farrell, et al., 2018), and other clauses, broadly referred to as discretion clauses which are not.

> *Some terms of contracts, which are more complex than the immediate transfer of value and property, are likely not to be efficiently encoded. This is because computer code (like mathematics) is well adapted to represent terms which are expressions of logic but not terms which are based in concepts such as reason or conscience* (Farrell, et al., 2018).

These clauses allow for a degree of flexibility and require human assessment to determine whether, for example, *Party A* has acted reasonably, with good faith or has carried out an action 'as soon as possible' (Werbach & Cornell, 2017).

The temptation is to modify those clauses to remove the discretion, in other words to limit a claim to where objectively assessable facts have occurred, and this is exactly what parametric insurance aims to achieve. The potential use case is much wider than just claims.

In addition, to address the risk of moral hazard, the trigger needs to be designed to preclude fraudulent situations or errors that would trigger a pay-out.

Obligations to act fairly and reasonably towards the customer *(see Section 4, p36, for further details)* will always need to be taken into consideration. Therefore, there is always a need for an alternative route for the insured to make a claim, which will receive human consideration, even if the objective facts cannot be demonstrated to have occurred.

Currently the technology does not support the coding of discretion clauses, and it may be some time, if ever, before such clauses can be reduced to computer-readable code. An important consideration in defining smart contracts, therefore, is to recognise these inherent limitations of the technology.

There needs to be a clear set of rules for payment in these cases, outlined in the underlying policy and understood by all parties to reduce the risk of moral hazard.

Independent third parties may still be required in these instances to provide an objective judgement of loss and could be contracted at the identification of certain triggers. This could be defined for a particular case, and workflow stages requiring human decision points set out to prompt the next steps.

Insight: quick wins – volume claims

Where the contract can be designed so that payout can occur independently of the exercise of human judgement, costs can be reduced dramatically.

For example, high volume, low value non-complex claims make up around 85% of total claims in the Lloyd's market and only 15% of the value (Lloyd's, 2018). A reduction of the time spent processing these claims is a desirable target that smart contracts can help achieve.

Smart contracts promise to be most useful for market players with highly standardized agreements, large-scale exploitation of the standard contractual terms and repeated enforcement efforts (Cuccuru, 2017).

Focus on the future

For more complex relationships, such as highly customized insurance policies, smart contract technology is likely to be inappropriate as a mechanism to automate performance fully.

While smart contract technology can still be used as a mechanism for performing some of terms of the contract (e.g. the collection and distribution of premium), it is most likely to be an add-on to existing processes in the short term.

Legality: don't get lost in translation

The legal nature of smart contracts raises some important issues. Although the common law jurisdictions, such as England and Wales, are likely to recognise pure smart contracts as legally binding agreements, some Civil Law jurisdictions impose formal requirements, such as physical writing and signature. This would result in the outcome of a self-executing transaction not being legally effective and enforceable by the parties in a court of law (Sherborne, 2017).

Ensuring that any disputes are decided in a favourable jurisdiction is therefore an important consideration when deciding what lines of business and policies could benefit from the application of smart contracts.

However, the agreement itself need not be written exclusively in computer code: the smart contract may be the chosen method of executing a primary contract entered into separately.

In this case the smart contract will exist alongside other records of the agreement expressed in traditional media such as writing. The code will act as an instrument for conclusion or automatic enforcement of contracts written in natural language (Savelyev, 2017; Schönfeld, 2018; Giancaspro, 2017).

In these cases, a combination of computer and legal skills needs to be engaged in the creation of the smart contract, as it will involve the expression of existing legal obligations in computer code.

An evident challenge is the need to ensure that the nature of the relationship between the contract parties is not "lost in translation". This consideration is particularly important in the event of a dispute arising where the exact terms of the legally binding agreement may need to be established considering all the circumstances.

Terminology: the importance of context

One difficulty is the conceptualization of smart contracts by technologists as equivalent to legally binding agreements, which has led them to use some legal terms in ways which do not exactly correspond to their legal meaning. It does not help that some computing terms are identical to legal terms, but with quite different meanings.

This is a key point to consider when thinking about classes of business and policies where smart contracts can bring efficiencies.

Box 2: The importance of context

Entered into: A smart contract is likely to be “entered into”, ie become “binding” on the parties (and, if applicable, also become irrevocable), after the time that the corresponding primary contract is entered into. The smart contract becomes “binding” when it is recorded on the applicable computer system and made live, so that its code runs once notice of the trigger event is received, and this recording will usually take place after the primary contract is formed.

Trigger events have already been explained, and fortunately this term has no pre-existing legal meaning and is thus not potentially ambiguous. As a result, whatever the parties define as being the trigger event should be given legal effect.

The risk here is that the trigger may not operate in circumstances where the primary contract provides that it should. This might be because the coding of the trigger event does not match the primary contract. It might also occur where a complex insurance obligation is defined using fuzzy or probabilistic logic, so that it is not fully predictable when it will trigger *(see Insight box ‘Smart contract triggers’, p14)*.

Execution: The action performed once a smart contract triggers is often described as the ‘execution’ of the smart contract, and often also as being the execution of the primary contract. But as already explained, the action is in fact only performance of one of a party’s contractual obligations, and may not even amount to complete performance.

For example, the action might be the issuance of a payment instruction to a bank, which is intended to achieve payment by that party. But the payment obligation will not be completely performed until the bank acts on that payment instruction and completes the payment transaction. Thus performance (‘execution’) of the smart contract is connected with, but not necessarily equivalent to, performance of the contractual obligation under the primary contract.

3. Potential uses of smart contracts

Given the anticipated advantages of smart contracting, much of the literature has considered how the technology could be implemented in practice.

In this section, the discussion first considers examples from the literature, which could be employed across the insurance industry.

There are more potential uses for smart contracts than has been possible to explain in this study, including:

- Exchanging Know Your Customer (KYC) data between institutions, and with external trusted sources;
- Sharing risk data and risk profiling information;
- Recording and sharing attributes of assets, such as maintenance history, current location, etc;
- Fraud detection during the claims process by sharing and processing data from past claims.

This study is aimed at outlining the capabilities of smart contracts and highlighting some of the pathways for their implementation. The specific focus in the project is the application of smart contracts in cargo, aviation, agriculture and property/catastrophe insurance policies.

A significant challenge in the implementation of such contracts will lie in identifying objective triggers, translating the parties' intentions accurately, and anticipating the impact on the market.

The four business models illustrate innovative ways to integrate smart contracts into insurance products, particularly for risks regarding which objective sources of data are available so that reliable triggers can be devised. These business models can be found at the end of this section.

3.1 Solutions for industry challenges

There are numerous initiatives taking place across Lloyd's and the wider London Market. The London Market Target Operating Model (TOM) is a core component of the market modernisation proposal, set out by the London Market Group (LMG), to make it easier to do business in the London market, locally and globally.

There are also other examples that are referenced throughout this study which are working towards increasing efficiency, facilitating end-to-end systems and future proofing the insurance model for the benefit of customers. Any new technologies should be considered within these initiatives to drive efficiency for the customer.

Challenges

Henry and Hogan have suggested that smart contracts have potential application in the "historically high cost centres (Henry & Hogan, 2018) of underwriting, claims management, fraud reduction and reinsurance. Their view is that automation via blockchain creates the potential for considerable savings (Henry & Hogan, 2018).

At the underwriting stage, Gatteschi et *al*. (2018) have suggested that a smart contract could be used to gather specific information relating to the prospective customer and the risk from a broad range of sources and third-party oracles (Gatteschi, et al., 2018). This would speed up the placement process as the onus on the insured to provide information may be lessened but could also result in a more accurate, tailored premium.

Property catastrophe

A similar suggestion has also been made by Pinsent Masons in the context of smart flood insurance. In their illustration, the customer would install a tamper-proof flood sensor, a GPS system and a camera capable of detecting and sending information on the water level to the Distributed Ledger System (in this case, blockchain) (Roughton & Bidewell, 2017).

This information would enable a tailored quote to be produced based on relevant information about the risk and details of the customer's specific circumstances (Roughton

& Bidewell, 2017). The customer would then select the policy, or a smart contract based on parameters they specified in advance. With the policy in place, Pinsent Masons envisage that a further smart contract could be used to debit the monthly premium payment from the customer and trigger the indemnity following a flood (Roughton & Bidewell, 2017).

Insight: automating indemnity

The automation of the indemnity is already being developed in relation to flight delay insurance. Axa have developed a smart contract known as 'Fizzy', which operates via Ethereum (AXA, 2017).

A payment is triggered when the smart contract receives information from air traffic databases that a flight has been delayed by more than two hours.

The product was launched in autumn 2017 for flights between Paris and the United States with a view to expanding internationally.

More generally, there would seem to be significant opportunity for automating payment in a subscription market. A smart contract could be used to automate the obligation of following underwriters once the lead underwriter has paid (Long Insurance, 2017).

The level of coding needed to insure a typical, complex multi-country, multi-exposure asset property programme, and all the potential triggers that might exist in hundreds of pages, is not realistic in the short-term. Relatively simple products of single catastrophe perils, with a clear index for damage that can be reasonably correlated, are likely to be more applicable in the short-term.

Cargo

Regarding cargo, IBM and Maersk have recently developed an electronic system to map container journeys between ports and to digitise the paper trail (Groenfeldt, 2017). This enables all interested parties to track the container and is intended to give rise to a streamlined, efficient shipment process.

The containers are fitted with sensors. The suggestion is that these physical sensors could provide information in cargo policies, much like physical sensors on roofs have been used in domestic buildings cover to initiate claims for damp (Groenfeldt, 2017).

The resulting data could be employed at underwriting – to calculate premiums more accurately and reduce the possibility of inaccurate data (Henry & Hogan, 2018) – and in loss mitigation and to automate the claims process. The suggestion is that in time telematics could be used to generate a claim without any further human interaction.

In relation to the final two scenarios, it is useful to take as an example a cargo prone to heating. In relation to loss mitigation, if physical sensors detected an increase in temperature, the customer could be advised to take measures to prevent further loss to the cargo.

Once a loss has been deemed to have occurred using agreed data from trusted oracles, the smart contract could trigger payment to the customer without the formal submission of a claim. This could be a combination of sources of data, such as IoT devices or trusted third party sources. See the Insight box *(overleaf)* for more thoughts in this space.

Contingency/Aviation

In relation to aviation, the existing technology appears to offer several ways in which smart contracts could be implemented in this field. Digital asset registers would enable customers to upload comprehensive information about their fleets. This information could then be sent via the distributed ledger to enable the calculation of an accurate premium (Long Insurance, 2017). This is critical given that insurance bands are dependent on the aircraft's take-off weight (UK Civil Aviation Authority, 2019).

Telematics, much like the systems already employed in car insurance (Helfand, 2017), could also be employed to gather and analyse data relating to the use and care of the aircraft to further tailor the underwriting process (Henry & Hogan, 2018).

Once the policy was in place, GPS trackers could be connected to the blockchain to track the location of the aircraft in real time (Windward, 2019). This would offer two opportunities:

1. To trigger the customer's liability for an additional premium if the aircraft entered a restricted zone (Long Insurance, 2017); and
2. To advise loss mitigation efforts if the aircraft were nearing unusually bad weather[d].

In relation to loss mitigation, GE have developed micro robots capable of inspecting and carrying out repairs inside jet engines (Sieger, 2017). Information gathered during routine inspections could be sent via the blockchain to trigger actions to mitigate potential losses as well as providing accurate information about the physical condition of the insured property.

[d] This may also be applicable in marine policies.

Photo comparison software could also be employed in relation to light aircraft policies (Helfand, 2017). Helfand also outlines the use of software which can estimate repair costs or indemnity by comparing images of the condition of the insured property at inception with photographs following the loss. Subject to the development of similar comparative technology, this would seem to offer potential in the light aircraft market.

Insight: IoT sensors on cargo and Lloyd's

Lloyd's (*2017a*) identified the challenges in accurately pricing cargo insurance in its Market Insight Report *"Goods to go: New approaches to cargo risk modelling".* Risk models struggle to model factors such as seasonality, logistic path variations, packaging, and regional risks.

