Hogan Lovells

Blockchain/DLT in the Insurance Sector

September 2017

Contents

Welcome

It is a time of great change in the insurance sector, with technology ushering in a new era of digital products and services.

'InsurTech' offers tantalising opportunities that are waiting to be grasped. But there's no escaping that these rapid advances in technology also throw up new legal risks and practical questions about how firms can safely capture this potentially game-changing value.

In this report we focus in particular on the impact of distributed ledger technology (DLT) on the insurance sector and discuss some of the key legal and regulatory issues that arise as a result of using it.

We have been inspired to write the report by the numerous clients who have told us that there is a lot of information available on the different DLTs, but a lack of engagement and education concerning the many legal and regulatory challenges that they would face, were they to implement these technologies.

Benefits

We have analysed the key issues in some depth and our research throws up some important areas where the industry could benefit, including:

- Significant cost and time savings, as well as fraud mitigation, particularly in areas like customer identity checking and AML;
- Simplified underwriting, with automated processes collating and assimilating information;
- New distribution methods, such as peer-to-peer (P2P) insurance;
- Innovative new products, embodied in 'smart contracts', which would offer solutions beyond 'pure loss' models;
- More efficient and transparent claims handling, with technology limiting the scope for disagreement between parties and offering automatic enforcement of contracts.

Barriers

The potential benefits of DLT to the sector are many, but it would be unwise for firms to rush headlong into adopting it. Some of the key issues standing between them and successful implementation include:

- Privacy challenges, with the different incarnations of DLT making analysis under data protection laws challenging;
- International jurisdiction raises concerns, as shared distributed ledgers have no specific location;
- Regulators across the world are taking different approaches to how they regulate DLT, meaning it will be difficult to determine who you answer to and how they will supervise the system going forward;
- Decentralised ownership means no one person is in charge of distributed ledgers and so no central authority is on hand to take responsibility or resolve disputes between participants;
- Governance needs careful attention as DLT is a technology that thrives on collaboration, meaning thought is needed when deciding how to accommodate operational developments, or when responding to legal changes.

Recommendations:

In light of these issues, we suggest certain steps as a starting point for any firm looking to use DLT. These include:

- an early review of key legal issues that might apply to your particular service, taking into account your key jurisdictions;
- keeping a close eye on regulators, who are all beginning to engage with this topic, allowing you to have an informed picture of regulation as it develops.

We hope that this report moves the debate on so that all of the different players in the insurance sector can make progress with their DLT implementation plans, and we welcome feedback and comments from you as we develop our own thinking.

John Salmon
Partner, London
+44 20 7296 5071
john.salmon@hoganlovells.com

Introduction

The insurance sector is currently experiencing the kind of disruption that has beset other parts of the financial services sector over the last few years. The term ‘InsurTech’ has come to the fore as many traditional players move to a more digital model and new entrants swarm into the market.

But where there is disruption, there is also opportunity. Insurance has long provided societal benefits and many visionaries see technology as a way of providing innovative new types of insurance protection for currently underserved sectors of society.

Google have identified seven key technologies that have already begun to disrupt the insurance sector and whose impact is expected to accelerate in the next three to five years. These include:

- infrastructure and productivity;
- online sales technologies;
- advanced analytics;
- machine learning;
- the Internet of Things;
- distributed ledger; and
- virtual reality.

A total of £218m has been invested in InsurTech companies in the UK during the first half of 2017, according to Accenture and CB Insights. These figures represent a 2,695% increase on 2016’s investments.

> “These figures represent a 2,695% increase on 2016’s investments.”

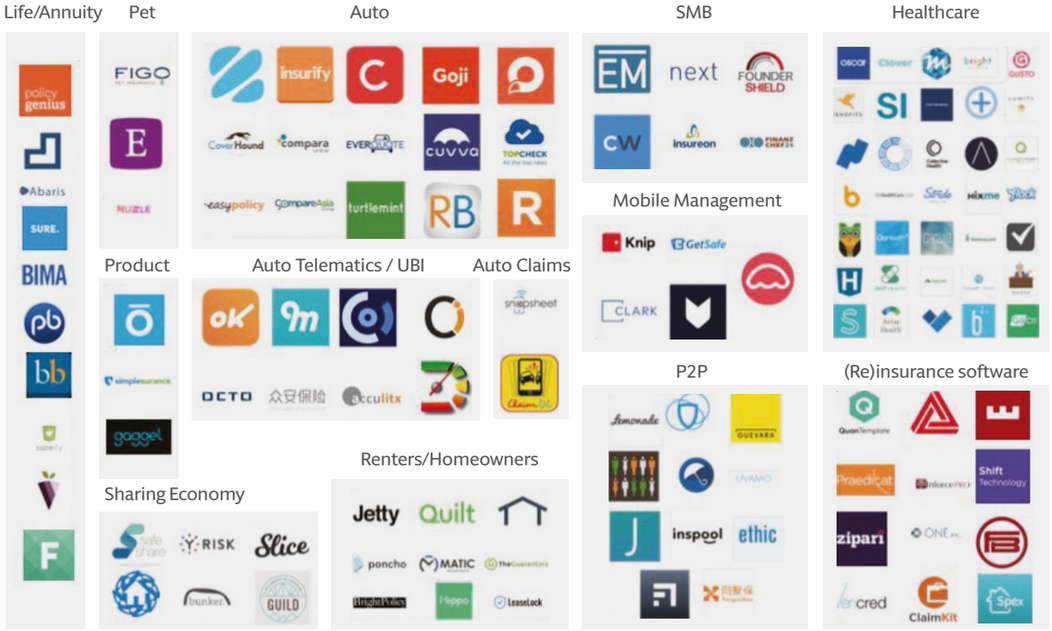
Insurance value chain and InsurTech disruption

Digital Benefits and Disruption

Product	Marketing & Distribution	Underwriting & Pricing	Claims	Customer Services
– Personalisation – Usage based products – AI – Sharing economy	– Digital marketing – Aggregators – Omni channel – Digital channels – STP – Machine learning	– Big data analytics – Internet of Things – Automated processing – Blockchain	– Use of mobiles and apps – Digital channels – Automated processing	– Online management – Operational efficiencies – Omni-channel experience – AI – Connectivity – Customer engagement

InsurTech key players according to CB Insights

Landscape today



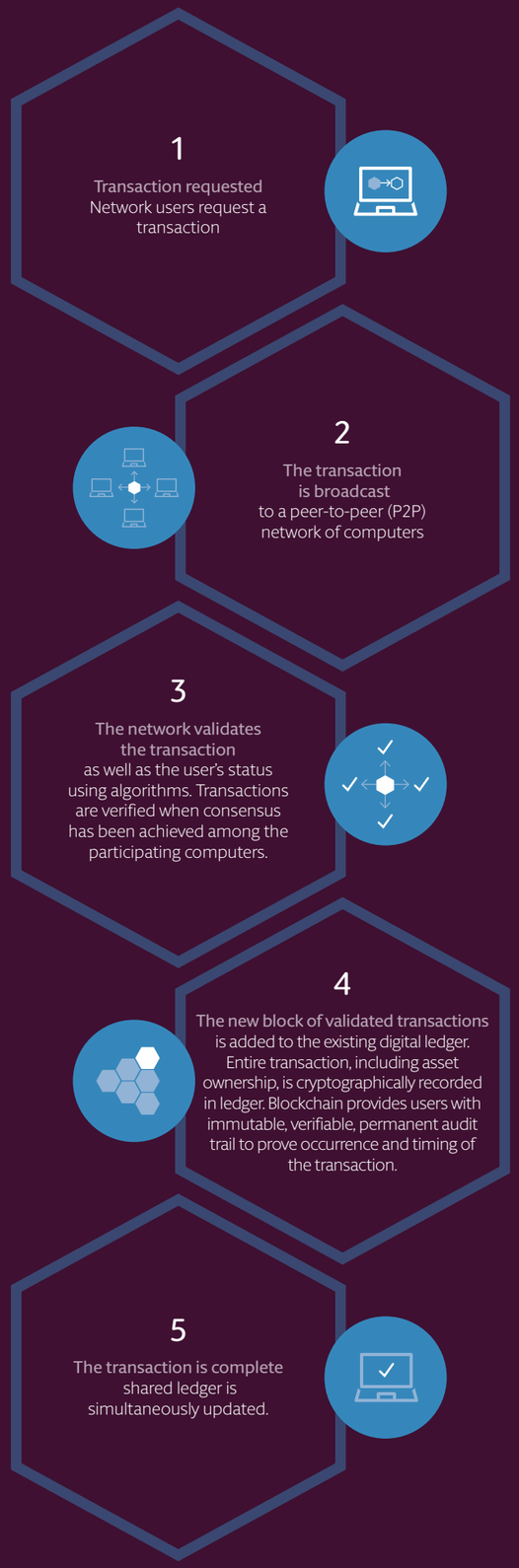
Terminology

DLT and blockchain

A distributed ledger is a replicated, shared, and synchronised digital data structure maintained by a consensus algorithm and spread across multiple sites, countries, and/or institutions. Blockchain is a type of distributed ledger, comprised of digitally recorded data in packages called blocks which are linked together in chronological order in a manner that makes the data highly resistant to alteration once recorded. Typically each node on the network contains a complete copy of the entire ledger, from the first block created—the genesis block—to the most recent one.