Keen to take this concern further, Lloyd's Data team within the Data Lab engaged Zuhlke Engineering, a software and hardware development consultancy with expertise in the IoT. A mutual hypothesis was proposed: using sensor devices to track cargo flows on a regular basis would provide insight on cargo journeys which would lead to better, more informed risk modelling. It was clear that it was not feasible to track the movement of every piece of cargo, rather selected items on logistics paths of interest.

Proof of concept

The first step in testing this hypothesis was for Lloyd's Data Lab and Zuhlke to engage with the market to gauge their view on the value of data sampled from a variety of typical cargo movements. Workshops were undertaken with a number of insurers, to share with them what was possible in cargo tracking, understand their risk modelling processes, and look for value in combining the two.

With respect to the technology available, cost-effective sensors are available to measure a wide range of factors. Location, temperature, humidity, shocks, vibration, moisture, and light levels all proved to be of interest to the insurers. There are also a number of different approaches to accessing the collected data, from real-time trackers connected via wireless networks to data logger devices.

While insurers deemed that real-time tracker data might be useful for claims processes, either to track high-value shipments or to get live data on unfolding catastrophic events, from a risk-modelling perspective the accuracy and coverage of the data was considered more important than receiving it in real-time.

Risk based modelling

The hypothesis was well received by the insurers. When examined in detail Lloyd's, Zuhlke, and the insurers all agreed that a sampled cargo monitoring initiative would better inform the risk modelling processes. Much risk modelling is driven on qualitative assessments, where relative risks are considered based on agents' experience of historical claims, knowledge of the logistics network, the perceived vulnerability of specific cargo types and shipping methods, and surveyors' involvement. Patterns identified from the tracking data are seen as a valuable way to add quantitative insight to a qualitative process.

The actions taken based on these insights could include a more accurate risk model which would highlight to an insurer which business would be expected to be profitable, and which should be avoided. The enhanced model could also influence renewal pricing. Discussing identified risks with customers and capturing these in contract clauses promotes the avoidance of risky shipping practices.

Next steps

The next step, which is currently in progress, is to conduct a short trial tracking of a small number of cargo types and routes. If this proves to generate actionable insight, then cargo risk modelling could become yet another area where the IoT brings real business value.

Agriculture

Data drawn from third-party oracles would seem to have considerable traction in agriculture insurance. In relation to crop insurance, physical sensors to monitor rainfall and temperature could feed information about local conditions to the blockchain (Roughton & Bidewell, 2017). This would be facilitated by connecting crop moisture monitors to the internet, which is expected by 2020 (Werbach & Cornell, 2017).

Henry and Hogan's suggestion that drones could be deployed via smart contract in the immediate aftermath of a natural disaster to estimate damage (Henry & Hogan, 2018) could also be useful in crop policies. Data could also be pulled from software oracles – such as weather data from the Met Office or other trusted source – to trigger payment in crop policies following a persistent period of high rainfall, temperature exceeding a certain reading or drought (Gatteschi, et al., 2018).

Savelyev has also suggested that smart contracts would facilitate the development of peer-to-peer insurance products (Savelyev, 2017)[e]. His suggestion was that farmers could form a collective to protect themselves against drought or other natural disaster. If the disaster occurred, the smart contract would be triggered by weather data from a trusted oracle to distribute resources as required (Savelyev, 2017).

3.1.1 Assessment and settlement of claims

The self-enforcing and contained nature of smart contracts has the potential to bring about wide-ranging efficiencies in the distribution chain such as renewals, updating information on changing circumstances, and making claims (Gatteschi, et al., 2018).

For example, transaction costs could also be lower given that computers can assess logic clauses more quickly than human operators and are necessarily less prone to human error (Surden, 2012). This could be a significant benefit for the industry when multiplied across an individual insurance company or markets (Surden, 2012).

The claims phase is an important moment in the insurance relationship. This is the moment at which the insurer is called upon to perform its contractual obligation, as traditionally understood (Marine Insurance Act, 1906)[f], but it involves significant costs for insurers in assessing the claim, negotiating and making payment to the customer (Henry & Hogan, 2018). At present, this is a lengthy process even in cases where there is no dispute about the underwriter's liability for the claim, as due diligence and those in the insurance chain work their way through the process to validate claims (Disparte, 2017; Gatteschi, et al., 2018).

Automating payment of the indemnity in these cases would mean that the customer would receive payment more quickly (Norton Rose Fulbright, 2016) and could therefore respond more effectively after a loss event (Henry & Hogan, 2018). The automation of claims in policies where there is unlikely to be coverage disputes would result in quick wins for customers and insurers.

Conditioning payment on an objective trigger has additional advantages. In the first place, the potential for coverage disputes between insurer and insured would be reduced and would reassure the customer that swift payment was forthcoming after the precondition had been met. This would increase certainty (Savelyev, 2017).

In complex claims, the lengthy and administrative nature of the process undermines the very foundation of the insurance relationship as dependent on utmost good faith (Werbach & Cornell, 2017). The automation of the claims process in suitable policies would overcome these difficulties and could result in an increase in trust between the parties (Roughton & Bidewell, 2017).

Choosing triggers

It is important to note that effective automation depends on how the triggers for pay-out are chosen. They need to be both objective and reliable. Objectivity might mean that the trigger information originates from a third party, for example an entry on an official database of stolen items, and not from the insured so that there is no incentive for fraud or exaggeration. But objectivity might also mean that the information is generated by a piece of automated equipment, irrespective of who owns that equipment.

As an example, the output of flood sensors on the insured's property might be accepted as a trigger. The insurer will need to decide which triggers are objective enough, in either or both senses, to justify automatic pay-out. Who owns the sensor, can it be trusted, is it maintained by an external service company? To address the potential for moral hazard (where e.g., the customer would wet the sensor to trigger a pay-out) the trigger may be designed to require data from an additional confirming source rather than a single version of the truth, e.g. official meteorological data or satellite imagery, or triggering via multiple sensors.

[e] For examples of these products and how they are designed see (Ralph, 2016)

[f] But see (Firma C-Trade SA v Newcastle Protection and Indemnity Assn (The Fanti and The Padre Island) (No 2) [1991] 2 AC 1, 35) per Lord Goff noting that the insurer's obligation is to hold the assured harmless from the perils specified in the policy.

Reliability

Reliability is a related issue, with objective triggers of both types being more reliable than statements from the insured alone. But there needs to be a recognition that triggers might sometimes be inaccurate – e.g. a weather or flood sensor might malfunction and produce a false trigger, and processes need to be put in place to respond.

On the assumption that the pay-out will occur automatically in those cases, the insurance contract will need to provide for repayment if the trigger was false and the insured event did not actually occur. And the converse is also true – an insured will want an alternative route to make a claim if the insured event *did* occur, but the triggering mechanism failed to operate.

Claims volumes

It has also been suggested that the automation of claims would reduce the number of valid claims an underwriter would need to pay. This is because the automatic notification of claim via smart contract would reduce the customer's ability to frame a claim in the best light (within the rules permitted by the legal system) or to provide additional information to the underwriter which would strengthen the claim (Henry & Hogan, 2018).

Careful thought will need to be given to alternative claims routes if the insured is dissatisfied with the result of the automated process while at the same time upholding contract certainty. The automation of claims would have benefits in terms of contract certainty because, as already explained above, the circumstances in which a pay-out will occur would have to be clearly defined before they can be codified in the smart contract.

3.1.2 Enforcement of warranties

Warranties are promises made by the customer which form part of the insurance contract[g]. The effect of breaching a warranty used to be the immediate discharge of the insurer[h], whether or not the customer remedied the breach. The reforms introduced by the Insurance Act 2015 have changed this effect to a suspension of cover[i], unless an opt-out from the new provisions (permissible only in business-to-business insurance, and not in consumer insurance) is validly incorporated into the contract[j].

Warranties are typically included in an insurance contract to ensure that the risk is maintained within a certain scope. For example, an insured vehicle may be restricted to certain uses, a ship may be prohibited from entering certain zones, and a building may need to be protected by burglar or fire alarms.

Provided oracle data is available to ascertain compliance or otherwise with a warranty, smart contract technology could trigger the various consequences that follow at law or by agreement upon the warranty being breached. If the contract contains a valid opt-out clause, the oracle data that confirms breach could terminate cover, precluding any pay-out from being made to the customer under the contract.

If the new Insurance Act 2015 provisions apply, the smart contract technology could suspend cover until data is received confirming that the customer is once again compliant. If the contract contains a held covered clause – which are typical in marine cover – providing that cover survives subject to additional premium being paid, the smart contract technology could trigger the payment of the additional premium by the customer.

3.1.3 New products

The use of smart contracts may also open new markets to insurers which are prohibitively expensive at present (Disparte, 2017). While there would be clear financial incentives for insurers to write more cover, social benefits would also flow from greater insurance coverage.

For example, Disparte has argued that a 1% increase in the uptake of flood insurance could reduce taxpayer exposure following a natural disaster by 22% (Disparte, 2017). This is a considerable advantage of the implementation of smart contracting.

Automation through smart contracts would also give insurers access to new sources of data which could be fed into existing analytical tools.This data could then be used to identify inconsistencies and duplications in existing patterns of liability and thereby increase efficiency (Helfand, 2017; Maull, et al., 2017; Surden, 2012).

As greater quantities of data were gathered over time, insurers would also be able to predict losses more accurately due to the law of large numbers. This would permit more accurate and efficient pricing (Helfand, 2017).

[g] See (Marine Insurance Act, 1906), s 33(1), and (HIH Casualty & General Insurance Co Ltd v New Hampshire Insurance Co [2001] EWCA Civ 735, 2001).

[h] See Pre-2015 version of (Marine Insurance Act, 1906), s 43(2).

[i] See (Insurance Act, 2015).

[j] See (Insurance Act, 2015), ss 16 and 17.

For example:

- Increasingly, more aircraft, ships, and vehicles generate real-time GPS data that could be used by smart contracts to identify high-risk locations (piracy, war zone, or earthquake) and adjust the insurance premium in real-time or take mitigating action accordingly (Long Insurance, 2017).
- In the smart home, smart devices, such as smart lights and windows, cameras, gas leak and smoke detectors, or door sensors, could collect data and connect to a single central home control unit.
- Sensors could be programmed to detect triggering events and automatically initiate the claim or even a pay-out. Such sensors could be installed by the insurer as part of the insurance policy.
- Big data could assess in advance the potential for moral hazard (i.e. deliberate activation of the sensor) and the product could be designed to address the risk (e.g. requiring corroboration from at least one additional data source before a pay-out is triggered).
- Geo-coding and the development of models would permit modular deals that would open up the retail market.
- The sharing economy also offers opportunities for new insurance products facilitated by smart contracts. Customers want an accessible interface, low complexity, modular product they can purchase with their smartphones.

Smart contracts have the required characteristics to support new forms of insurance-on-demand and usage-based insurance, where risks under these products can be bundled together, enabling both the automated payment of premiums and, provided appropriate oracles are available, automated pay-outs.

Automating action with cargo smart contracts

The cooling unit in a container in the centre of the stack fails. It is known and agreed that goods are total loss at > 35 °C and this is a covered risk...

If this then that

Trigger

- Sensor > 35°C
  AND
- Location = XYZ

Action

- Notify broker
- Alert suppliers
- Request decision "Order new shipment? Y/N"
- Request closest approved surveyor using location XYZ

Class of business Cargo

Cargo is a field where the prospects of transitioning to products featuring smart contracts triggered by data from an objective source are looking increasingly realistic for a number of reasons. First the use of sensors and other data-generating devices on cargo ships, and the introduction of intelligent containers (CMA CGM, 2018) means that the availability of reliable, real-time information about the status of cargoes is increasing. Second, there are a number of projects under development which have the aim of recording transport data onto a blockchain (TradeLens, 2019).

Thus one can envisage a system where real-time information about the cargo gathered by objective sensors is transmitted onto the record pertaining to that cargo on the blockchain.

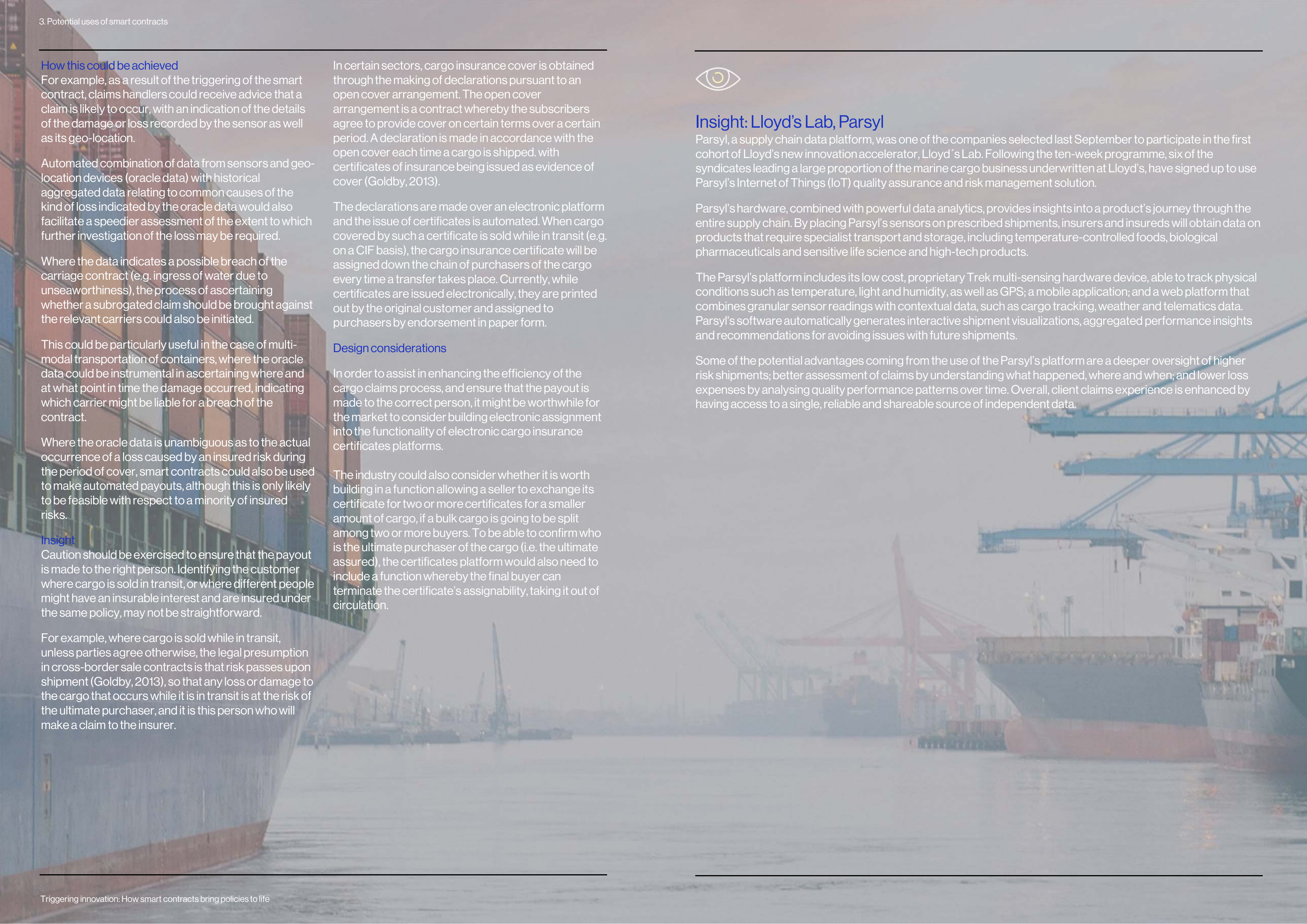
This blockchain data could be used beneficially in the insurance space in a number of ways, most notably in the risk assessment and pricing exercise that underlies underwriting decisions, but it can also be used to trigger the execution of smart contracts programmed to initiate the workflows necessary to service claims, where the data indicates loss of or damage to cargo.

For example, a smart contract could trigger a workflow that notifies a broker about potential recovery action, or provide risk mitigation for customers to make them aware that a threshold is about to be breached so corrective action could be taken where possible.

The use of IoT sensors could facilitate loss mitigation, with the ability to establish workflows that appoint a surveyor to inspect the cargo immediately following the discharge of the vessel. Examples might include:

Examples might include:

1. A certain level of humidity or a certain temperature was reached inside a hold or a container. An alert is generated, prompting an inspection at the port of arrival. A workflow is triggered as a consequence of which, deteriorated cargo is sold in a secondary market for a higher price than would otherwise have been achieved, assisting in mitigating the claim.
2. A vibration or shock alert could indicate that the cargo has shifted in transit. An inspection upon discharge from the vessel could give an opportunity to add further securing to the cargo and reduce damage potential during the onward transit.



How this could be achieved

For example, as a result of the triggering of the smart contract, claims handlers could receive advice that a claim is likely to occur, with an indication of the details of the damage or loss recorded by the sensor as well as its geo-location.

Automated combination of data from sensors and geo-location devices (oracle data) with historical aggregated data relating to common causes of the kind of loss indicated by the oracle data would also facilitate a speedier assessment of the extent to which further investigation of the loss may be required.

Where the data indicates a possible breach of the carriage contract (e.g. ingress of water due to unseaworthiness), the process of ascertaining whether a subrogated claim should be brought against the relevant carriers could also be initiated.

This could be particularly useful in the case of multi-modal transportation of containers, where the oracle data could be instrumental in ascertaining where and at what point in time the damage occurred, indicating which carrier might be liable for a breach of the contract.

Where the oracle data is unambiguous as to the actual occurrence of a loss caused by an insured risk during the period of cover, smart contracts could also be used to make automated payouts, although this is only likely to be feasible with respect to a minority of insured risks.

Insight

Caution should be exercised to ensure that the payout is made to the right person. Identifying the customer where cargo is sold in transit, or where different people might have an insurable interest and are insured under the same policy, may not be straightforward.

For example, where cargo is sold while in transit, unless parties agree otherwise, the legal presumption in cross-border sale contracts is that risk passes upon shipment (Goldby, 2013), so that any loss or damage to the cargo that occurs while it is in transit is at the risk of the ultimate purchaser, and it is this person who will make a claim to the insurer.

In certain sectors, cargo insurance cover is obtained through the making of declarations pursuant to an open cover arrangement. The open cover arrangement is a contract whereby the subscribers agree to provide cover on certain terms over a certain period. A declaration is made in accordance with the open cover each time a cargo is shipped. with certificates of insurance being issued as evidence of cover (Goldby, 2013).

The declarations are made over an electronic platform and the issue of certificates is automated. When cargo covered by such a certificate is sold while in transit (e.g. on a CIF basis), the cargo insurance certificate will be assigned down the chain of purchasers of the cargo every time a transfer takes place. Currently, while certificates are issued electronically, they are printed out by the original customer and assigned to purchasers by endorsement in paper form.

Design considerations

In order to assist in enhancing the efficiency of the cargo claims process, and ensure that the payout is made to the correct person, it might be worthwhile for the market to consider building electronic assignment into the functionality of electronic cargo insurance certificates platforms.

The industry could also consider whether it is worth building in a function allowing a seller to exchange its certificate for two or more certificates for a smaller amount of cargo, if a bulk cargo is going to be split among two or more buyers. To be able to confirm who is the ultimate purchaser of the cargo (i.e. the ultimate assured), the certificates platform would also need to include a function whereby the final buyer can terminate the certificate's assignability, taking it out of circulation.

Insight: Lloyd's Lab, Parsyl

Parsyl, a supply chain data platform, was one of the companies selected last September to participate in the first cohort of Lloyd's new innovation accelerator, Lloyd´s Lab. Following the ten-week programme, six of the syndicates leading a large proportion of the marine cargo business underwritten at Lloyd's, have signed up to use Parsyl's Internet of Things (IoT) quality assurance and risk management solution.

Parsyl's hardware, combined with powerful data analytics, provides insights into a product's journey through the entire supply chain. By placing Parsyl's sensors on prescribed shipments, insurers and insureds will obtain data on products that require specialist transport and storage, including temperature-controlled foods, biological pharmaceuticals and sensitive life science and high-tech products.

The Parsyl's platform includes its low cost, proprietary Trek multi-sensing hardware device, able to track physical conditions such as temperature, light and humidity, as well as GPS; a mobile application; and a web platform that combines granular sensor readings with contextual data, such as cargo tracking, weather and telematics data. Parsyl's software automatically generates interactive shipment visualizations, aggregated performance insights and recommendations for avoiding issues with future shipments.

Some of the potential advantages coming from the use of the Parsyl's platform are a deeper oversight of higher risk shipments; better assessment of claims by understanding what happened, where and when; and lower loss expenses by analysing quality performance patterns over time. Overall, client claims experience is enhanced by having access to a single, reliable and shareable source of independent data.

Automating action with aviation smart contracts

The runway is out of commission due to a severe storm with high windspeeds and lightning that make it unsafe to fly. All planes are grounded and flights cancelled, which is a covered risk...

If this then that

If this (Trigger)	then that (Action)
• NOTAM confirms runway unavailable AND • Delay ≥ departure time AND • Cause is within list of covered losses	• Pay claim • Alert customer to potential new flights

Class of business Contingency/Aviation

General aviation includes light aircraft, gliders, private jets, drones etc. It excludes scheduled passenger transport and cargo aircraft. Insurance normally covers third party liability, damage to the aircraft, and total loss.

Why this line of business

As agreed value policies, most aircraft hull insurance policies already pay out an agreed, fixed sum in the case of a total write-off, rather than assessing the value of the aircraft.

However, payout occurs after ascertainment by a loss adjuster that the cost of repair exceeds the agreed value, so it is not automatic. Most repairs following an accident cannot be priced in advance, because of their complexity and the need to return the aircraft to a state where it meets regulatory standards.

These features render payout automation unsuitable for aircraft hull insurance, although smart contracts may be used to trigger human actions and initiate workflows in the claims process. Thus, the main scope for use of smart contracts for automated payouts in this space is in relation to what might be seen as add-ons, or possibly replacements for certain elements of the existing insurance.

Overleaf we have set out some examples that could serve as proof of concepts, but other areas where the principles can be applied also include scenarios where the cost per day in business interruption is well calculated.

Smart contracts for automated payouts in aviation could be applied to add-ons or as replacements for parts of existing insurance contracts.

Automatic payout pursuant to the triggering of a smart contract may be suitable for two add-on products:

1. Business interruption due to unavailability of the runway or adverse weather conditions; and
2. Business interruption due to technical defects which make aircraft unserviceable.

These scenarios are suitable because they are based on facts which can be confirmed by independent data.

How this could be achieved

In the case of business interruption due to unavailability of the runway, the objective trigger could be data derived from the Notices to Airmen (NOTAM) generated by the airfield and disseminated online by the National Air Traffic Services (NATS).

This data can confirm e.g. that the airfield was closed during a certain period. In the case of business interruption due to weather conditions, the objective trigger could be data derived from the Meteorological Aerodrome Report (METAR), a specially encoded weather observation report.

Third party weather data is independently available from a number of airfields, collected several times a day and made available online in the form of METARs. A comparatively simple formula could be used to identify 'non-flying' weather via the METARs from the nearest recording airfield, probably taking as inputs visibility, cloud base, amount of cloud cover and wind speed. Thunderstorms might be included.