Although the term "blockchain" is used generally to mean "distributed ledger" in most discussions, as well as in the media (particularly in financial services), a blockchain is only one of many types of data structures that provide secure and valid achievement of distributed consensus. While blockchain focuses on how data is stored and linked to one another in a chronological manner within blocks, a DLT is the more general term which covers the sharing of the database amongst all the operational participants (nodes) of the network. As such, not all DLT is blockchain. In this report we will refer to DLT to cover the broader applications of the technology, unless the context we are using is specifically blockchain technology.

How blockchain works



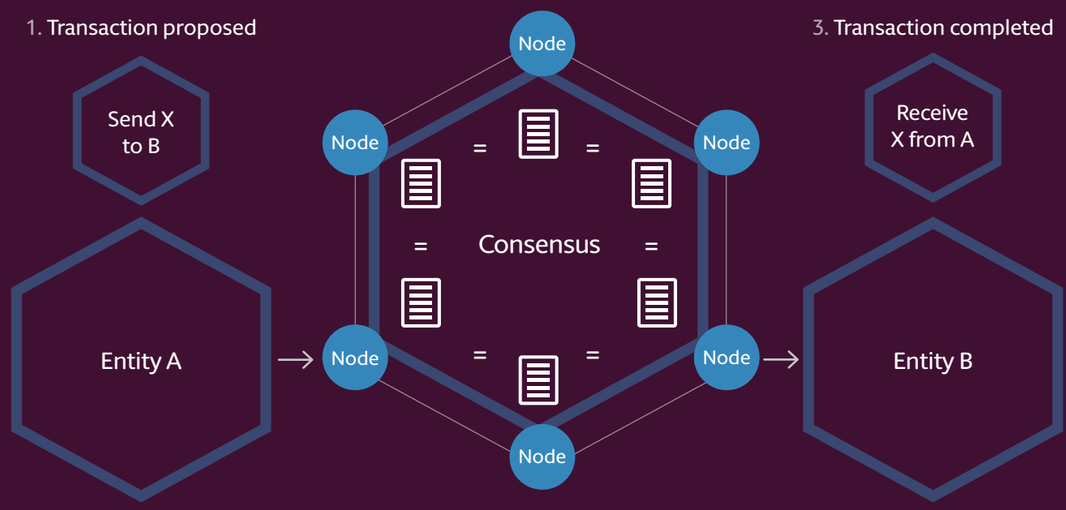
Permissioned vs. Permissionless DLT

There is also a distinction to be made between permissionless ledgers (public) and permissioned ledgers (private). Permissionless ledgers allow anyone to contribute data to the ledger with all participants possessing an identical copy of it. Permissioned ledgers, on the other hand, allow for distributed identical copies of a ledger, but only to a limited number of trusted participants who are pre-selected or subject to gated entry upon meeting certain requirements.

What are smart contracts?

Smart contracts use DLT. The term is used to describe computer program code, maintained on the various nodes constituting a distributed ledger network, which is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement upon the occurrence of pre-defined conditions. The smart contract code executes on each node and the resulting output is stored on the distributed ledger. Where "tokens" of value are involved, the smart contract code can also automatically transfer these tokens (and underlying value), thus effectively enforcing the outcome of the smart contract code.

The consensus protocol in the blockchain network



Peer-to-peer distributed network
2. Nodes in network undergo consensus process to validate and agree on updates to the distributed ledger, ensuring that no two nodes have conflicting records.

How could smart contracts be used?

The application of smart contracts is limited due to the pre-programmed nature of the smart contract code. This means that smart contracts are suitable for agreements that have clearly defined obligations and parameters at the outset. There are a number of examples in the insurance sector which would potentially satisfy these requirements:

a) Term insurance claims – a smart contract could be created between the insured and the insurer which will pay out death benefits to the beneficiary upon the death of the policy holder. The smart contract could be connected to the death registries. On receiving a notification of a person's death by the appropriate registry, the smart contract can automatically verify the person is covered, then initiate and settle the claim payment.

b) Micro-insurance – DLT-powered smart contracts combined with real-time recording of data relevant to the policy can be applied to automate the settlement of insurance policies covering very small claim amounts. These sorts of claims can be verified by insurance agents and recorded on the distributed ledger in order to trigger rapid payment. DLT-powered automation can significantly reduce the time of settlement and streamline the operations in an efficient manner, thus providing a means of reaching untapped markets and insuring assets that might otherwise not be worth covering.

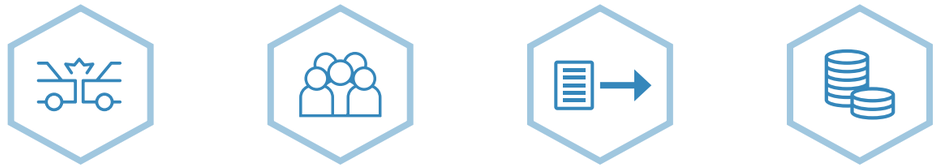
c) Reinsurance – smart contracts could be applied to the back office transactions that take place between insurers and reinsurers. Normally, after a claim is settled the insurer verifies the validity of any reinsurance contracts and works with reinsurers for recovery. A smart contract could be placed on a DLT platform to initiate a recovery transaction as soon as a claim meeting reinsurance contract specifications is settled.

The Benefits

The business logic underlying smart contracts can bring clarity and reduce unnecessary legal intervention, in turn saving time and money for insurers. As claim events are recorded in the distributed ledger, duplicate claim reporting can be prevented and fraud attempts can be minimised. Multiple parties can also have access to a 'single source of truth' thereby reducing the time-consuming and cumbersome exchange of many documents.

> "DLT-powered automation can significantly reduce the time of settlement"

Smart-contract use case: car insurance claim



Customer is involved in an accident

Control claims costs – smart contract used to enforce rules on where insured can spend money

Customer is directed to an authorised garage, where someone inspects the damage and posts details and repair estimate to the blockchain

Claim is automatically initiated, cover is verified, and repair is approved (or not)

Fraud detection – allows duplicate claims for the same incident to be detected automatically

Garage repairs vehicle and confirms this, and cost, on the blockchain. Claim is settled automatically

Reduce claims processing cost – no human involvement (at insurer) after smart contract created

What are oracles?

Distributed ledgers cannot access data outside their network on their own. An oracle – also known as a data feed – is a third party service designed for use in smart contracts on the distributed ledger. The oracles provide external data when needed and push it onto the distributed ledger. The key is for all the parties to the smart contract to agree the identity of the oracle.

Smart contracts contain value and only unlock that value if certain pre-defined conditions are met. The external data could be anything, from weather temperature to successful payment, price fluctuations, and so on. When a particular value is reached, the smart contract changes its state and executes the programmatically predefined algorithms, automatically triggering an event on the ledger.

The primary task of oracles is to find and verify real world occurrences and provide these values to the smart contract in a secure and trusted manner. For instance, with term insurance the oracle would provide the data from the death registries, which would then trigger the pay out of death benefits to the beneficiary of a life insurance policy.

Challenges

The challenge with oracles are that they are not part of the distributed ledger, they are third party services; the parties need to trust these sources of information and the sources must be secure from hacking. Trusted and secure information sources are crucial for the users of smart contracts, because, in the case of mistakes or the oracle changing the information taken from other sources or providing defective data then there is no rewind or reset button.

What are the key advantages of DLT?

DLT has the potential for *"modernising, streamlining and simplifying the siloed design of the financial industry infrastructure with a shared fabric of common information."* (DTCC 'Embracing Disruption' January 2016).

According to a WEF report, "The Future of Financial Infrastructure", published in August 2016, DLT is one of many transformative new technologies that will shape future financial services infrastructure. The WEF identifies six key value drivers of DLT:

a) Operational simplification: DLT reduces manual efforts required to perform reconciliation and resolve disputes. The current practice of managing policy and claims data in separate ledgers can lead to inconsistent master and transaction data, resulting in erroneous, duplicated information, as well as a significant loss of time reconciling and correcting this data. This not only slows down the process but also forms a source of contract uncertainty. DLT is expected to bring significant efficiencies to this process.

b) Regulatory efficiency improvement: DLT enables real-time monitoring by regulators of the financial activity of regulated entities.

c) Counterparty risk reduction: DLT challenges the need to trust counterparties to fulfil obligations as agreements are codified and executed in a shared, immutable environment.

d) Clearing and settlement time reduction: DLT disintermediates third parties that support transaction verification / validation and so accelerates settlement.

e) Liquidity and capital improvement: DLT reduces locked-in capital and provides transparency into sourcing liquidity for assets.

f) Fraud minimisation: DLT enables asset provenance and full transaction history to be established within a single source of truth.