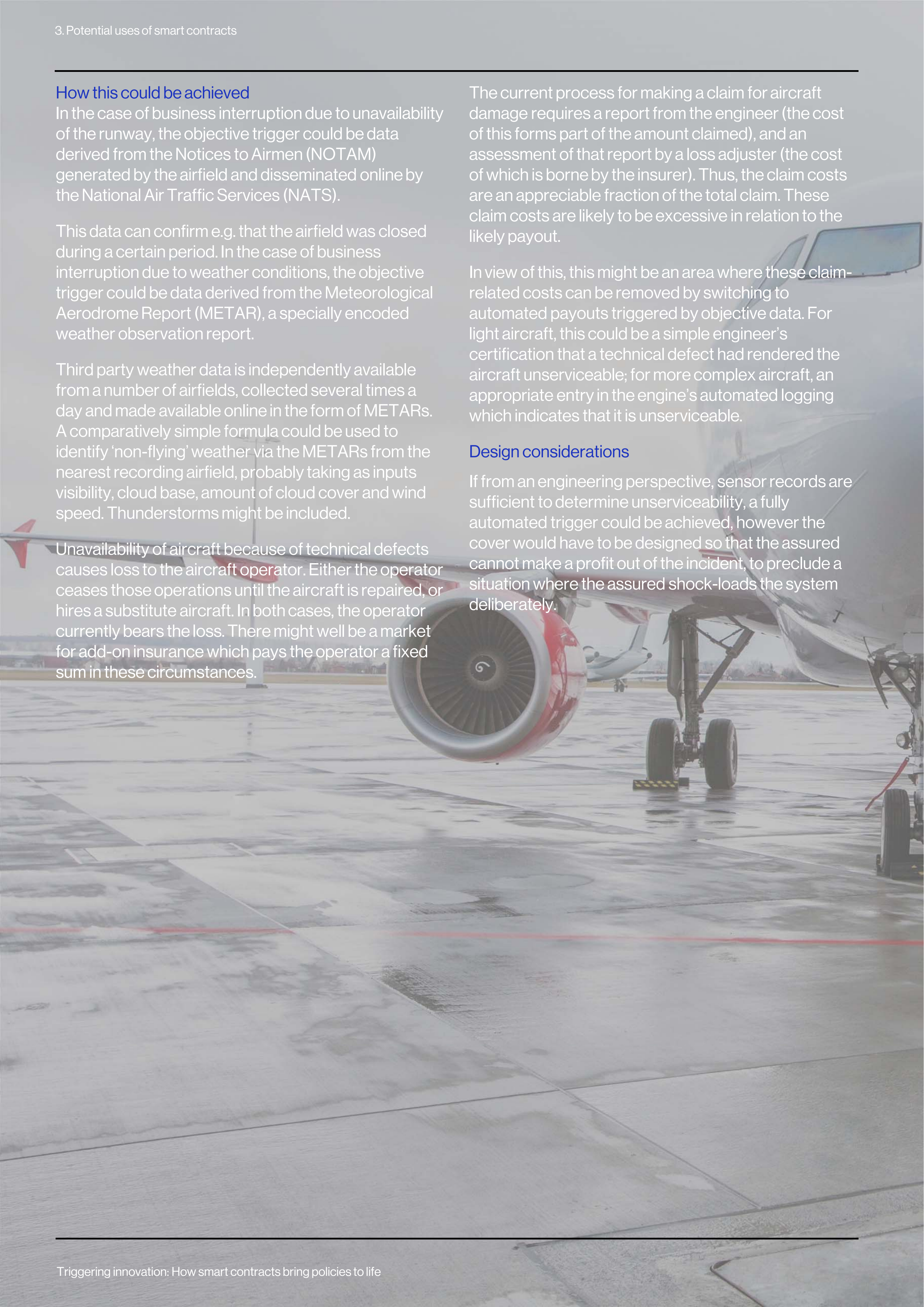
Unavailability of aircraft because of technical defects causes loss to the aircraft operator. Either the operator ceases those operations until the aircraft is repaired, or hires a substitute aircraft. In both cases, the operator currently bears the loss. There might well be a market for add-on insurance which pays the operator a fixed sum in these circumstances.

The current process for making a claim for aircraft damage requires a report from the engineer (the cost of this forms part of the amount claimed), and an assessment of that report by a loss adjuster (the cost of which is borne by the insurer). Thus, the claim costs are an appreciable fraction of the total claim. These claim costs are likely to be excessive in relation to the likely payout.

In view of this, this might be an area where these claim-related costs can be removed by switching to automated payouts triggered by objective data. For light aircraft, this could be a simple engineer's certification that a technical defect had rendered the aircraft unserviceable; for more complex aircraft, an appropriate entry in the engine's automated logging which indicates that it is unserviceable.

Design considerations

If from an engineering perspective, sensor records are sufficient to determine unserviceability, a fully automated trigger could be achieved, however the cover would have to be designed so that the assured cannot make a profit out of the incident, to preclude a situation where the assured shock-loads the system deliberately.



Automating action with agriculture smart contracts

Prolonged drought occurs and water shortages are in effect making mitigation impossible. It is known and agreed that the crop will be damaged beyond recovery under certain temperature and moisture conditions, and this is a covered risk...

If $\underbrace{\text{this}}_{\text{Trigger}}$ then $\underbrace{\text{that}}_{\text{Action}}$

Trigger

- Temperature sensor ≥ 35°C AND Moisture sensor ≥ 0.1 for 20 days

AND

- Location = XYZ

Action

- Can mitigation action be taken? If so, and in coverage, instigate service
- If not, notify broker
- Alert farmer and pay claim
- Alert supply chain

Class of business Agriculture

The most likely area in which parametric insurance might fit the agricultural sector is insurance against crop failure. Crop failure can depend on many variables – one vineyard can be devastated by a frost, while the vineyard next door escapes completely; a drought can halve crop yields in some fields while their neighbours, with different soil structure and drainage, suffer very little.

Why this line of business

This means that assessing crop failure requires on the ground inspection, which is necessarily labour-intensive given the large geographical areas to be assessed (inspection of one square metre of a field will not reveal the state of the whole field). Also, assessment is either speculative, if made at the time of the causal event, because some or all of the crop might recover, or if assessment is postponed until harvest, it is made so long after the causal event that it may be impossible to tell if the cause was one insured against.

Thus, an insurance product which operates as a smart contract would have to cover against the main causes of crop failure, with an automated payout occurring if these eventuate, based on the assumption that, on their occurrence, crop damage or failure is inevitable.

The two main causes would be:

1. Adverse weather conditions; and
2. Pests and disease.

Adverse weather is ideal for parametric insurance in countries where weather data is continuously captured at closely-spaced weather stations by a trusted third party, which in the UK would be the Meteorological (Met) Office. Much of this data is aggregated and publicly accessible.

How this could be achieved

The main data factors determining weather conditions are temperature, rainfall and wind. The last has least effect on crop yields, so the smart contract trigger would be based on either temperature (excessive heat and excessive cold), and/or excessively low rainfall or flooding.

To take the UK as an example, data on seasonal averages is available for all regions, allowing suitable thresholds to be set for duration and intensity. Advice will be needed from agronomists on whether to set the parameters as simple values (X or more days of excessively high temperature) or as more complex formulae (high temperatures coupled with low rainfall).

It is more challenging to set parameters for pests and disease. In the UK, pest infections tend to occur in small areas and are affected by farming methods, while crop diseases tend either to occur in a similar fashion or (like Dutch Elm disease or Ash Die-Back) spread slowly over a period of years. However, for countries where catastrophic pest or disease crop failures occur on a regular basis (e.g. swarms of locusts) official data which can be used as a parametric trigger is usually available (FAO, 2018).

A multitude of indices are available providing objective sources of data (Greatrex, et al., 2015), but should these be unavailable for a particular locality, or should the structuring of the product require corroboration from more than one data source that the conditions for trigger have been met, aerial sensors, e.g. drone enabled imagery, and ground sensors e.g. soil probes, and miniature weather stations which provide actionable insights with maximum accuracy for crop monitoring can be used.

It could also be possible to use technology developments in this area, such as drone technology and satellite imagery, alongside machine learning to provide evidence of damage developing over time.

This could be used alongside trusted third-party sources to provide an accurate picture of an event. For example, temperature maps indicate prolonged dry conditions that would be defined as drought conditions; however, water irrigation sensors and soil moisture detectors show the crops were irrigated so no loss occurred.

Smart contracts could be used at the portfolio level to support underwriting and risk decisions. For example, factors affecting known disease vectors might be detected, and trigger an underwriting decision or risk control to support closing the performance gap.

Design considerations

Disease insurance for livestock might be less challenging – for example, in the most recent UK Foot and Mouth outbreak, government agencies defined the affected areas and imposed livestock movement restrictions, so announcements of that kind could serve as objective triggers.

Parametric insurance would pay the insured sum to farmers in those areas, whether or not their herds or flocks were affected, and it would be for farmers to decide what level of risk they wished to insure against (e.g. if they think their biosecurity is strong, they might wish only to insure for the losses resulting from movement restrictions).

Automating action with property catastrophe smart contracts

A magnitude 6.2 earthquake occurs 20km from the property. Based on the materials damage is known to be severe enough to prevent access, and the customer wanted accommodation booked to allow them to stay in the area for their business. These conditions were an agreed part of the coverage, and is a covered risk...

If this then that

Trigger

- Sensor ≥ M6
  AND
- Location = XYZ

Action

- Notify broker
- Contact customer, pay claim, check local hotels and book room
- Request closest approved surveyor

Class of business Property catastrophe

Parametric catastrophe re-insurance is already in existence and well-developed, especially in certain regions of the world (Artemis, 2018). The use of parametric triggers in catastrophe re-insurance has facilitated alternative risk transfer and the structuring of catastrophe bonds palatable to capital markets investors (Risk Management Solutions, 2012). In a parametric bond the consequences of a catastrophe for investors are determinable immediately after the occurrence of a catastrophe (Artemis, 2017; Risk Management Solutions, 2012).

Why this line of business

Recent reports suggest that in the future parametric cat bonds could be designed as smart contracts to accelerate, simplify and reduce the costs of payment and settlement between insurers and investors (Gould, 2016).

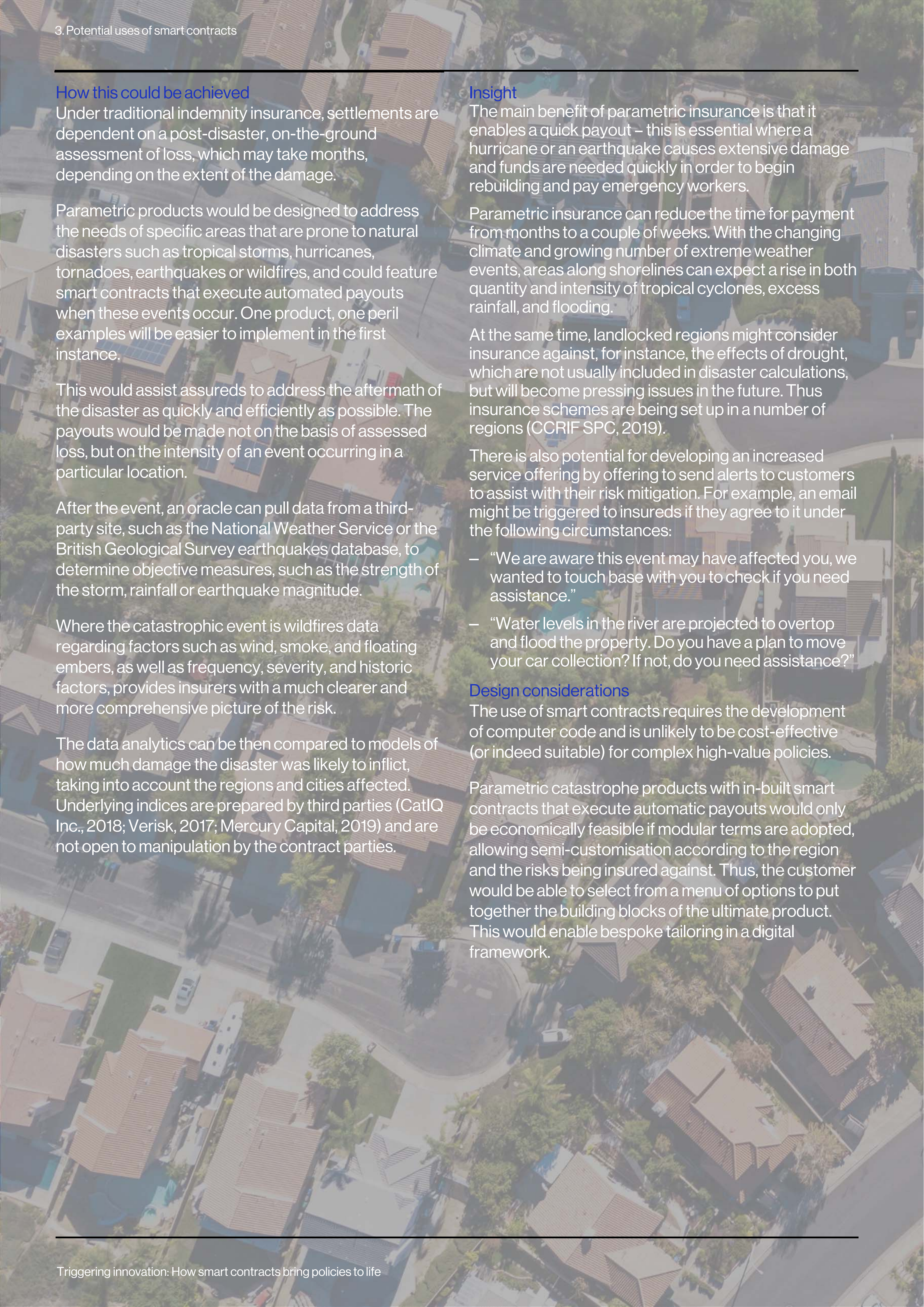
On the other side, an insurer might not obtain coverage for its full exposure because compensation does not depend upon the insurer's actual loss (Risk Management Solutions, 2012).