These value drivers could:

a) lead to a reduction in costs, errors and time;

b) provide instant access and legal certainty;

c) minimise reputational risks; and

d) create an environment where there is no single point of failure.

Potential benefits of blockchain

- Reduce costs of overall transactions
- Reduction in systemic risks
- Irrevocable and tamper-resistant transactions
- Fraud minimisation
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators

Interest in DLT in the insurance sector has grown rapidly since 2015. For example, in September 2015 the consortium, R3, was launched and is now working with over 80 banks, financial institutions, regulators, trade associations, professional services firms and technology companies to develop Corda, a distributed ledger platform designed specifically for financial services. The Lloyd's insurance market in London has included DLT as part of their target operating model or TOM initiative, while AXA Strategic Ventures (along with other partners) invested around $55 million into a blockchain startup in February 2016. In October 2016 Aegon, Allianz, Munich Re, Swiss Re and Zurich launched the blockchain insurance sector initiative, B3i, aiming to explore the potential of DLT to better serve clients through faster, more convenient and secure services. Firms are now developing proofs of concept using DLT to replace parts of the traditional insurance sector infrastructure. Most recently, Allianz has announced its successful pilot of a smart contract solution to automate catastrophe swap transactions. In April 2017, the UK's Financial Conduct Authority (FCA) stated in their 'Discussion Paper on distributed ledger technology' (DP17/3) that *"in the second half of 2017 into 2018 we expect to see more movement from 'Proof of Concept' to 'real-world' deployments"*. It appears this prediction was correct, for on 15 June 2017 AIG announced it had sold the first blockchain-based multinational insurance policy to Standard Chartered. The policy for Standard Chartered consists of a "master policy" in the UK, which is linked to local policies in the US, Kenya and Singapore.

How DLT could disrupt the Insurance Sector

a) Potential for ultra-low transaction costs introduced globally.

b) The ability to insure assets or risks that are not currently insurable.

c) More efficient interactions between all the players leading to fewer errors and less legal uncertainty.

Implications of DLT in the Insurance Sector

The IAIS report on "FinTech Developments in the Insurance Industry" published in February 2017 found that the expected implications of DLT in the insurance sector are as follows:

a) Competitiveness: DLT could lower the barriers to entry and allow non-traditional companies to compete with current insurers. In the longer term, the players that remain may be the ones that apply DLT for risk selection, claims management and fraud prevention.

b) Consumer choice: Consumer products may become more standardised due to operational issues associated with smart contracts. However, different types of product offerings may arise, including offerings using real time data created by linking DLT and other devices such as telematics and Internet of Things (IoT).

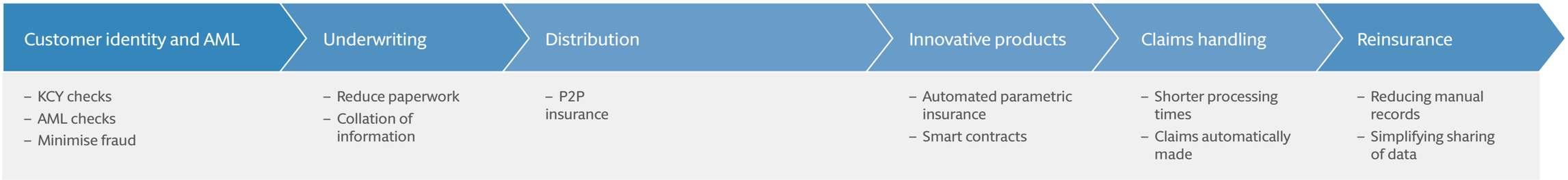
c) Level of interconnectedness: The level of interconnectedness could increase since DLT platforms and protocols may need to be standardised for the entire financial sector.

d) Business model viability: Insurers that adopt DLT may see cost reductions and improved efficiencies that could increase their competitiveness and enhance viability in the long term.

e) Data ownership: In current DLT data is maintained simultaneously across many different computers owned by different parties. Therefore, it would be difficult to say which party owns what data. In the future, some cryptographic anonymisation algorithm could be devised, but it would cause other issues (for example, around AML and performance).

f) Supervisory oversight & prudential requirements: Capital requirements and customer protection are still going to be key issues even in a DLT environment (except, in some jurisdictions, for peer-to-peer ("P2P") schemes). DLT may increase liquidity risk if proper controls are not put into place due to increased claims efficiency and the use of smart contracts.

> "DLT could lower the barriers to entry and allow non-traditional companies to compete with current insurers."



DLT in the insurance value chain

Almost all of the activities in the insurance value chain could be impacted by DLT. Working through the lifecycle of an insurance transaction we identify these below:

> “Use of DLT will reduce the amount of time and money involved in underwriting by using automated processes to collate and assimilate the required information.”

a) Customer identity and AML

Brokers, insurers and reinsurers must carry out appropriate KYC and AML checks, sanction screening and identify the ultimate beneficial ownership for all of their counterparties – both legal entities and individuals. If a client engages a broker who works with multiple underwriters, this can lead to the involvement of several participants, each of whom has to do the same verification along the chain. This can mean significant costs and delays.

A distributed ledger-based certified file transfer utility would speed up this process and reduce these costs. The distributed ledger would contain the key information in relation to the client, as well as the evidence of validation by each player in the insurance life cycle. All of this would be encrypted with keys belonging to the client. The client can then provide the appropriate subset of keys to their next business partner and that business partner can rely on the validation done by those in the chain previously without any delay. This would result in stakeholders spending less time on KYC and AML checks and less money on administration.

As a result of the use of DLT, the risks of consumers committing identity fraud is minimised and therefore it is arguable that rates, risk liabilities and premiums could be lowered.

b) Underwriting

Provision of information in relation to risks to underwriters has traditionally involved a lot of paper with inherent costs, time inefficiency and the risk of omissions.

The use of DLT will reduce the amount of time and money involved in underwriting by using automated processes to collate and assimilate the required information. The result will be a more transparent, simplified and faster process. A good hypothetical example would be the use of DLT in property insurance. One can imagine property underwriters having access to land registry records via DLT providing them with clear, accurate and immutable information in relation to the property to be insured. For example, Lemonade, a new P2P insurer discussed more fully below, searches municipal databases for building age, confirms structural materials for building durability, searches environmental databases for distance from coast, and checks storm and fire sensitivity before issuing a quote for renters insurance.

c) Distribution

DLT could be used in new distribution methods like P2P insurance. A group of participants not individually eligible for suitable insurance cover might use the decentralised trust, autonomous processing and smart-contract capability of distributed ledgers. This would allow them to self-insure the group by sharing risk between the participants at a reduced cost.

d) Innovative products

Use of DLT is expected to drive the development of new services, for example automated parametric insurance products. In this case, the insurance policy would be embodied in a smart contract and, instead of indemnifying the pure loss, insurers would agree to pay a certain amount upon the occurrence of triggers specified within preset computer coding instruction, in the form of a smart contract, stored and executed on the distributed ledger. So, if an earthquake were to occur in a given region above a magnitude of five, the smart contract would automatically pay 20% of the premiums paid, split rateably among the policy holders. Contracts would require oracles to agree that a trigger event had occurred.

e) Claims handling

Traditional claims-handling processes can often allow scope for disagreement between the insured and the insurer over information that has previously been shared. This can result in claims taking a long time to process, as well as being costly, particularly if the parties have to resort to litigation.

Smart contracts held on a distributed ledger can be used to maximise efficiency and minimise costs in the following key ways:

i) Policy conditions can be written as computer code in smart contracts and stored on a distributed ledger. The distributed ledger is connected to the internet and can use publicly available data to determine when an insured event has taken place, in which instance the policy will pay out.

ii) Claims are automatically enforced by computer protocols using the code (with no need for claims assessors for simple products). There is the potential for payouts to be made against insured events without the need for the client to submit a claim, which means that payouts can be made more quickly (and, in some cases, almost instantly).

iii) Insurers can stipulate certain conditions under which a payout will be made. For example, in the motor insurance sector, smart contracts could be written so that customers are prevented from claiming on insurance for more expensive repairs than are necessary. In some jurisdictions, insurers could set the terms so that the automated payout will only be made if the insured uses specified third parties designated by the insurer to carry out the work.

iv) Another key advantage of using DLT in claims-handling is that it has the potential to enhance transparency and minimise the number of payouts on fraudulent claims. The effect is that insurers reduce losses incurred by paying out on such claims, whilst simultaneously reducing the requirement for expensive manual checks when a claim is made. Ultimately, this should drive down the costs incurred by clients.

> “Use of DLT is expected to drive the development of new services.”

f) Reinsurance

Traditional treaty reinsurance involves the collation of significant manual records in the form of bordereaux and claims databases which are then shared between the insurer, broker and reinsurer.

Incorporating this information into verified, immutable blocks on a chain will result in time and cost savings plus efficiency in making payments and applying set-offs.

g) Capital markets

Prior to the advent of DLT, insurers had already been developing a significant new means of defraying risk using capital markets. In fact, the 2008 ‘Global Competitiveness Report’ from the WEF found that the diversification of risks (such as the risk of a hurricane event in a particular geographic area) away from the correlated risks, found in most financial markets instruments, made insurance-linked securities particularly desirable to capital markets investors.

At the same time, insurance-linked securities also provide a means for insurers to obtain additional insurance capacity, allowing them to expand their coverage of a wide variety of catastrophic risks. The capital markets can also provide another source of independent data for pricing these risks. Nevertheless, the development of the insurance-linked securities market since 2008 has been modest, with relatively few new transactions coming to market each year.

> “DLT has the potential to improve efficiency and reduce costs in securities settlement.”

DLT has the potential to greatly expand the insurance-linked securities markets by addressing some of the key impediments holding back their natural growth. These include:

i) Authentication of data: DLT allows a secure “audit trail” to be created for all data that is utilised. The person or entity uploading the data can be identified and a “hash” (or digital fingerprint) of the data can be stored on the distributed ledger. This gives investors certainty that the data was not tampered with after being certified by a trusted party.

ii) Reconciliation of data across many stakeholders: With DLT, all data inputs can be tracked in real time via the common distributed ledger without the time or cost of reconciling data stored on different systems by different parties at multiple stages of a transaction.

iii) Transparency and reporting: While the information provided to investors in insurance-linked securities in the primary markets has been very robust, DLT would allow this level of transparency to continue into the secondary markets as well. Because the securities would be issued on a private ledger, near real-time information about the status of underlying risks and the performance of any investments could be provided to those investors shown on the ledger as holders.

iv) Automation of processes: Perhaps most interestingly, smart contract code can be used to automate many of the features of an insurance-linked securities offering. For example, if an oracle showed that a certain event had occurred, such as the wind speed exceeding a certain threshold for a given period of time in a given geographic area, this data could trigger a payment by the smart contract code without the time or delay of needing a trustee to double-check the same information. However, the efficiencies that come with this automation would have to be balanced against the issues of introducing a potential point of failure in an oracle.

In addition, as investors such as fund managers are starting to become more comfortable with owning and trading digital assets, we may see new areas of secondary market interest arise to meet the supply of “tokenised” insurance risks. The Bank of England aptly concluded in their Staff Working Paper No.670 on ‘The economics of distributed ledger technology for securities settlement’ (published in August 2017) that:

“DLT has the potential to improve efficiency and reduce costs in securities settlement, but the technology is still evolving and it is uncertain at this point what form, if any, a DLT-based solution for securities settlement will ultimately take.”

Regulatory challenges

The regulatory position relating to the use of DLT is still evolving. Most of the regulators across the globe are now engaging with the possible impact this technology could have on the financial services sector.

In the UK, the FCA and PRA are only at the early stages of considering the risks posed by DLT and what regulatory requirements should apply to its use. For example, the FCA published DP17/3 asking for comments in order to start a dialogue on the potential for future development of DLT in the markets they regulate. The FCA is due to publish a Summary of Responses or further Consultation Paper based on the comments they have received.

In France, the government has shown some interest in the technology but unlike the UK it has not yet launched any major initiatives. In March 2016 the Ministry of Economy passed a decree to allow debt-based instruments to be issued on a distributed ledger. In May 2017, France Stratégie, the French Prime Minister's cabinet for national strategies analysis, held several hearings on DLT issues such as legal and social issues or regulations. Most recently, Finance Innovation, a French institution dedicated to fostering the French financial sector, is said to be setting up a working group to guide the government over initiatives they will need to lead in the DLT sector. However, the French regulators have not joined a number of other countries in setting up real DLT experimentations, instead continuing to hold conferences and workshops.

In Australia, the ASIC published "Information Sheet 219" about evaluating DLT which stated that it will follow a 'technology neutral' regulatory approach in line with its historical approach to these types of technologies. ASIC has set up an Innovation Hub to help start-ups developing innovative financial products to navigate the regulatory system. However, similarly to the UK, ASIC has made clear that, at this stage, they believe the existing regulatory framework is able to accommodate DLT use cases that have emerged. But the regulator intends to engage extensively with a wide number of these organisations as the technology matures and they will evaluate various use cases and consider their potential impact on specific services within the market.

In January 2017, the U.S. FINRA issued a report entitled "Distributed Ledger Technology: Implications of blockchain for the Securities Industry". This was very much in line with the various other papers that regulators have produced in order to elicit views, stating that – *"This paper is intended to be an initial contribution to an ongoing dialogue with market participants about the use of DLT in the securities industry."* Later, in March 2017, the US Illinois Department of Financial and Professional Regulation became the first US State regulator to become a member of the R3CEV consortia.

In the U.S., the NAIC established an Innovation and Technology Task Force to monitor emerging technologies, including DLT. The Task Force's mission is to *"provide a forum for regulator education and discussion of innovation and technology in the insurance sector, to monitor technology developments that impact the state insurance regulatory framework, and to develop regulatory guidance, as appropriate."*

The regulatory approach in the EU has thus far been an 'active' wait-and-see approach. In June 2016 the European Parliament voted for 'smart regulation' of DLT, with German MEP Jacob von Weizäcker noting: *"To avoid stifling innovation, we favour precautionary monitoring rather than pre-emptive regulation"*.

In February 2017, ESMA issued a report on DLT concluding that regulatory action was premature given that the technology was still at an early stage, as well as finding that the current EU regulatory framework did not represent an obstacle to the use of DLT in the short term.

In April 2017, the European Commission established a 'European Union Blockchain Observatory' to develop expertise on topics such as infrastructure, governance and validation mechanisms, contracts, regulatory and legal challenges, interoperability and standards, and will explore possible use cases within the EU. In June 2017, the European Commission announced the launch of its '#Blockchain4EU Project' to help industrial use cases for blockchain and DLT. The objective is to identify, discuss and communicate possible uses and impacts of blockchain and other DLT objects, networks and services within EU industrial or business contexts.

The EIOPA is also taking an active role in the discussions around DLT. In April 2017 EIOPA organised its first InsurTech roundtable to discuss with stakeholders the benefits and risks of digitalisation for the sector and consumers as well as potential obstacles to effective innovation. It was concluded at the roundtable that:

"Arguably, supervisory oversight is less necessary in regards private blockchains (notwithstanding antitrust and competition matters, or powers necessary to supervise possible illegal activities). In public blockchains, supervisors may need to focus on a range of different issues, such as the role of miners and nodes, or security and privacy challenges. Some participants also noted that regulatory authorities could also consider addressing some of the legislative barriers preventing the implementation of blockchain."

In June 2017, the EIOPA also responded to the European Commission's public consultation on 'Fintech: A more competitive and innovative European Financial Sector', stating that:

"There are also some risks arising from digitalisation that supervisory authorities need to examine very carefully. This is for instance the case with possible price discrimination issues or with vulnerable consumers' access to insurance. Digitalisation could also lead to an increasingly fragmented insurance value chain, raising challenges from a supervisory perspective, similar to the increasing exposure of undertakings to cyber risks… This includes automation of financial advice, blockchain, artificial intelligence, and peer-to-peer insurance. While it is still early days for some of these financial innovations, EIOPA will closely monitor them in view of their potential impact and take action as relevant."

Regulators across the globe have also made efforts to collaborate with their counterparts in other countries to gain and share knowledge in regulating these new technologies. For example, in June 2017 the Monetary Authority of Singapore and the Association of Supervisors of Banks of the Americas signed a Memorandum of Understanding (MOU) to bolster FinTech ties between Singapore and the Americas. ASIC has also signed a number of fintech-related MOUs with overseas regulators in the UK, Kenya, Singapore and Canada.

DLT and blockchain have found its way onto the websites of other regulators like BaFin in Germany. The technology's potential to significantly change transactions including payment transactions is clearly recognised. For example, Felix Hufeld, the President of BaFin, in his speech at the G20 Conference on "Digitising Finance, financial inclusion and financial literacy" on 25 January 2017, made clear that:

"regulation should be neutral and not discriminate against digital processes as such. As new risks emerge – to financial stability as well as consumers – we have to adapt… Digitisation offers no doubt considerable opportunities – but a host of opportunities for cyber-attacks as well…Given the nascent and dynamic nature of technological developments, it is quite challenging for us regulators to get the timing right: we shouldn't try to be quicker than market developments themselves, stifling innovation and producing regulation prematurely. On the other hand, we are carefully examining new threats to financial stability and shouldn't wait until the next global crisis comes about…"

In the absence of specific new legislation, the application of existing laws to DLT is likely to depend on the use to which the technology is put. However, there are a variety of initial hurdles, detailed below, which will need to be overcome in the face of existing legislation, if DLT is to take off.

Privacy challenges

Data privacy is often highlighted as one of the key barriers to DLT implementation. DLT and its various incarnations come in many shapes and sizes, making analysis under data protection law challenging. Some DLT systems will have little or no contact with personal data, whereas others will involve highly sensitive personal data (e.g. medical records).