This type of bond therefore is not designed to "indemnify" in the pure sense of the word, because the quantum of the payout depends not on the extent of the loss but on the meeting of the pre-set parameters, and correlation must be carefully assessed.

Parametric products can be used not just for reinsurance purposes, but can be developed to provide insurance to individual assureds at risk. Indeed, this would improve the alignment between the insurer's exposure and the protection available through reinsurance by the issue of a catastrophe bond.

Parametric products could be designed to address the needs of specific areas that are prone to natural disasters such as:

- Tropical storms
- Hurricanes
- Tornadoes
- Earthquakes
- Wildfires



How this could be achieved

Under traditional indemnity insurance, settlements are dependent on a post-disaster, on-the-ground assessment of loss, which may take months, depending on the extent of the damage.

Parametric products would be designed to address the needs of specific areas that are prone to natural disasters such as tropical storms, hurricanes, tornadoes, earthquakes or wildfires, and could feature smart contracts that execute automated payouts when these events occur. One product, one peril examples will be easier to implement in the first instance.

This would assist assureds to address the aftermath of the disaster as quickly and efficiently as possible. The payouts would be made not on the basis of assessed loss, but on the intensity of an event occurring in a particular location.

After the event, an oracle can pull data from a third-party site, such as the National Weather Service or the British Geological Survey earthquakes database, to determine objective measures, such as the strength of the storm, rainfall or earthquake magnitude.

Where the catastrophic event is wildfires data regarding factors such as wind, smoke, and floating embers, as well as frequency, severity, and historic factors, provides insurers with a much clearer and more comprehensive picture of the risk.

The data analytics can be then compared to models of how much damage the disaster was likely to inflict, taking into account the regions and cities affected. Underlying indices are prepared by third parties (CatIQ Inc., 2018; Verisk, 2017; Mercury Capital, 2019) and are not open to manipulation by the contract parties.

Insight

The main benefit of parametric insurance is that it enables a quick payout – this is essential where a hurricane or an earthquake causes extensive damage and funds are needed quickly in order to begin rebuilding and pay emergency workers.

Parametric insurance can reduce the time for payment from months to a couple of weeks. With the changing climate and growing number of extreme weather events, areas along shorelines can expect a rise in both quantity and intensity of tropical cyclones, excess rainfall, and flooding.

At the same time, landlocked regions might consider insurance against, for instance, the effects of drought, which are not usually included in disaster calculations, but will become pressing issues in the future. Thus insurance schemes are being set up in a number of regions (CCRIF SPC, 2019).

There is also potential for developing an increased service offering by offering to send alerts to customers to assist with their risk mitigation. For example, an email might be triggered to insureds if they agree to it under the following circumstances:

- “We are aware this event may have affected you, we wanted to touch base with you to check if you need assistance.”
- “Water levels in the river are projected to overtop and flood the property. Do you have a plan to move your car collection? If not, do you need assistance?”

Design considerations

The use of smart contracts requires the development of computer code and is unlikely to be cost-effective (or indeed suitable) for complex high-value policies.

Parametric catastrophe products with in-built smart contracts that execute automatic payouts would only be economically feasible if modular terms are adopted, allowing semi-customisation according to the region and the risks being insured against. Thus, the customer would be able to select from a menu of options to put together the building blocks of the ultimate product. This would enable bespoke tailoring in a digital framework.

4. Making it happen

Although smart contracts were originally conceptualised as part of permissionless blockchain technology (Bacon, et al., 2017), the report assumes that a permissionless system, which means that participants do not need to identify themselves, is highly unlikely ever to be appropriate for the insurance sector.

While a scenario may be conceived in which neither customer nor insurer identifies themselves, and don't need to because the necessary risk information about the insured is on the blockchain, and pay-out by the insurer is guaranteed by the smart contract, even then, Know-Your-Customer (KYC) requirements imposed by regulation (including anti-money laundering regulation) make it unlikely that the industry could ever consider such a model.

4.1 Design choices for smart contracts

The customer needs to be sure that the insurer is in fact an authorised insurer, and receipt of premiums and payment of claims will require the customer to be identified to comply with KYC regulation. Therefore, a smart contract will be an element of either a permissioned blockchain system, or a centralised database system (or some equivalent).

In either case, the system will be controlled by some entity, the system 'owner'. That owner will need to make several design choices which have legal and regulatory consequences.

Revocation

There may be circumstances where the smart contract needs to be revoked before it triggers – one obvious example is where the insured cancels the insurance. In permissionless blockchains, this can only be done via digitally signed instructions from both parties.

This may be inappropriate for insurance, because it requires the insured to cooperate, and it is an important design question whether revocation requires some technical indication of agreement by both parties or whether it can be revoked unilaterally by the insurer.

Rectification

If unilateral revocation is not allowed, there will need to be some mechanism via which errors can be rectified. For example, if a defect in the coding is spotted, or if the insured cancels the insurance.

Rectification will normally be carried out by the system owner, and there will need to be rules and processes which ensure that the legal and regulatory obligations of the insurer are complied with before rectification takes place. Rectification may also be a route for changing the name and identity of the relevant contract party in case a contract is novated or a policy assigned.

Payment of claims

If the smart contract is linked to a payment system, then triggering the smart contract can result in a payment instruction being issued. Alternatively, the smart contract could alert the insurer, who would then make payment via its normal processes.

In either event, provision for anti-money laundering compliance needs to be built in to the technology or the processes. For example, if the insurer has come into possession of information which raises suspicion that the insured is engaged in money laundering, then in addition to reporting the transaction the insurer will need to be able to delay payment until instructed by the authorities.

Closed or open code

Open code, where the source code is disclosed to the whole world (or at least to the insured) is a useful way to engender trust that the code will operate as intended.

It also gives the customer theoretical notice about how the code will operate. While in practice most customers will be unlikely to be able to understand code, the open availability of code might assist the courts in interpreting any apparent conflict between the code and a human-centred description of its functionality.

Closed code preserves trade and technical secrets but is necessarily less trustworthy. If closed code is used, we think that a court would wish to focus on the human-centred description of its functionality in deciding whether the insurer had fulfilled its contractual obligations, because only the insurer has access to the code.

Code testing

In addition to ensuring that the code performs according to the insurer's contractual obligations, insurers should also be mindful of their general obligation to treat customers fairly. Both these suggest that there should be a testing regime for code before it is implemented as a smart contract. Insurers or contracted code developers will need to retain records of the testing regime, to demonstrate compliance.

Certification and standards

If smart contracts become widely used for performance of common obligations, there is likely to be a role for independent certification and/or the creation of standards, most likely by industry bodies. Certification or standard compliance will go some way to demonstrating regulatory compliance and producing confidence that the code will operate as intended.

Bespoke code

If smart code contract is rewritten to meet a customer's requirements, this potentially invalidates any testing, certification or standards compliance. This would be so even if Artificial Intelligence (AI) machines became sufficiently advanced to code bespoke relationships.

A sensible design choice might be to write the smart contract code in a modular fashion so that, ideally, only its input parameters are changed and not the code itself. In effect, the customer would be given a menu of choices, all of which were known to work without code modification.

If a complex parametric function involving fuzzy or probabilistic logic were to be devised individually for some customers, again it would help if that function were a discrete code element so that the remainder of the code would not need further testing and would still meet its certification or standard.

Market alignment

A subscription insurance policy is in reality a bundle of separate contracts[k] on identical terms between the customer and each individual subscriber to the risk, meaning that in theory each subscriber is free to exercise any discretion permitted by the contract terms, and to take pay-out decisions, in any way it deems fit.

In a subscription market, where the terms of the primary contract allow the insurer to choose among different oracles, subscribers would need to consider whether they will be adopting the same oracle or different ones. If consistency in pay-out decisions is desirable, the former approach should be adopted, to obviate the risk of different oracles reporting different data.

This risk of inconsistency may be particularly acute where AI output is being used as the trigger, bearing in mind the uncertainties that may arise as machine learning progresses.

4.2 IT infrastructure

Readers who have come across the concept of smart contracts before will probably have done so in relation to blockchain. Blockchain is where the current interest in the concept originated, but this does not mean it is the only technology on which smart contracts can be implemented.

The concept is technology-independent. It can theoretically be implemented on any computer system which keeps records and is capable of input from and output to external devices. This could be a variety of distributed ledger technologies or existing databases.

The baseline technological implementation is less important than understanding the concept of smart contracts and how they might be used in the insurance sector.

Similarly, how smart contracts are implemented into that technology is less important than the specifics of the business models, which is what should drive the technology used to implement solutions.

The real questions are about, for example, whether smart contract technology can assist in reducing the time required for things such as compliance and regulatory checks (currently undertaken by DXC, formerly Xchanging or central bureau), which require human judgment.

[k] See (Touche Ross v Colin Baker [1991] 2 Lloyd's Rep 230) , per Neill LJ and (The Zephyr [1984] 1 Lloyd's Rep. 58, 66) where Hobhouse J describe the policy as 'a mechanism whereby the assured can be put, by means of a single contractual document, in direct and distinct contractual relations with a large number of insurers; what might seem to be a single contract is in fact a bundle of a large number of distinct contracts on the same terms except as to the amount of each individual insurer's liability.' This analysis is supported by s 24(2) of the Marine Insurance Act 1906.

Distributed ledgers

Blockchain is just one example of distributed ledger technology, but because most of the literature tends to use the term 'blockchain' we will do likewise. A conceptual description is also more useful here to illustrate the legal issues it raises.

At heart, a blockchain is no more than a series of records, which contain information such as the identity of the person who is entitled to dispose of an asset (colloquially, 'ownership' of that asset) and attributes of that asset, such as its value, location etc.

Each record's origin is authenticated by means of the digital signature of the person who created it, and the digital signature provides a level of authentication which is, in practical terms, infeasible to forge.

If the record is of entitlement to an asset, the digital signature of the person who owns that entitlement is also the mechanism used to dispose of it.

In a blockchain implementation, a smart contract is a record in a block which is part of the blockchain, authenticated by the digital signatures of those whose rights and obligations are affected by its triggering. Because it takes the form of code it will (if the blockchain technology supports this functionality) trigger and execute itself automatically.

What are their capabilities?

Blockchain, whose origins are linked with the cryptocurrency Bitcoin (World Bank Group, 2017; MacDonald, 2015), is an example of Distributed Ledger Technology (DLT) (World Bank Group, 2017) that has been described as:

> *a means of recording and sharing data across multiple data stores (ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes (World Bank Group, 2017).*

Blockchains can store other kinds of information too, for example a series of climate readings from a weather station.

Box 3: Blockchain background

A record becomes part of the blockchain when it is aggregated with other transactions by a block creator, to form a block. This block is completed by incorporating the "hash" of the preceding block and then added to the blockchain by authenticating the new block with the block creator's digital signature. A hash function takes a document (in this case the aggregated transactions of the block) and applies a mathematical function to produce a number, termed the message digest or the hash value.