A fundamental tenet of DLT is the immutability of the data in the distributed ledger. By this, it is meant that data cannot be changed once it is validated and bound to the ledger and that data in the ledger will persist for as long as the system exists. With ledgers being distributed across the full network, and in many cases openly available to all network participants, it is imperative to carefully consider any potential privacy concerns with the data that is being stored in it.

The major difference between DLT and most cloud computing environments is that DLT systems do not rely on a single provider of storage or computing resources. Each user of the DLT system uses his or her computing resources, on a peer-to-peer basis. Moreover, each user has a complete copy of the distributed ledger on his or her own computer. Consequently, the user of a DLT system may at the same time be data controller for the data that he or she uploads onto the distributed ledger, and data processor by virtue of storing the full copy of the distributed ledger on his or her own computer.

While there is some degree of alignment across the data protection regimes in a number of the jurisdictions across the globe, there are also important distinctions.

For example, in Singapore the Personal Data Protection Act was only implemented in 2013, meaning that Singapore has not yet generated much precedent in respect of data protection law. This means that the answers to difficult questions with regards to the treatment of anonymous and pseudonymous data, and questions around the re-identification of data, may be uncertain.

In Australia, the privacy law underwent a number of updates in 2014 which increased the focus on cross-border transfers of personal information. The transferring entity must ensure that the recipient of the data holds it in accordance with the principles of Australian privacy law. The entity transferring the data out of Australia remains responsible for any breaches by or on behalf of the recipient entity. This is unlikely to be possible in a public distributed ledger context and could mean that there will be significant potential liability for any Australian node in a public distributed ledger.

> Data privacy is often highlighted as one of the key barriers to DLT implementation.

In the US, there is no overarching law regulating data protection. Instead the law is fragmented, resulting in collectors contending with a wide range of state and federal laws. Public ledgers with US nodes will therefore need to consider and meet the requirements of a broad spectrum of regulation. For example, in addition to the specific rules and requirements related to customer data privacy in each state, protection of financial and personal customer information is a key responsibility and obligation of the Financial Industry Regulatory Authority member firms. SEC Regulation S-P (Privacy of Consumer Financial Information and Safeguarding of Personal Information) states that broker-dealers must have written policies and procedures in place to address the protection of customer information and records. Specifically, as detailed in NASD Notice to Members 05-49 (Safeguarding Confidential Customer Information), the policies and procedures must be reasonably designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- protect against unauthorised access to, or use of, customer records or information that could result in substantial harm or inconvenience to any customer.

Application of Data Protection law to DLT in the EU

The definition of personal data in the EU is broad and it is not always possible to eliminate personal data from your systems. Personal data is defined as any information which can identify a living individual. However, that has been interpreted very widely to include any data which can single out particular individuals or can be combined with other data sets to identify individuals. The rules on data privacy in the EU are currently being reformed by the General Data Protection Regulation 2016 ("GDPR"). Organisations have until 25 May 2018 to adapt their processing activities in line with the GDPR.

In order to determine the applicability of data protection rules, the first question that needs to be addressed is whether personal data is being processed when the distributed ledger is used. When using most blockchain systems both (i) the message in the block and (ii) the 'header' of a block (which lists any transactions, the time at which the list was made, and a reference back to the hash (or the "digital fingerprint") of the most recent block) may qualify as personal data.

Anonymisation vs. Pseudonymisation

In 2014, the Article 29 Working Party, provided guidance on the difference between pseudonymised and anonymised data in its Opinion 05/2014 (WP 216). This distinction is important in relation to DLT as data protection rules do not apply to anonymised data; as such data cannot be traced back to a living individual. However, the threshold for data to qualify as anonymised is very high.

Pseudonymisation is where one attribute (usually the unique attribute) is replaced in a record with another, such that the data can no longer be attributed to a specific data subject without the use of additional data. Although this technique reduces the ability to link a dataset to the original identity of a data subject, the Article 29 Working Party concluded that the 'natural person is still likely to be identified indirectly' so that when this technique is used alone it will not result in an anonymous data set.

The guidance also states that *"anonymisation results from processing personal data in order to irreversibly prevent identification."* Data controllers must have regard to all means "likely reasonably" to be used for identification (either by the controller or any third party). Encrypted personal data can often still be traced back to a person if enough effort is put into it by experts or someone holds the key to decryption. Therefore, encrypted data will often qualify as personal data and not as anonymous data. This means that in most instances the privacy rules will be applicable to at least some of the data involved in distributed ledger systems.

Case law has also confirmed the broad interpretation of data privacy rules. In the judgement in Case C-582/14 Patrick Breyer v Brundesrepublik Deutschland, the Court of Justice of the European Union ("CJEU") made clear that dynamic IP addresses may constitute 'personal data' even where only a third party has the additional data necessary to identify the individual. The possibility to combine the data with this additional data must constitute a "means likely reasonably to be used to identify" the individual. This approach focuses on the possibility of (potentially) identifying an individual and whether an online media service provider has the legal and practical means that enable it to do so with additional data a third party has about that person.

Who is the Data Controller?

Most of the privacy obligations are directed at the 'data controller'. The data controller is the party that determines the purposes and the means of processing, and who has the primary legal responsibility. Data processors process data on behalf of the data controllers. Under the GDPR, the obligations will not only be directed at controllers, but also at parties engaged by controllers as data processors. Therefore, the first step is to identify the roles of the parties involved. But, in the case of distributed ledgers, this is not clear cut. More than one party participating in a distributed ledger network could be responsible for compliance with the relevant privacy requirements. It is also likely that there will be a number of processing categories involved.

This combination of factors makes the application of data privacy to DLT a challenge. These issues will need to be carefully considered, especially in the face of fines for breaches of data protection, which can now cost firms up to 4% of global annual turnover for the preceding financial year, under the GDPR. The extent of the challenge will vary from case to case; for example, with permissioned distributed ledgers where only certain parties are able to add information, the allocation of control will be more clear and it will be easier to identify which parties should comply with what privacy requirements.

Another tenet of DLT is that the chain will most likely involve various computers that are located in different countries. As a result it may not be clear as to which rules of which jurisdiction will apply. The GDPR applies to controllers if it concerns:

a) the offering of goods or services to data subjects in the EU; and

b) the monitoring of their behaviour as far as their behaviour takes place within the EU.

As of 25 May 2018, the applicability of the European privacy rules will be expanded for controllers without an EU establishment. An assessment of the relevant jurisdiction will therefore also need to be made.

Automated Decisions

The GDPR provides protection for individuals against the risk that a potentially damaging decision is taken without human intervention. The incoming GDPR provides that individuals:

"shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

However, this is not an absolute right; exemptions apply when an automated decision is either provided by the law, is necessary to enter into a contract, or is based on the individual's consent. Nevertheless, the latter two exemptions still require that individuals have the right to obtain human intervention and to receive a justification of the automated decision. So while a fully automated system can exist, in practice, human intervention must still be possible.

"It may not be clear as to which rules of which jurisdiction will apply."

Singling-Out Risk

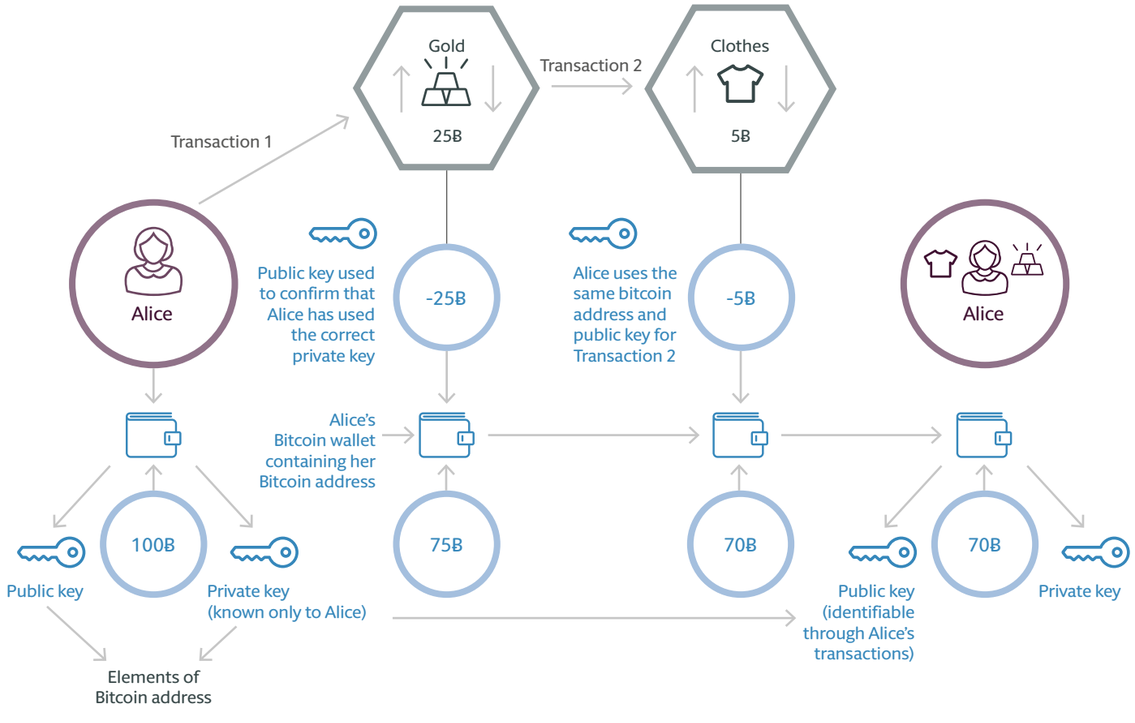
The nature of the public distributed ledger means that every transaction taking place will be published and linked to a public key that represents a particular user. That key is encrypted so that no-one who views the public ledger would be able to directly identify the individual or corporate entity that represents the user.

However, the re-use of the public key enables individuals to be singled out by reference to their public key, even if they cannot be directly identified. Indeed the very purpose of the public key is to single out the authors of a given transaction, to ensure that transactions are attributed to the correct people. The public key, when associated with an individual, will likely qualify as personal data for the purposes of European data protection legislation. Some newer DLTs permit the public key not to be published, which may alter the analysis.

When the public key is visible, it could be possible to attain information that enables an individual to be identified, either because it is held by the service provider or because someone is able to connect a public key to an individual or organisation, (for example, through their IP address or its connection with a website). At that point, all transactions that the relevant individual has made are publicly available and the individual can be re-identified.

Public key/Private key on a bitcoin transaction

Ƀ = Bitcoin



Re-identification Risk

In Recital 26, the GDPR recognises re-identification risk by considering whether a method of re-identification is *"reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."* Such an analysis is necessarily contextual and *"account should be taken of all the objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*

Right to Erasure

One key feature of DLT is that information cannot be removed from the ledger: for it is an immutable record. However, if there is personal data on the ledger, individuals have the right to have their data 'erased' when data is no longer necessary for the purpose for which it was collected or processed or when the individuals withdraw consent to processing. It is hard to reconcile these two principles. For example, in the case of blockchain, destruction of records affects the integrity of the blocks and so is not possible. We do not know how regulators will react to this, but at the very least this point will need to be made very clear to users.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

a) where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

b) when the individual withdraws consent;

c) when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;

d) the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);

e) the personal data has to be erased in order to comply with a legal obligation; and

f) the personal data is processed in relation to the offer of information society services to a child.

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

a) to exercise the right of freedom of expression and information;

b) to comply with a legal obligation for the performance of a public interest task or exercise of official authority;

c) for public health purposes in the public interest;

d) archiving purposes in the public interest, scientific research historical research or statistical purposes; or

e) the exercise or defence of legal claims.

> "The right to erasure does not provide an absolute 'right to be forgotten'."

International jurisdiction

Shared distributed ledgers have no specific location. This creates a problem in terms of jurisdiction and applicable law, as each network node could be subject to different legal requirements and there is no "central administration" responsible for each distributed ledger, the nationality of which could act as an source in terms of governing law and regulation. This also creates concerns regarding liability, as there may be no party ultimately responsible for the functioning of distributed ledgers.

Decentralised ownership

One of the advantages of DLT is that there is no single point of failure, as there is no centralised ownership. However, this advantage also comes with a number of complications: There is no central administering authority to decide a dispute between participants; Who is responsible for any defects, corrupted messages etc.?; Creating dispute resolution mechanisms where there is decentralised ownership is problematic.

Governance

Partly due to its decentralised nature, DLT is a technology that thrives on collaboration, but in the absence of a central party setting the rules, careful attention will be needed to establish cooperation mechanisms and clear governance rules to enable the DLT solution to evolve and respond to unexpected events.

From a practical perspective, there will be a need for someone to determine when changes to the DLT system are required to accommodate operational developments or to respond to legal or regulatory changes. Each participant should ensure it is clear within its organisation who has authority to write/validate entries. There must also be processes in place to limit the operation of access keys (e.g. through public key infrastructure or 'PKI') to authorised personnel, as participants are likely to be liable for the actions of those using their access keys.

From a regulator's perspective, a decentralised governance arrangement that simply operates as a set of contractual rules between the users of the system is likely to be less attractive than a centralised governance arrangement, as it would make it more complicated for the regulators to supervise the system. The nature of the governance arrangement therefore needs to be carefully considered before the launch of any proposed DLT system.

The FCA's discussion paper on DLT published in April 2017 raises the point that there also will be implications for firms regarding their third party service providers.

"For example, if a regulated firm using a DLT platform relies on third parties to add, validate, safeguard and preserve transaction, does it have sufficient oversight of these activities to fulfil its regulatory obligations around having appropriate system, governance and controls? What interaction would firms have with the 'core developers' group of public, permissioned DLT networks, who typically carry out update and have other important responsibilities?"

IPR issues

Like any other new technology, the practical implementation of DLT solutions in the insurance sector will require navigation of a complicated landscape of intellectual property rights (IPR). That IPR landscape becomes a potentially global, multi-jurisdictional, concern when cross-border distributed ledgers are considered. Patent and copyright issues present in the context of traditional insurance activities are compounded by DLT-specific IPR issues.

The offering, sale, implementation, and processing of insurance products and services using DLT are all potentially subject to patent protection. Many of the expected benefits of such new offerings flow from underlying technological innovations that may be patentable. However, patent laws in many countries continue to evolve. While abstract ideas, methods of doing business, and computer software, for example, may be ineligible for patent protection in some jurisdictions, other jurisdictions allow it. In the hope of finding fertile ground, a patent land rush is already underway in connection with many distributed ledger-based technologies.

Copyright law also presents challenges for DLT-based insurance innovations. Much like content on the internet, the easy accessibility of information on a distributed ledger does not guarantee that information is in the public domain. Documents published on a public distributed ledger are still protectable under copyright law. Stores of data on a distributed ledger can be a copyrightable database. Even the data accessed by a smart contract running on a distributed ledger may be content owned and licensed by a third-party provider. However, the issue for the copyright owner will be in enforcing its rights

The computer software that builds the distributed ledger, the individual applications that access information on a distributed ledger, and the graphical interfaces presented to human users are all capable of being protected by copyright. The smart contracts may be copyright protected too.

Parametric Insurance and DLT

Parametric insurance may lend itself particularly well to smart contracts. Unlike traditional insurance products, parametric insurance does not typically pay claims based on actual losses incurred by the insured. Rather, it pays a pre-set, actuarially-determined amount upon occurrence of the triggering event.

Under such a framework, the actual loss sustained by some of those insured may be more than the specified payment amount, while the loss sustained by others may be less. Gone from the equation is the need for adjusters to determine the amount of the actual loss or whether non-covered, concurrent causes of loss, such as an old roof in ill repair or flood damage, were contributing factors. The claims payment process is streamlined and automatic. Other potential weather-related parametric insurance applications include crop insurance and travel insurance.

Faster claims payments mean that those insured can recover more quickly following weather-related losses. Furthermore, smart insurance contracts could dramatically lower insurers' administrative costs, with at least a portion of that saving potentially passed on to consumers in the form of lower premiums. Because parametric policies generally do not cover the actual losses of those covered, traditional insurance policies may be desirable to cover any amounts above the parametric policy payout.

At least certain aspects of the parametric insurance paradigm are potentially applicable to other lines of insurance as well. An often cited example is a life insurance smart contract.

In the U.S., one potential source of external verification that a covered individual has died is the Social Security Administration's so-called "Death Master File." Upon such verification, a smart contract could automatically generate payment to the contract's beneficiary. The contract could forego typical exclusions for death caused by suicide, for example, or could require a second verification ruling out excluded causes of death.

A permanent, immutable record of the smart contract on a distributed ledger could virtually eradicate the frequent inability of family members or other beneficiaries to locate, or even confirm the existence of, a decedent's life insurance policy. In the U.S., the NAIC is currently attempting to assist potential beneficiaries through manual enquiries with insurers who participate in its "Life Insurance Policy Locator Service" on a voluntary basis. Smart life insurance contracts have the potential to efficiently and effectively replace such a labour-intensive and incomplete solution.

Great care is needed in the design and drafting of this type of insurance to ensure that it will be categorized as insurance in the relevant jurisdictions in which it is arranged, bought, sold and enforced. This is important from both a legal and a regulatory point of view.

Two key issues which must be considered in the UK are the questions of:

– whether it is necessary for insured to have an insurable interest in the traditional sense; and

– whether the insured has to suffer a loss to be able to claim.

It should be noted that the FCA is considering providers of this type of insurance in its regulatory sandbox and it will be fascinating when it reveals its views.

P2P Insurance and DLT

How does P2P Insurance on DLT work?

As discussed above, a group of participants could use the decentralised trust and autonomous processing capabilities of smart contracts as a means by which to spread risk among group members. Smart contract coding allows risk pooling among participants according to specified terms and conditions. This means there is no need for a centralised authority to determine insurability, provide premium quotes, send evidence of coverage, or determine and pay claims. Alternatively, it allows for a centralised authority with a more limited role than a traditional insurer.