It is highly unlikely that two documents will produce the same message digest, and for hash functions used in practice (NIST, 2012) the probability of this occurring can be demonstrated to be so low that it is computationally infeasible, given a particular message digest, to devise a different document which produces the same message digest (NIST, 2012).

Each block is thus linked to its predecessor, and thus any attempt to incorporate a forgery of a previous block will be detected because its hash will not match that recorded in the subsequent block.

Blockchain was designed to be distributed, to be held in multiple copies at multiple locations, and copies are compared and synchronised regularly. A new block could be added to any one of these copies, and so there is need for a "consensus protocol" if multiple block-creators add blocks nearly simultaneously.

For Bitcoin this protocol is first in time – newer rival blocks are simply discarded, and their transactions recorded in later blocks. "Mining" is what qualifies a block creator, and is not the protocol itself. Other implementations might seek consensus on which block is to be added from a group of trusted block-makers (Government Office for Science, 2016). This consensus protocol is vital to maintaining the evidential value of the blockchain, and therefore needs to be robust against fraud and cybersecurity attacks (Lloyd's, 2015).

The fundamental determinant of how a blockchain implementation is designed is the level of trust required in participants. At least in theory, "trust in conventional actors such as banks, courts, brokers, and trading parties can be dispensed with in favour of trust in a thing – the computational power of the internet." (Giancaspro, 2017; Maull, et al., 2017)

Implementation pathways

While smart contracts are perceived as part of blockchain technology, and some understanding of that technology is necessary to understand their likely uses, they are conceptually separate and can be implemented successfully elsewhere.

Other examples of implementations include standard database software that could achieve equivalent functionality through use of extensions to the Standard Query Language (SQL) (Greenspan, 2016).

Some market computer systems already incorporate technology which has similar functionality, automating certain actions. For example, well developed Straight-Through-Processing (STP) is a precursor to the use of smart contracts.

A paper commissioned by the London Market Group suggested that smart contracts could be implemented within the existing wholesale insurance market without reliance on blockchain technology (Long Insurance, 2017), using conventional fiat currencies and the market's current settlement infrastructures, to implement STP:

> *… in the context of wholesale insurance, processing and the use of smart contracts will continue to be done mainly in an environment of single-company computing and databases, while mutual distributed ledgers may provide multi-company data sharing with a rigorous audit trail* (Long Insurance, 2017)

It will be important to ask, though, whether it is most efficient to implement smart contracts on blockchain (or a similar distributed ledger technology) or whether they can function effectively within existing IT infrastructures.

Almost all the literature assumes that blockchain will be an integral part of smart contract use (Hingley, 2018). Gatteschi et al., for example, have implicitly recognised that smart contracts need not exist on the blockchain, but assume that the majority of such contracts would be recorded there to facilitate a system of mutual trust between parties (Gatteschi, et al., 2018).

Further, they contended that it was only in conjunction with blockchain that the "full potential" (Gatteschi, et al., 2018) of smart contracts could be unleashed (Giancaspro, 2017; Clack, et al., 2017; Roughton & Bidewell, 2017).

Savelyev has taken a more explicit position, connecting the very definition of a smart contract to its interaction with blockchain, "thus not every contract embodied in a computer language can be regarded as a Smart contract, but only the one based on Blockchain technology, and having a self-enforcement nature." (Savelyev, 2017).

An important element of smart contracts is that a transaction or data stored on the distributed ledger triggers the smart contract and that transaction would then be recorded (World Bank Group, 2017).

Where the objective trigger will require input from a third-party oracle e.g. weather data, most blockchain technology already provides appropriate linking mechanisms (Roughton & Bidewell, 2017).

Linking technology would need to be written for existing IT infrastructures. Admittedly the third-party data could be inputted manually to trigger the smart contract, but this would be less streamlined than the automatic input of data from the oracle.

4.3 Legal and regulatory considerations

The first thing that should be noted is that the modern notion of smart contracts is in its infancy and that there are no international standards applicable to or uniform legal regime governing the use of this technology.

Some initial efforts have been made in terms of formalising and standardising smart contracts:

- Translating natural language contract terms into the most common smart contract language, named Solidity (Solidity, 2018).
- The International Organisation for Standardisation (ISO) is currently working to develop draft standards to govern blockchain and distributed ledger technologies (ISO, 2018), and the task force on this project includes a working group focusing on smart contracts.
- The Accord project (Aitken, 2017) provides open source software tools to create what its website describes as enforceable smart contracts (Accord Project, 2018), translating natural legal language into smart contract code. Several international law firms are represented within the consortium (Aitken, 2017; Hernández, 2018).

In view of the current dearth of uniform internationally applicable standards, below we shall base the discussion on the legal and regulatory framework applicable in the UK.

However, each jurisdiction will raise its own legal and regulatory issues and care should be taken to consider local requirements when designing products incorporating smart contracts.

4.3.1 Indemnity and Insurable Interest

From a regulatory perspective, insurers are only permitted to write insurance contracts[l].

In "smart insurance", where the smart contract envisages pay-out triggered by objective data from the pre-selected oracle(s), payment would be made regardless of the extent of any actual loss suffered, provided the trigger is activated. There would therefore be no scope for calculating the loss and indemnifying the customer according to that loss. So the question arises, is this really an insurance contract?

In practice, most policyholders will have an exposure at the outset (and therefore an insurable interest). This can be verified at the placement stage. If this is the case, and insurable interest is present, some extent of loss is likely to be inevitable upon the occurrence of an event at trigger level[m].

If the relevant contract is one of property indemnity, insurable interest is required not only at the time of inception of the insurance but also at the time of the loss (L&C & SLC, 2016)[m].

So, if, for example, the subject matter of the insurance is a maritime cargo which has been traded while afloat, it must be ensured that the pay-out is made to the ultimate owner of the cargo rather than the original customer (provided the insurance is assignable).

The smart contract must be linked up with a database/ register/ ledger that records assignments of the cover down a string from the cargo's sellers to the cargo's buyers, so that the ultimate owner may be verified at the time of the pay-out.

In view of the recognition of "valued policies"[n] (where the value of the subject matter is pre-agreed and does not need to be ascertained at the time of loss) as insurance contracts, the absence of a requirement to establish the extent of the loss should not preclude these contracts from being considered insurance contracts.

For some products, the objective trigger itself may give some proof of loss (e.g. satellite imagery showing the destruction of the insured property).

Another option is to consider whether innovative products that are designed with smart contracts technology in mind may be regarded as non-life contingency insurance (L&C & SLC, 2016), which pay out not in response to a loss but on the occurrence of a pre-specified event[o].

In the absence of an insurable interest in the non-occurrence of the relevant event (e.g. a devastating storm or shipwreck), at the inception of the contract on the part of the customer, these would be more in the nature of derivative contracts or perhaps even wagers, rather than insurance.

So the insurable interest requirement remains key, but only at the time where the insurance policy is acquired (L&C & SLC, 2016).

[l] See (PRA, 2019) para 9.1: 'A firm … must not carry on any commercial business other than insurance business and activities directly arising from that business.' Insurance business is defined in the Glossary as 'the regulated activities of effecting contracts of insurance or carrying out contracts of insurance.' The Chapter on Conditions Governing Business applies also to Lloyd's: see para 1.1.

[m] See (Marine Insurance Act, 1906), s 6.

[n] See (Marine Insurance Act, 1906) s 27 (2) and (3).

[o] Unless the product can be conceptualised as valued indemnity insurance, however, subrogation by the insurer into the rights and remedies of the assured may be precluded. See (Marine Insurance Act, 1906) s 79.

Insight: Insurable interest

Insurance contracts have two essential characteristics:

1. The identification of a risk to which the assured is exposed, by reason of having an insurable interest in the subject-matter of the insurance; and
2. An undertaking by an insurer to compensate the assured should that risk materialise, in exchange for a premium.

Insurance contracts can be of two main types: indemnity or contingency.

In indemnity insurance, the extent of the compensation is measured by reference to the assured's loss, although the value of the subject-matter insured may be agreed in advance, which precludes the need to prove its value after the loss.

In contingency insurance, the compensation payable upon materialisation of the risk is agreed in advance and the payout is not intended to indemnify the assured, so there is no requirement to prove loss.

It is still necessary, however that the assured have an insurable interest in the subject matter insured at the time of entering into the insurance contract. It is important, when designing products that make use of smart contracts, to ensure that they maintain the essential characteristics of insurance.

4.3.2 Conduct of Business Regulation

In the UK, a smart contract set-up which envisages automatic pay-outs upon the occurrence of certain events would mean that insurers would not fall foul of Part 4A of the Insurance Act 2015 on Late Payment of Claims and that Conduct of Business requirements falling under "treating customers fairly" would be more efficiently met (FCA, 2018). This is because there would be no or minimal waiting time for pay-outs in the case of simple low-value products (FCA, 2019); and because customers would be able to purchase modular products suited to their needs rather than packaged products which might cover them for risks which are not relevant to them (FCA, 2019).

In the interests of treating customers fairly and providing clarity[p], customers would need to be made fully aware (FCA, 2019) that the pay-out may well be less than their actual loss because of the "agreed value" element: the policy limit is the 'most the insurer will pay' (L&C & SLC, 2016) and would be 'a reasonable estimate, or smaller amount, of the actual economic loss that will be suffered' (L&C & SLC, 2016) by the insured as a result of an insured peril.

It is important to ensure that when purchasing a product, the design of which includes automated pay-outs executed using smart contracts technology, the right questions are asked, and the right warnings are communicated over the relevant portals to ensure compliance with these requirements.

Decisions should also be made on the value of acceptable automatic pay-outs for insurers if they decide to implement pay-out in some cases, or workflows in others to take into account the potential for fraudulent claims (FCA, 2019) . This may be varied by jurisdiction, the number of verifiable oracles, or a risk scoring system that the customer has been made aware of.

Regard should also be had to relevant aspects of the Consumer Rights Act 2015 (Norton Rose Fulbright, 2015), which, among other things, requires that services be performed within a reasonable time[q] and provides that only exclusion clauses which are transparent and prominent can be excluded from an assessment of fairness[r]. One mitigation could be to pose a 'risk adjusted' delay on payments (Long Insurance, 2017).

As discussed in Section 3, a large amount of business is conducted through coverholders as intermediaries. The use of intermediaries in this way creates issues e.g. of white labelling and conduct of business risk, especially when one considers the requirements of the Insurance Distribution Directive (IDD)[s] (European Union, 2016).

While how a claim is dealt with is an underwriting issue, the design of the product, including potentially the quality of the coding, could also raise conduct-of-business issues. It is therefore necessary to ensure that the smart contract

[p] See Financial Conduct Authority (FCA), General Insurance Add-Ons: Provisional findings of the market study and proposed remedies, MS 14/1, March 2014; FCA, General Insurance Add-Ons: Final Report – Confirmed Findings of the Market Study, MS 14/1, July 2014; FCA General Insurance Add-ons Market Study – Proposed Remedies: banning opt-out selling and supporting informed decision-making for add-on buyers, CP 15/13, 25 March 2015 and FCA General Insurance Add-ons Market Study – Proposed Remedies: banning opt-out selling and supporting informed decision-making for add-on buyers including feedback on CP15/13 and final rules and guidance, PS 15/22, 28 September 2015, updated 31 March 2016.

[q] See (Consumer Rights Act 2015) s 52.

[r] See (Consumer Rights Act 2015) s 64.

[s] See in particular Chapter V (articles 17-25) of the IDD on Information Requirements and Conduct of Business Rules.

product is designed to comply with the insurer's conduct of business obligations.