Regulatory perspectives and potential challenges

Unresolved regulatory questions in connection with P2P insurance based on smart contracts include, for example:

- who the appropriate regulatory authority is, given that transactions could occur across widely dispersed jurisdictions;
- potential consumer data privacy issues; and
- the extent to which the volatility of cryptocurrencies used to pay premiums and claims poses a solvency risk.

Different jurisdictions will treat P2P insurance using DLT in very different ways depending on whether the P2P activities could, for instance, represent the provision of insurance or the carrying on of insurance mediation and whether those activities are regulated activities in the jurisdiction in question.

The legal tests for the delineation of those activities varies quite widely by jurisdictions.

In France it is possible that a P2P service might not constitute an insurance contract if a premium is not paid by the insured or an indemnification is not made to the insured on the occurrence of the risk which has been insured. This may very well be the case in some P2P solutions.

Under UK law and regulation it is possible to see how some P2P arrangements might be considered to consist of regulated activities.

The FCA in the UK is yet to publish specific rules and guidance on this form of insurance. P2P insurance arrangements must, therefore, be designed with existing law and regulation in mind. This can give rise to some challenges for P2P insurance start-ups. It is encouraging that the FCA is considering some P2P insurance operations in its regulatory sandbox and it is hoped that tailored guidance will emerge shortly.

The EIOPA also stated in April 2017 at its roundtable event on 'How technology and data are reshaping the insurance landscape' that: *"regulatory and supervisory authorities may need to consider whether the classification of P2P insurance is sufficiently clear, and whether there is also a case for developing specific regulation for P2P insurance."*

In the U.S. existing insurance regulatory requirements will likely be interpreted to cover P2P insurance. For example, where each participant in a P2P insurance arrangement is obligated to pay another participant upon the happening of a "fortuitous event," the entire enterprise, and each participant, could be considered to be acting as an insurer.

The NAIC has stated that *"although, P2P insurance could and should be regulated like any other insurance company within the existing regulatory framework of state regulation, this innovative model of managing and delivering insurance products presents a new challenge for state insurance regulators to study its strengths and weaknesses as well as its differences from traditional insurers."* Further, the NAIC cautioned that *"understanding the need for innovation, state insurance regulators' actions are always guided by the need to protect the interests of policyholders who rely on the insurance coverage as well as to help maintain the stability and reliability of the insurance industry."*

Potential challenges of Parametric Insurance and DLT

Another potential issue with P2P insurance smart contracts is a possibility for increased fraud with internet-based claims verification processes that rely solely upon documentary evidence of a claim or a policyholder's statements, without any in-person inspection of loss. P2P insurer Lemonade detects fraud by supplementing videos created by those insured with the use of anti-fraud algorithms. It also aims to decrease the incentive for insurance fraud by donating "leftover" premiums to charities chosen by policy holders themselves. The effectiveness of this approach remains to be seen.

Potential benefits

Despite some potential regulatory challenges, there appears to be wide recognition of the significant consumer benefits that DLT facilitated P2P insurance could offer. The NAIC has observed that P2P insurance as a business model is *"already being offered using standard technology,"* and that DLT *"could make it even more transparent and trustworthy for consumers as no central authority controls its operation."*

Streamlined claims handling and an accompanying reduction in claims adjustment costs can result in consumer savings and enhanced consumer satisfaction.

> There appears to be wide recognition of the significant consumer benefits that DLT facilitated P2P insurance could offer.

Lemonade

Lemonade, for example, also uses videos created by policy holders to determine the validity of homeowners and renters insurance claims, and reports to have paid claims in as little as three seconds. Lemonade's co-founder and CEO, Daniel Schreiber, reportedly claimed that costs in the insurance sector could be reduced by a factor of ten. He also claimed that expense ratios in homeowners insurance are responsible for almost one third of premiums and loss adjustment expenses account for 10-12% of premiums. By lowering overhead and utilising alternative methods of claims adjusting, P2P insurance programs, like Lemonade, could lower premiums for consumers.

In Spain, the local interpretation of the Insurance Mediation Directive emphasises the need for insurance mediators providing real advice to customers, in case a distribution chain through auxiliaries is needed. An automated selling process will still require, according to that interpretation, that customers have access to "real human" advice, at least when requested.

DYNAMIS

Dynamis is another DLT facilitated P2P insurance platform that uses innovative methods of underwriting and claims adjudication. The platform provides supplementary unemployment insurance using LinkedIn as an oracle to verify information regarding applicants and claimants, including verifying employment status through an insured's LinkedIn connections. Smart contract logic is used to automate the underwriting and claims processes, and claims are verified by policyholder peers. In order to have a claim validated, a claimant must first contact potential peer validators via LinkedIn, have at least two conversations in person or over the phone, and ask the validator to respond to a validating email.

Such procedures suggest that while smart contracts have the potential to lower transactional costs and increase efficiency in the insurance market to the benefit of both insurers and consumers, P2P insurance smart contracts are unlikely to entirely eliminate the need for human intervention, at least in the near term.

ai gang

Aigang Network is a new name in this space and has recently made history with the launch of its Android and iOS demo app. The firm is based in Singapore and was formed in 2017 to research and develop prototypes for digital insurance built on, and powered by, blockchain technology. The Aigang Network's blockchain protocol provides next-generation digital insurance for Internet of Things (IoT) devices using Decentralised Autonomous Organisation (DAO) and smart contracts. For a showcase of their blockchain protocol for digital insurance, Aigang has selected smartphones. The most common technical issue for a smartphone is battery malfunction, and a trend in decreased warranty periods has resulted in many owners facing costly repairs or battery replacement. Aigang implements risk assessment software to monitor the degradation of the phone battery. Once the battery reaches a critical state, the payout is automatically processed and executed by smart contracts.

Aigang Network is in the process of expanding its team of blockchain protocol professionals. The demo app showcases how a new technology can enable digital insurance for IoT devices. In the future, the company plans to roll out digital insurance for self-driving cars and drones.

KYC and DLT

As noted above, it is possible for DLT to assist in verification of the identity of users, intermediaries, beneficiaries, and counterparties. Some companies have begun developing "KYC shared utilities" to compile, verify, and store customer information sent from financial institutions. They then centralise such data, periodically verify it, and then offer the information back to financial institutions as "verified" identities for KYC purposes.

However, there are several challenges to the use of DLT for KYC purposes:

a) it remains to be seen whether AML regulators will allow insurers (and other financial institutions) to rely on such technologies to perform their KYC due diligence;

b) in addition – and a function of AML issues generally – these KYC issues are often at odds with data privacy (and sometimes cybersecurity) requirements. Depending upon the level of "pseudonymisation" used for the data, the data may be of limited utility for AML/KYC compliance purposes; and

c) this issue is further exacerbated in cross-border transactions and financial arrangements, especially where the privacy regimes are different. For instance, a U.S.-based financial institution may not be able to rely on a "KYC shared utility" if some of that information is restricted because of overseas requirements on the disclosure, maintenance, or use of personal information of a foreign citizen.

Yet, there are also challenges beyond basic "personal" KYC (i.e. information solely related to verifying the identity of a natural personal), some of which might in fact be addressed by DLT technology:

a) frequently, financial institutions (including insurance providers) are responsible for knowing their customers' source of funds – in other words, sometimes financial institutions are required to know not just the identity of their customer, but also ensure that their customer's financial transactions are not predicated upon unlawful activity; and

b) financial institutions are faced with growing regulatory expectations (and sometimes criminal law requirements) to understand the ultimate beneficial owner of legal entities, such as shell and shelf corporations, nominee accounts, and other entities and structures used to conceal the underlying identity of the owner or controller of a certain business or account.

DLT technologies may allow insurers and other financial institutions to determine the ownership or control of these entities, in furtherance of their AML/KYC requirements, so it will depend on how the regulators address the challenges of using DLT technologies in AML/KYC which will ultimately determine how effective the technology is at addressing some of the more general issues with AML/KYC.

Conclusion

As can be seen from the issues raised in this report there are many legal and regulatory factors which need to be considered when considering DLT implementation in the insurance sector. There are some difficult issues which, as you will have seen, do vary depending on the jurisdiction involved.

This is at the heart of the challenge of DLT implementation. It is clear that an early review of the key legal issues that might apply to your particular service, taking into account your key jurisdictions, will be important. It is equally clear that the regulators are all beginning to engage on this topic and we will see a developing picture of regulation in the foreseeable future.

We hope that the report has fulfilled its principal objective of education and moving the debate forward and would welcome feedback and comment as we ourselves develop our thinking.

Glossary

"AML"
means Anti-Money Laundering which refers to a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions.

"ASIC"
means the Australian Securities & Investments Commission, an independent Australian government body that acts as Australia's corporate regulator. ASIC's role is to enforce and regulate company and financial services laws to protect Australian consumers, investors and creditors.