To ensure that the code functions properly, and in line with the insurer's obligations towards its customer, Quality Control (QC) needs to be undertaken. There are, broadly speaking, four stages relevant to QC in coding:

1. The first is the specification of the function(s) which the code is to perform. If this does not specify those functions fully or accurately enough, the code will not perform as it ought. This specification is a co-operative exercise between the insurer and the code writer.
2. The second stage is the checking of the coding itself, to ensure that it does not contain technical errors or processing inefficiencies which degrade its technical performance – this would be undertaken within the coding entity as a matter of internal QC.
3. The third stage is testing the code against the specification, which is normally undertaken by the coder with some input from the customer in relation to how much testing is to be undertaken. Often QC stops at this stage.
4. However, the final stage is testing in real-world operation, which almost always produces some unexpected errors in code performance. The extent of this testing in operation should depend on the risks which would arise if the code does not perform as it should.

Insight: Quality control

It should be apparent that, from an insurance regulation perspective, the insurer (who is subject to the regulatory obligation) needs to focus most strongly on stages one and four.

These are where the insurer attempts to ensure that its regulatory obligations are met if the code is used (stage one) and checks that the code in action does enable compliance (stage four).

4.3.3 Data Protection

The General Data Protection Regulation (GDPR) (European Union, 2016), adopted by the European Union in 2016, which came into force in 2018, places important restrictions on data controllers when it comes to processing personal and sensitive data.

Should smart contracts come into more widespread use, it may mean that insurers are managing a much larger volume of personal data that was the case previously.

Since objective triggers are likely to be used in more immediate, standardised offerings, oracles may be feeding individuals' personal data into the electronic platform where the smart contract is held.

For example driver's licence and car registration details may be pulled directly from the Driver and Vehicle Licencing Agency (DVLA) database. It would be important to consider how to do this in a manner permitted by the Regulation.

These considerations would also be relevant where the design of the smart contract product involves the use of big data techniques to assess certain risks.

It is also important to note that some of the changes to business relationships which smart contracts make possible will also change the status of the participants for data protection purposes. A market entity which was previously a data processor might become a data controller and thus be subject to additional obligations, and an entity which previously had no data protection obligations might acquire them.

It is only possible to analyse the application of the law for detailed scenarios, and so it will be important that a full data protection assessment is carried out for any activities or products which change because smart contracts have been introduced.

5. Issues to overcome

There are certain limitations to be aware of before smart contract technology is embedded within business operations (World Bank Group, 2017).

5.1 Standardisation

A major challenge to the implementation of fully coded smart contracts *(see p15)* relates to the "significant challenges in accurately representing and interpreting contractual semantics in computer form" (Werbach & Cornell, 2017; World Bank Group, 2017). This process will typically be carried out by an expert programmer following instructions from the contracting parties.

Training

This brings human resources and talent development into the mix, as sufficient professionals will be required to carry out the required coding (World Bank Group, 2017).

Once programmers are trained – whether this is programmers given insurance knowledge, or insurance professionals trained in coding – there are a further two issues relating to the translation process:

1. The contracting parties fail accurately to explain their intentions to the computer programmer (human – human misunderstanding); and
2. The potential for errors in the translation from natural language to computer code (human – computer misunderstanding).

   (Savelyev, 2017)

In either case, the risk is that the execution of the smart contract differs from that which the parties had intended (Savelyev, 2017).

This was emphasised by Werbach and Cornell in the following terms: "if the parties do not or cannot represent all possible outcomes of the smart contract arrangement *ex ante*, the results may diverge from their mutual intent" (2017).

Testing

Even apparently correctly-written code may produce unexpected results in unusual circumstances, and so smart contract code also needs a programme of testing against historic, synthetic and extreme scenarios before it is put into commercial use. Thus, whether the problem of divergence is a bounded or unbounded one (which is to be avoided as there will be no identifiable solution) should be assessed by testing.

Before any smart contract solution is adopted, testing must show that the contract's variable outcomes are bounded meaning that, while the use of the technology may be risky, it is still viable as there are no known unknowns. This may be achieved through Quality Control procedures, the various steps of which are discussed in Section 4.2 *(see p37)*, which are also important to ensure compliance with regulatory requirements.

Another aspect which needs to be tested is the extent to which relevant jurisdictions recognise the contract in its "smart" form once it has been translated into code from the primary contract.

For example, if the underlying terms of an open cover or binding authority are agreed as a primary contract, but all contracts entered into on those terms are smart contracts (skipping the "primary" stage), these contracts might fall foul of requirements imposed by local regulators e.g. local regulations requiring the insurance contract to be concluded in writing and signed.

In the long term we foresee the development of what might be described as "industry-standard" smart contracts. Standard-setters exercise substantial control over their markets (Reed, 2013). This could be the development of existing groups or new ones.

For example, In the Lloyd's market there is a wordings repository (Lloyd's, 2019) where market participants can access 'vetted policy wordings and clauses regularly used within the London market.'

5.2 Inflexibility

The current technology will only support the coding of logic clauses. This means that smart insurance contracts will exist alongside other aspects of the agreement expressed in traditional contract form. This explains why a significant portion of the literature has focussed on questions relating to this interface between smart and traditional contracts.

Much consideration would need to be given to the interface between the smart and traditional aspects of an insurance contract and the infrastructure which would facilitate a mixed contract (Farrell, et al., 2018; World Bank Group, 2017).

Insurers opting to implement smart contracts will need to take 'significant care in the design of the smart contract's architecture to provide the flexibility required for real world operation.' (Farrell, et al., 2018).

Artificial intelligence

It is worth noting that advances in Artificial Intelligence (AI) technology (Alves, 2018) might change many aspects of insurance. For example, machines could be fed data regarding a car crash pulled from various sources (including e.g. CCTV footage, speed camera data, a police report, photographs taken by the customer or a third party and even data extracted from social media) and "digest" it to make a decision regarding whether a pay-out should be made or not. Further information on this topic can be found in a forthcoming Lloyd's report that explores AI through an insurance lens.

However, the fundamental legal analysis will remain unchanged. The AI will be a tool for assessing some aspect of the claim (whether the insured has a valid claim, the quantum of the claim, any contribution the insured has to make, etc). The output of the AI can be used in a smart contract just like any other parameter, i.e. the smart contract could be set up so that output of the AI machine could constitute the execution-triggering data.

How soon the use of AI technology might become commonplace in insurance is hard to assess, though, especially where the decisions that have to be taken are predicated on fairness and reasonableness.

AI technology can already predict how, on average, a human would behave, but this only simulates fairness and reasonableness (and by no means entirely accurately, as has clearly been identified in relation to AI tools to assist probation and criminal sentencing decisions[t]). In the end, the determining factor is likely to be market need, with law and regulation adapting slowly to follow on.

Claims notification clauses

A discussion of automating the claims process would not be complete without consideration of claims notification clauses. Commercial insurance policies typically require customers to inform the insurer of a potential claim and such obligations are usually expressed as a 'discretion clause' i.e. 'promptly'[u], 'as soon as possible'[v].

The ability to streamline the claims process would depend on these clauses being rewritten as logic terms, such as the backstop to notification within the International Hull Clauses that insurers must be notified within 180 days[x], or requiring human input after an assessment that the customer had acted in the prescribed manner.

At present, not all loss-making events result in a claim (Long Insurance, 2017). Insureds may choose not to claim due to issues of proof, the size of the deductible and for relationship considerations.

It was also argued in the report commissioned by the LMA that claims handling is a human process which would be difficult to replicate with computers. In particular, "excessive process automation could reduce pressures keeping down invalid or inflated claims." (Long Insurance, 2017)

Insurers should be aware of the possibility of a larger number of pay-outs if the trigger to payment is automated and no longer dependent on the submission of a claim by the customer. The adoption of objective triggers for pay-outs, therefore, must be viewed as a business decision, based on careful exposure assessment and management.

Automation of pay-outs using smart contracts may be found to be completely unsuitable for high-value complex cover, where human decision-making remains key to managing the claims process and the insurer-customer relationship more generally.

While in these situations, smart contract code may be used to render the process more efficient, for example by alerting a claims handler that an action needs to be taken and initiating workflows, the need to exercise human judgment to deal with complex situations precludes full automation.

On the other hand, in the case of low-value, low-complexity, high-volume products, where claims do not normally require in-depth scrutiny and the costs of processing the claim manually may exceed the benefits, a redesign of the contractual framework to accommodate objective triggering of a pay-out would seem to be beneficial.

[t] See (State of Wisconsin v Loomis 881 N.W.2d 749 (Wis. 2016)).

[u] See (Institute Time Clauses (Hulls) (01.11.95) cl.13.1., 1995).

[v] See (International Hull Clauses (01.11.03) cl.43.1., 2003).

There are also situations where automatic pay-outs would benefit the insurer-customer relationship, in that they are made available in a personal lines area where customers might have a negative claims experience when claiming for relatively small amounts, due to what they may perceive as disproportionate administration (Accenture, 2014).

5.3 Error, malfunction and cyber attack

As noted above, smart contracts result in irrevocable and secure transactions. While some commentators, such as Wheeler (2017), have argued that objective trigger will mean that there are no disputes relating to performance and breach in smart contracts (Savelyev, 2017), others – including the World Bank – have suggested that disputes may still occur (Norton Rose Fulbright, 2017; World Bank Group, 2017).

In these circumstances, a mechanism would need to be developed in order to settle disputes and, where necessary, correct erroneous transactions (Reed, et al., 2018; World Bank Group, 2017), i.e. a pay-out where no pay-out should have occurred or a failure to pay out where a pay-out was contractually due. This action may be more suitable to triggering a workflow with the need for human input until such time there is trust in automated systems. This is outlined in Section 4.1 *'design choices' (see p36)*.

Finally, insurers should note the risk that future technological advances could undermine current cryptography protocols and the transactions they protect, before implementing automation.

The robustness of digital signatures will be challenged by the availability and affordability of computing power, which is still increasing in accordance with Moore's Law (Kenton, 2018), doubling approximately every 18 months, and so a key length which is secure today will cease to be so within a finite number of years (NIST, 2015; Beckett, 1988).

This may be an issue for smart contracts involving long-term performance. Thus, actions that may currently be infeasible (e.g. the changing of entries in a distributed ledger) (World Bank Group, 2017) may in future no longer remain so, as computer power increases and cryptography methods advance.

Due regard must be given to these potential risks so that suitable mechanisms for addressing them, should they materialise, may be devised in advance.

6. Conclusion

Smart contracts could be a promising solution to improve efficiency in the insurance sector. Other product innovation such as parametric insurance is helping drive this technology forwards and there are likely to be more examples of innovation in this area as awareness of smart contracts grows.

It is important for anyone thinking about using smart contracts or parametric insurance to seek legal advice to ensure regulatory compliance.

Any new product is subject to Lloyd's normal guidelines around planning and class specific requirements, and managing agents should refer to their syndicate business performance manager for questions.

The Lloyd's class of business team is available to accompany and assess managing agents in all stages of parametric product development, and expects to analyse the viability and legality of new products individually.

References

Accenture, 2014. The Digital Insurer Claims Customer Survey Why claims service matters. [Online]
Available at: https://www.accenture.com/t20150523T041505__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents15/Accenture-Insurance-Claims-Survey-Web.pdf

Accord Project, 2018. Accord Project. [Online]
Available at: https://www.accordproject.org/

Aitken, R., 2017. Accord Project's Consortium Launching First Legal 'Smart Contracts' With Hyperledger. [Online]
Available at: https://www.forbes.com/sites/rogeraitken/2017/07/26/accord-projects-consortium-launching-first-legal-smart-contracts-with-hyperledger/#20e6c77d472c

Alves, P., 2018. 3 measurable benchmarks for enterprise AI that define the future. [Online]
Available at: https://venturebeat.com/2018/10/31/3-measurable-benchmarks-for-enterprise-ai-that-define-the-future/

Artemis, 2017. Unusual levels of cat bond trading recorded on TRACE. [Online]
Available at: http://www.artemis.bm/blog/2017/11/22/unusual-levels-of-cat-bond-trading-recorded-on-trace/

Artemis, 2018. Catastrophe bonds and ILS issued and outstanding by year. [Online]
Available at: http://www.artemis.bm/deal_directory/cat_bonds_ils_issued_outstanding.html

AXA, 2017. AXA goes blockchain with fizzy. [Online]
Available at: https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

Bacon, J., Michels, J. D., Millard, C. & Singh, J., 2017. Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017, 20 12.

Beckett, B., 1988. Introduction to cryptology. Oxford: Blackwell Scientific Publications.