"BaFin"
means Federal Financial Supervisory Authority (German: Bundesanstalt für Finanzdienstleistungsaufsicht), the financial regulatory authority for Germany. It is an independent federal institution under the supervision of the German Federal Ministry of Finance

"DTCC"

means the Depository Trust & Clearing Corporation, a subsidiary of the National Securities Clearing Corporation (NSCC). The DTCC, established in 1973, settles transactions between buyers and sellers of securities and through its subsidiaries, advances industry-leading solutions that help secure and shape the future growth and development of the global financial marketplace.

"EIOPA"
means the European Insurance and Occupational Pensions Authority, it is a part of the European System of Financial Supervisors that comprises three European Supervisory Authorities, one for the banking sector, one for the securities sector and one for the insurance and occupational pensions sector. It is an independent body providing advice to the European Commission, the European Parliament and the Council of the European Union.

"ESMA"
means the European Securities and Markets Authority, an independent EU Authority that contributes to safeguarding the stability of the European Union's financial system by enhancing the protection of investors and promoting stable and orderly financial markets

"FCA"
means the Financial Conduct Authority, the conduct regulator for financial services firms and financial markets in the UK.

"FINRA"
means the US Financial Industry Regulatory Authority, a not-for-profit organisation authorised by Congress to protect America's investors by making sure the broker-dealer industry operates fairly and honestly.

"IAIS"
means the International Association of Insurance Supervisors, a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions, constituting 97% of the world's insurance premiums.

"KYC"
means Know Your Customer this refers to the process of a business identifying and verifying the identity of its clients.

"NAIC"
means the National Association of Insurance Commissioners, the U.S. standard-setting and regulatory support organisation. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight.

"PRA"
means the Prudential Regulatory Authority, which is a part of the Bank of England and responsible in the UK for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. It sets standards and supervises financial institutions at the level of the individual firm.

"WEF"
means the World Economic Forum, the International Organisation for Public-Private Cooperation.

Quotes from industry experts

We asked some industry experts for their view of DLT in the insurance sector:

Gary Nuttall, has over twenty-five years working on all aspects of information delivery with a passion for promoting better informed decision making. Gary moved into the insurance sector in 2010 with Chaucer Syndicates where he built up the Business Intelligence practice. In early 2016 he founded Distlytics Ltd with the aim of providing insight, consultancy and expertise in Distributed Ledger / blockchain technology and its application in the commercial insurance sector.

Use cases

"Blockchain is (wrongly) being sold as a cost reducing technology. In this instance we'll see claims transformation, policy management and accounting systems adopting the technology. However, blockchain (particularly smart contracts combined with other emerging technologies such as IoT and AI) will see new products and services created. This is far more exciting and could disrupt the industry far more than just improving the claims process. Think of the creation of new insurance marketplaces, Usage Based Insurance, etc."

Technical Challenges

"The only "technology" challenge is the upheaval and replacement (or upgrading) of legacy applications and their associated multi-year investments. Insurers have invested millions on policy admin and general ledger systems. To truly benefit from blockchain, these need to be replaced, retrofitted or retired, perhaps sooner than originally planned."

Legal and regulatory challenges

"I don't foresee an issue with blockchain adoption per se. Trying to replace Insurance Contracts with Smart Contracts is another matter. Unfortunately too many people think they know what the word smart and the word contract mean and so assume they understand what a smart contract is. This misunderstanding is likely to be a hurdle if technologists try to "legalise" a smart contract. It's not quite that simple. As for turning an Insurance Contract into a smart contract? The techies should take a look at just how thick a policy document is. It's not just a series of IF / THEN /ELSE statements."

Regulations you think impede the progress of implementing blockchain

"Financial regulations don't apply to technologies but rather to their application. The FCA doesn't regulate SQL databases and Excel spreadsheets. It does however put an onus of responsibility for compliance of organisations using the results of the technology. I expect blockchain to follow the same pattern."

How long do you think it will be until blockchain is a fully integrated part of the insurance sector?

"I expect to see green field insurers, particularly MGA's, using the technology within twelve months. Mainstream insurers will need to revisit their technology platform strategies and so are likely to not use DLT mainstream for three to five years."

Josep Cascals, is an entrepreneur and a data architect. He founded Masvoz, a specialized telecoms operator in Spain. More recently, he has been involved in IoT and large scale data analytics as head of data engineering of the Centrica group company hivehome.com.

Use cases

"Mainly applications on public distributed ledgers. There are applications in private or corporate blockchain networks, but in my view, these are much more limited and may not represent an improvement over known distributed databases"

Technical challenges

"Main technical challenges are the security of Smart Contracts and capacity/throughput of public blockchain networks. Also, ensuring minimal capital requirements is technically quite complex."

Legal and regulatory challenges

"I see two major problems. Firstly, there's a jurisdiction problem. It's very difficult to control the country of residence of anyone who sells or buys this kind of insurance given that its automated from purchase to payment and open to anyone. Secondly, it's difficult to determine who is the "principal" or underwriter in a smart contract. It could even be that the policy holders become the underwriters in a sort of distributed mutual."

Regulations you think impede the progress of implementing blockchain

"In a public network, nowadays I believe it's impossible to implement unless one is willing to take the risk (similar to the current case of some ICOs). I think there'll be jurisdictions who'll be cooperative. The UK is still working on the policy for these cases, but I know they FCA is committed to it. I also have hopes for Switzerland and Estonia. Within the EU, Solvency II is a big obstacle because no single country can override this."

How long do you think it will be until blockchain is a fully integrated part of the insurance sector?

"I think there'll be a parallel insurance sector taking over part of the current insurance sector business. If we make an analogy with Telecoms companies and the Internet, there are still telecoms companies, but many traditional telecoms applications are now performed by unregulated Internet companies (e.g. Skype). Something similar may happen with insurance once crypto currencies become mainstream".

Insurance/ blockchain contacts

Helen Chapman
Partner, London
+44 20 7296 2588
helen.chapman@hoganlovells.com

Theodore Mlynar
Partner, New York
+1 212 918 3272
ted.mlynar@hoganlovells.com

Therese Goldsmith
Partner, Baltimore
+1 410 659 5071
therese.goldsmith@hoganlovells.com

Lewis Cohen
Partner, New York
+1 212 918 3663
lewis.cohen@hoganlovells.com

Gregory Lisa
Partner, Washington, D.C.
+1 202 637 3647
gregory.lisa@hoganlovells.com

John Salmon
Partner, London
+44 20 7296 5071
john.salmon@hoganlovells.com

Susan McKiernan
Counsel, London
+44 20 7296 5011
susan.mckiernan@hoganlovells.com

Winston Maxwell
Partner, Paris
+33 1 53 67 48 47
winston.maxwell@hoganlovells.com

Dr. Christoph Küppers
Partner, Dusseldorf
+49 211 13 68 523
christoph.kueppers@hoganlovells.com

Joaquin Ruiz Echauri
Partner, Madrid
+34 91 349 82 74
joaquin.ruiz-echauri@hoganlovells.com

Dr. Sebastien Gros
Partner, Paris
+33 1 53 67 16 23
sebastien.gros@hoganlovells.com

Kerri Cutry
Associate, New York
+1 212 918 3736
kerri.cutry@hoganlovells.com

Hogan Lovells Engage: blockchain tool

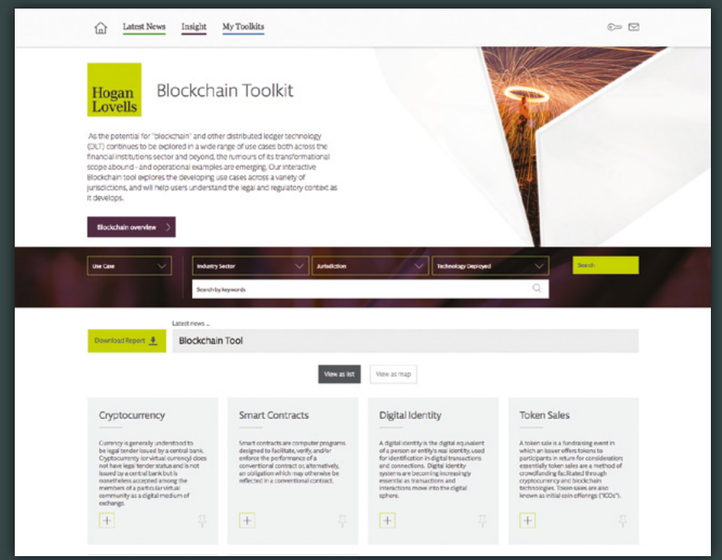
Take advantage of blockchain's huge potential and disruptive impact, while avoiding falling foul of ever-developing regulatory and legal requirements.

The Hogan Lovells Engage: Blockchain Toolkit lets you:

- investigate the different ways blockchain can be used
- see where the new technology is shaking up industries
- track unfolding legal and regulatory approaches across jurisdictions
- use interactive functionality to download reports and share information

Get started now by registering on:

hlengage.com/blockchain



Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com