CatIQ Inc., 2018. CatIQ Inc.. [Online]
Available at: https://www.catiq.com/

CCRIF SPC, 2019. Climate Risk Adaptation and Insurance in the Caribbean Project. [Online]
Available at: https://www.ccrif.org/projects/crai/climate-risk-adaptation-insurance

Clack, C. D., Bakshi, V. A. & Braine, L., 2017. Smart contract templates: Foundations, design landscape and research directions. Cornell University Library.

CMA CGM, 2018. Connected containers: CMA CGM deploys its innovative solution for containers tracking, TRAXENS. [Online]
Available at: https://www.cmacgm-group.com/en/news-medias/connected-containers-cma-cgm-deploys-its-innovative-solution-for-containers-tracking-traxens-by-cma-cgm

Consumer Rights Act 2015, 2015. Consumer Rights Act 2015. [Online]
Available at: https://www.legislation.gov.uk/ukpga/2015/15/contents

Cuccuru, P., 2017. Beyond bitcoin: an early overview on smart contracts. International Journal of Law and Information Technology, 1 9, 25(3), pp. 179-195.

Disparte, D., 2017. Blockchain Could Make the Insurance Industry Much More Transparent. [Online]
Available at: https://hbr.org/2017/07/blockchain-could-make-the-insurance-industry-much-more-transparent

D'Silva, V., Kroening, D. & Weissenbacher, G., 2008. A Survey of Automated Techniques for Formal Software Verification. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 7, 27(7), pp. 1165-1178.

Eidenmüller, H. & Aggarwal, N., 2018. Introducing a Special Series on Law and Autonomous Systems | Oxford Law Faculty. [Online]
Available at: https://www.law.ox.ac.uk/business-law-blog/blog/2018/03/introducing-special-series-law-and-autonomous-systems

European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

FAO, 2018. Desert Locust situation update 3 December 2018. [Online]
Available at: http://www.fao.org/ag/locusts/en/info/info/index.html

Farrell, S., Machin, H., Hinchliffe, R. & Mallesons, W., 2018. Lost and found in smart contract translation-considerations in transitioning to automation in legal architecture 1. J Int Bank L & Reg 24, Volume 25.

FCA, 2018. FCA Handbook: PRIN 2.1 The Principles. [Online]
Available at: https://www.handbook.fca.org.uk/handbook/PRIN/2/?view=chapter

FCA, 2019. Insurance: Conduct of business - Chapter 5 Identifying client needs and advising. [Online]
Available at: https://www.handbook.fca.org.uk/handbook/ICOBS/5/

FCA, 2019. Insurance: conduct of business - Chapter 6 Product Information. [Online]
Available at: https://www.handbook.fca.org.uk/handbook/ICOBS/6/?view=chapter

FCA, 2019. Insurance: Conduct of business - Chapter 8 Claims handling. [Online]
Available at: https://www.handbook.fca.org.uk/handbook/ICOBS/8/?view=chapter

Firma C-Trade SA v Newcastle Protection and Indemnity Assn (The Fanti and The Padre Island) (No 2) [1991] 2 AC 1, 35.

Gatteschi, V. et al., 2018. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?. Future Internet, 20 2, 10(2), p. 20.

Giancaspro, M., 2017. Is a 'smart contract' really a smart idea? Insights from a legal perspective. Computer Law & Security Review, 1 12, 33(6), pp. 825-835.

Goldby, M., 2013. Electronic documents in maritime trade: law and practice. Oxford: Oxford University Press.

Gould, J., 2016. Allianz Expects Blockchain Tech to Expedite Cat Bond Deals. [Online]
Available at: https://www.insurancejournal.com/news/international/2016/06/15/416971.htm

Government Office for Science, 2016. Distributed ledger technology: Blackett review. [Online]
Available at: https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

Greatrex, H. et al., 2015. Scaling up index insurance for smallholder farmers: Recent evidence and insights | CCAFS: CGIAR research program on Climate Change, Agriculture and Food Security. [Online]
Available at: https://ccafs.cgiar.org/publications/scaling-index-insurance-smallholder-farmers-recent-evidence-and-insights#.XC3zu-j7SUk

Greenspan, G., 2016. Why Many Smart Contract Use Cases Are Simply Impossible. [Online]
Available at: https://www.coindesk.com/three-smart-contract-misconceptions

Groenfeldt, T., 2017. IBM And Maersk Apply Blockchain To Container Shipping. [Online]
Available at: https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#455e7cd23f05

Harley, B., 2017. Are Smart Contracts Contracts?. [Online]
Available at: https://www.cliffordchance.com/briefings/2017/08/are_smart_contractscontracts.html

Harley, B., 2018. Are Smart Contracts Contracts. [Online]
Available at: https://talkingtech.cliffordchance.com/en/emerging-technologies/smart-contracts/are-smart-contracts-contracts.html

Helfand, R. D., 2017. Big data and insurance: What Lawyers Need to Know and Understand. Internet Law, 21(3).

Henry, K. J. & Hogan, B. W., 2018. Insurance and blockchain: What policyholders need to know. [Online]
Available at: https://www.bradley.com/insights/publications/2018/02/insurance-and-blockchain-what-policyholders-need-to-know

Hernández, G. O., 2018. Magic circle firms double down on legal smart contracts. [Online]
Available at: https://www.law.com/legal-week/2018/04/03/magic-circle-firms-double-down-on-legal-smart-contracts-378-79500/?slreturn=20190003083004

HIH Casualty & General Insurance Co Ltd v New Hampshire Insurance Co [2001] EWCA Civ 735 (2001).

Hingley, T., 2018. Blockchain and smart contracts. [Online]
Available at: https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/fintech/blockchain-and-smart-contracts/

Institute Time Clauses (Hulls) (01.11.95) cl.13.1. (1995).

Insurance Act (2015).

International Hull Clauses (01.11.03) cl.43.1. (2003).

ISO, 2018. ISO/TC 307 - Blockchain and distributed ledger technologies. [Online]
Available at: https://www.iso.org/committee/6266604.html

Kenton, W., 2018. Moore's Law. [Online]
Available at: https://www.investopedia.com/terms/m/mooreslaw.asp

L&C & SLC, 2016. Joint review of insurance contract law: Insurable interest and parametric policies, April 2016. [Online]
Available at: https://www.scotlawcom.gov.uk/files/7814/6107/9636/Insurable_interest_in_parametric_policies_-_April_2016_stakeholder_note.pdf

Lloyd's, 2015. Bitcoin: Risk factors for insurance. [Online]
Available at: https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bitcoin

Lloyd's, 2018. Volume Claims. [Online]
Available at: https://www.lloyds.com/market-resources/claims/volume-claims

Lloyd's, 2019. Lloyd's Wordings Repository. [Online]
Available at: https://www.lloyds.com/tools-and-systems/lloyds-wordings-repository

Long Insurance, 2017. From Slips To Smart Contracts: Intelligent Technology In The London Wholesale Insurance Market, London: Z/Yen Group.

MacDonald, M., 2015. 50 Shades of Grey: Bitcoins in a Legal Vacuum?. [Online]
Available at: https://www.linkedin.com/pulse/50-shades-grey-bitcoins-legal-vacuum-michaela-macdonald/

Marine Insurance Act (1906).

Maull, R. et al., 2017. Distributed ledger technology: Applications and implications. Strategic Change, 1 9, 26(5), pp. 481-489.

Mercury Capital, 2019. MiCRIX. [Online]
Available at: http://www.mercurycapital.bm/micrix

NIST, 2012. Federal Information Processing Standards Publication 180-4: Secure Hash Standard (SHS). [Online]
Available at: http://dx.doi.org/10.6028/NIST.FIPS.180-4http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.htmlN/A

NIST, 2015. NIST Special Publication (SP) 800-57 Part 3, Rev.1: Recommendation for Key Management, Part 3 - Application-Specific Key Management Guidance. [Online]
Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

Norton Rose Fulbright, 2015. Consumer Rights Act 2015 receives Royal Assent – what do insurers need to know?. [Online]
Available at: http://www.nortonrosefulbright.com/knowledge/publications/126807/consumer-rights-act-2015-receives-royal-assent-what-do-insurers-need-to-know

Norton Rose Fulbright, 2016. The future of smart contracts in insurance. [Online]
Available at: http://www.nortonrosefulbright.com/knowledge/publications/142730/the-future-of-smart-contracts-in-insurance

Norton Rose Fulbright, 2017. Arbitrating Smart Contract disputes. [Online]
Available at: http://www.nortonrosefulbright.com/knowledge/publications/157162/arbitrating-smart-contract-disputes

PRA, 2019. Conditions Governing Business (see para. 9.1). [Online]
Available at: http://www.prarulebook.co.uk/rulebook/Content/Part/212969/03-01-2019

Ralph, O., 2016. Peer to peer insurers go back to the future. [Online]
Available at: https://www.ft.com/content/c4bd7bcc-872f-11e6-a75a-0c4dce033ade

Reed, C., 2013. Cloud Governance: The Way Forward. In: Cloud Computing Law. Oxford University Press, pp. 362-390.

Reed, C., Sathyanarayan, U. M., Ruan, S. & Collins, J., 2018. Beyond BitCoin - legal impurities and off-chain assets. International Journal of Law and Information Technology, 1 6, 26(2), pp. 160-182.

Risk Management Solutions, 2012. Cat Bonds Demystified: RMS Guide to the Asset Class. [Online]
Available at: http://forms2.rms.com/rs/729-DJX-565/images/cm_cat_bonds_demystified.pdf

Roughton, T., 2017. Applying blockchain to insurance contracts. [Online]
Available at: https://www.out-law.com/en/articles/2017/may/applying-blockchain-to-insurance-contracts/

Roughton, T. & Bidewell, P., 2017. Smart insurance contracts. [Online]
Available at: https://www.pinsentmasons.com/PDF/2017/Financial-Services/FinTech_Smart_Insurance_Contracts_Flyer.pdf

Savelyev, A., 2017. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 4 5, 26(2), pp. 116-134.

Schönfeld, C., 2018. Smart Contracts under Swiss Law. The FinTech Edition, Issue 1.

Sherborne, A., 2017. Blockchain, Smart Contracts and Lawyers. [Online]
Available at: https://www.ibanet.org/Document/Default.aspx?DocumentUid=17badeaa-072a-403b-b63c-8fbd985d198b

Sieger, M., 2017. How GE Will Use OC Robotics' Robots For Jet Engine Maintenance. [Online]
Available at: https://www.ge.com/reports/snake-plane-longed-arm-robot-will-help-fix-aircraft-engines/

Solidity, 2018. Solidity 0.4.24 documentation. [Online]
Available at: https://solidity.readthedocs.io/en/v0.4.24/index.html

State of Wisconsin v Loomis 881 N.W.2d 749 (Wis. 2016).

Surden, H., 2012. Computable Contracts. U.C. Davis Law Review, 1 1.

Szabo, N., 1996. Smart Contracts: Building Blocks for Digital Markets. [Online]
Available at: http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html

The Zephyr [1984] 1 Lloyd's Rep. 58, 66.

Touche Ross v Colin Baker [1991] 2 Lloyd's Rep 230.

TradeLens, 2019. The TradeLens Solutions. [Online]
Available at: https://www.tradelens.com/solution/

UK Civil Aviation Authority, 2019. Aircraft insurance. [Online]
Available at: https://www.caa.co.uk/Commercial-industry/Aircraft/Operations/Insurance/Aircraft-insurance/

Verisk, 2017. How PCS develops catastrophe estimates. [Online]
Available at: https://www.verisk.com/siteassets/media/pcs/pcs-everything-you-need-to-know.pdf

Werbach, K. & Cornell, N., 2017. Contracts Ex Machina. s.l.:Duke University School of Law.

Wheeler, S., 2017. Visions of Contract. Journal of Law and Society, , 44(5), pp. 1-19.

Windward, 2019. Maritime Risk Insights & AI. [Online]
Available at: https://wnwd.com/

World Bank Group, 2017. FinTech Note No. 1: Distributed ledger technology (DLT) and blockchain. [Online]
Available at: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf