CRO FORUM

2019

Insurance and Distributed Ledger Technology

A risk manager's perspective

Table of Contents

Executive Summary

Hype has surrounded Distributed Ledger Technology (DLT) and especially blockchain[1] over the last few years since the birth of the Bitcoin cryptocurrency. Hype, and criticism too, have been fuelled by fervent visions as well as misconceptions. These technologies have not yet delivered on promises, but several experts believe that DLT has the potential to transform the financial services industry. According to Gartner, a research and advisory company, DLT has now passed the 'peak of inflated expectations' and in 2020 will start to deliver full value propositions[2]. This paper by the CRO Forum is meant as a practical tool for risk managers to accelerate the accomplishment of the productive phase of DLT.

In line with its emerging technology status, DLT's risk profile is developing along with its business potential. Plus, the decentralized nature of DLT creates threats that are different from the ones arising from traditional centralized solutions. The CRO Forum believes that, although traditional risk management frameworks remain valid, there are specific issues to consider when assessing the risk of a DLT-based application. Are the technology and its place in the business process well understood? Is a DLT approach truly necessary and applicable? How to ensure appropriate governance around an emerging complex technology? How to guarantee that all relevant risks are identified and managed?

The paper introduces the technology, provides advice on how to perform a risk assessment, discusses risk management governance, and highlights the contribution that CROs can provide within respective companies as well as to the broader DLT ecosystem. A detailed risk catalogue is provided along with possible risk mitigation strategies. Since there are still vast areas to be explored around DLT, also experts in compliance, law, security and technology, along with business specialists, can obtain hints to address challenges and inform collaboration.

1 See the following chapters for high-level explanations of technical terms.
2 Five Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, Gartner, 2018 and The 4 Phases of the Gartner Blockchain Spectrum, Gartner, 2019.

The authors have purposely decided not to deal with specific technology features and examples from recent developments. Indeed, while technology evolution will make current solutions and stories obsolete in a relatively short time span, the risk management approach described herein will make this paper valuable in the longer run.

To make the paper practical, however, two risk assessments of real DLT-based solutions are provided as examples. The first analysis regards an application developed by B3i[3] to manage the entire placement process of catastrophe excess-of-loss reinsurance (CAT XL) across cedants, brokers and reinsurers. The second assessment examines a travel insurance product, which automatically reimburses those insured travellers who experience a flight delay. These two cases, although not exhaustive, cover a broad range of conditions and features. CAT XL is a reinsurance B2B solution piloted by a startup aiming to create an ecosystem, while the travel insurance product is a B2C solution commercialized by a leading industry player.

Key paper findings address the early stage of DLT-based solutions when adopters, without standardization, face uncertainty as well as strategic risks. As discussed in the conclusions section, with emerging technologies risk assessments must be refreshed often to cope with a rapidly evolving context. A decentralized system is appropriate only under specific circumstances like, for example, when numerous independent parties wish to maintain common data. When smart contracts are used, their logic needs to be validated thoroughly and when oracles are used, data availability and integrity can be critical. Interoperability can also be a challenge both among DLT applications and between DLT and legacy systems. Many of the challenges in adopting DLT solutions, however, are pretty much like the ones linked to the adoption of traditional IT.

3 B3i, The Blockchain Insurance Industry Initiative was formed in late 2016 as a collaboration of insurers and reinsurers to explore the potential of using DLT within the industry for the benefit of all stakeholders in the value chain.

1 Introduction to Distributed Ledger Technology (DLT)

A distributed ledger can be considered as a database that is distributed across several independent computing devices where changes to data are protected and manged by cryptography and consensus[4], providing guarantees that data cannot be tampered with and that all parties have identical copies that can be considered as a reliable single source of truth. The functionality of a distributed ledger system can be enhanced by the use of smart contracts (i.e. computer programs deployed and executed on the ledger's network) and oracles (i.e. data feeds that trigger specific conditions defined within smart contracts). The blockchain is a very specific case of DLT that became famous through its use with Bitcoin.

Several experts believe that DLT has the potential to transform the financial services industry[5]. Parties will be able to maintain accurate and shared records of financial agreements without duplications, alterations, reconciliations or failed matches. Many consider a distributed ledger a particularly transparent way of handling records in financial services because the information is shared, and thereby witnessed, across a network. DLT creates and maintains a 'single version of the truth' between multiple parties thereby reducing time-consuming and cumbersome exchanges as well as reconciliation of many documents. When a secure single source of truth is available, audits and regulatory scrutiny can also become much more reliable and efficient.

In insurance, for example, DLT enables more efficient claims handling by automating business processes and limiting the scope for disagreement between parties. As claim events are recorded in a distributed ledger, duplicate claim reporting can be prevented and fraud minimised.

Benefits of DLT can also include simplified underwriting, with automated processes collating and assimilating information, more efficient reinsurance processes, clearing and settlement time reduction, and new Peer-to-Peer (P2P) distribution methods. Automated parametric insurance can also benefit from DLT and smart contracts[6].

However, while promising to drive efficiency in business practices and mitigate certain existing risks, the adoption of DLT may trigger new risks to insurance firms and markets. Adoption of DLT at scale is therefore likely to be several years away. For insurers, a key issue resides with the building of a DLT 'ecosystem', as companies that build DLT networks of their own enjoy only limited benefits. Successful DLT initiatives require competitors to work together and whilst that may be possible for non-competitive tasks, it will be a challenge for competitive use cases.

4 Process by which the participants in the network reach a general agreement that the ledger is in a valid state.
5 Corda: An Introduction, R. G. Brown et al., 2016.
6 Blockchain/DLT in the Insurance Sector, Hogan Lovells, 2017.

1.1 Blockchain and DLT, in brief

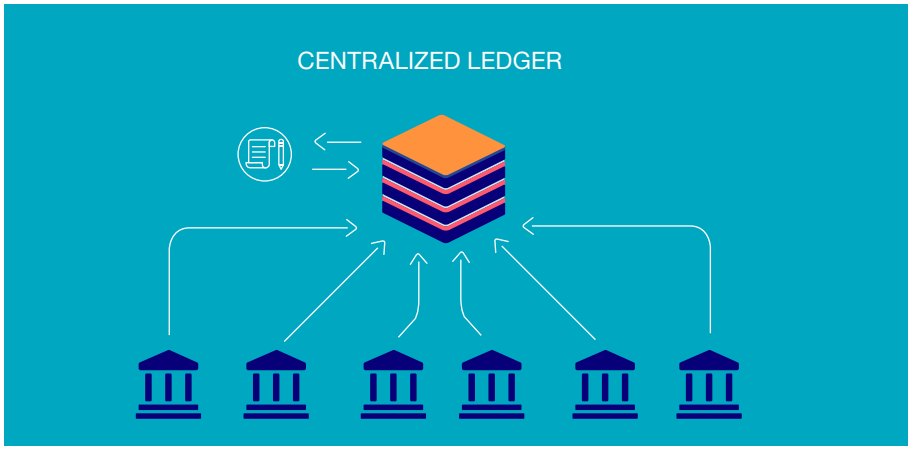
In essence, a distributed ledger is a database spread across several independent computing devices (nodes). The value proposition of DLT is that data is created and maintained as a 'single version of the truth' and stored in a ledger that is not controlled by any central authority. Each node, with which the data is shared, replicates and saves the transactions in the ledger in consensus with counterparties. Therefore, data cannot be modified without the consent of all the involved parties.

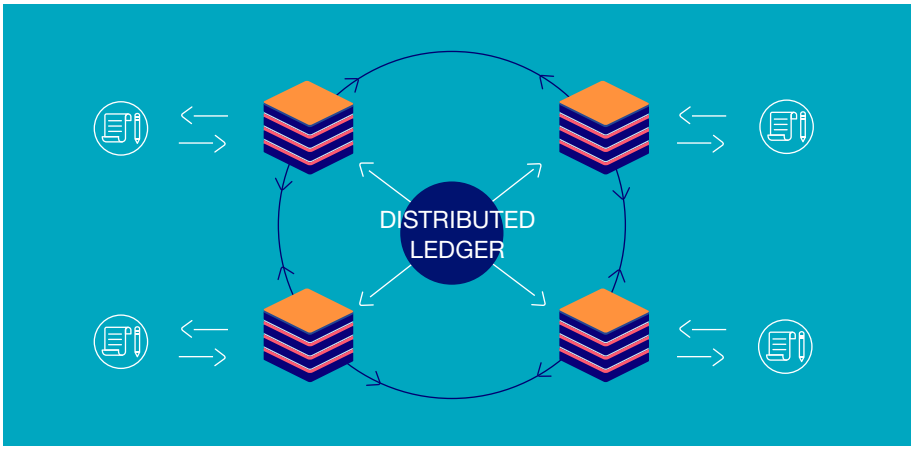
Blockchain technology was designed for enabling Bitcoin, the first decentralized cryptocurrency. Since Bitcoin, the technology has evolved to enhance the original implementation's scalability, privacy and security. The new term DLT has been introduced because selected recent implementations have no concept of blocks or chains anymore and the term blockchain is no longer accurate. Therefore, every blockchain is a distributed ledger, but not every distributed ledger is a blockchain. Nevertheless, DLT is always based on decentralization and consensus among nodes.

Blockchain technology organizes data in blocks linked to one another in a chronological manner and updates these entries using an append-only structure. As entries are added, the nodes validate these updates to ensure that they agree with the conclusion reached. This validation and agreement on a single copy of the chain is called consensus and is typically conducted automatically by a consensus algorithm. Once consensus has been reached, the chain updates itself and the latest, consented version is saved on each node separately.

This process only allows data to be added to the ledger, so altering or deleting previously entered data on earlier blocks is impossible without controlling the majority of the consensus algorithm.

Centralized ledgers need a trusted operator to collect and store data, on the other hand DLT allows all contributors to collectively validate the data.

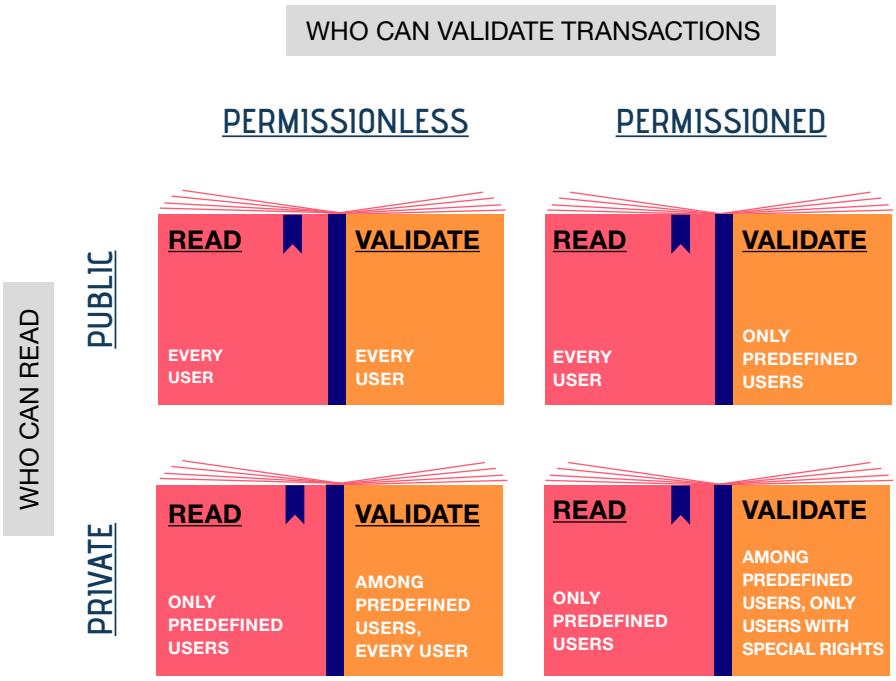




A blockchain is essentially a continuously growing list of records and blockchain technology is thus well-suited for use-cases like recording events, managing records, processing transactions, tracing assets, and voting.

While blockchain technology stores data items linked to one another in a chronological manner within blocks, DLT can also store data in the form of graphs or tree structures. These sophisticated structures enable use-cases requiring 'need-to-know' sharing of data[7] and other privacy requirements. For example, R3 Corda DLT platform enables nodes to share data only with selected parties while the original blockchain implementation, Bitcoin, requires all data to be shared with all participants.

Throughout this paper, unless otherwise specified, the words blockchain and distributed ledger may be used interchangeably.



Contributors' access to distributed ledgers can be open or restricted according to permission protocols.

Does blockchain truly maintain a single version of the truth? The 51% attack

Blockchain technology organizes data items in blocks and network nodes validate the updates as they are entered. This agreement on a single copy of the chain is called consensus. Altering or deleting previously entered data on earlier blocks is impossible without controlling the majority of the consensus algorithm. The Proof-of-Work (PoW) consensus algorithm requires participants to invest significant computational power to participate in the consensus process. Simply put, the PoW algorithm is a way to deter blockchain malicious parties from committing abuses by requiring work (i.e. computational effort) to participate in the consensus process. Therefore, malicious network participants, given enough computational power, might be able to take control of a PoW-based blockchain network (e.g. Bitcoin, Ethereum) and rewrite its most recent transaction history.

The hypothetical vulnerability of a cryptocurrency depends, among other factors, on its value and network size. The website Crypto51 estimates the cost of the computational power required to match the network power of various cryptocurrencies. Overtaking Bitcoin and Ethereum for one hour, for example, at the time of writing would cost about $600.000 and $150.000, respectively. Other cryptocurrencies are more exposed. Based on this information, it is possible to calculate the cost of a 51% attack as well as evaluating whether an attack against a specific cryptocurrency would be worthwhile.

In 2018, cryptocurrency hackers earned about $20 million through 51% attacks[8], while in January 2019 a series of attacks were made on the Ethereum Classic blockchain and about $200.000 worth of transactions were revoked after being traded on multiple cryptocurrency exchanges[9]. In its non-blockchain versions, however, DLT has no concept of blocks or chains and is not vulnerable to 51% attacks.

7 Under need-to-know restrictions, one is given access to data only if he or she needs information access to conduct own duties.
8 Group-IB, Annual Hi-Tech Crime Trends 2018 report.
9 Bloomberg, Cryptocurrency Deals Can Always Be Erased for a Price, 2019.

1.2 Smart contracts and oracles

A smart contract is a deterministic computer program[10] that is deployed and executed on a DLT network. Smart contracts, for example, are capable of automatically validating a condition and it will automatically determine whether an 'asset' should go to a nominee, or back to source, or a combination thereof. In contrast to what the name might suggest, a smart contract does not necessarily mean the creation or performing of a contract or other legal act.

On public, permissionless blockchains (e.g. Ethereum) smart contracts execute on each node while permissioned DLT (e.g. R3 Corda) can limit the execution of smart contracts to selected parties. If cryptocurrencies or other crypto-assets are involved, the smart contract code can also automatically transfer these tokens, thus effectively enforcing the outcome of the smart contract. The application of smart contracts is limited due to the pre-programmed nature of the smart contract code.

In order to determine whether the conditions for the performance of a smart contract have been met, data (input) from outside the ledger will often be required. As smart contracts are evaluated by multiple parties at different times, retrieving information from the outside, non-DLT world, requires careful design. For instance, smart contracts for parametric insurance built on an external trigger are exposed to different evaluation results if the trigger's value is modified. This is where so-called oracles come into the picture. Oracles can provide secure input to smart contracts.

An oracle, also known as a data feed, is typically a third-party service designed for use in smart contracts on a distributed ledger. Oracles provide external data when needed, attest to the correctness of the data and push it onto the distributed ledger. The key is for all the parties to the smart contract to agree on the identity of the oracle. The challenge with oracles is 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. If the oracle alters the information taken from other sources or provides defective data, there may be no rewind or reset.

Are smart contracts that smart? The DAO incident

A smart contract is a deterministic computer program that is deployed and executed on a DLT network. On public and permissionless blockchains, smart contracts execute on each node. If cryptocurrencies are involved, the smart contract code can also automatically transfer these tokens, thus effectively enforcing the outcome of the smart contract. Unlike traditional software where bugs can be fixed through patches, in the decentralized blockchain world deploying live smart contracts can be problematic. The critical point is that blockchain transactions cannot be undone.

The Decentralized Autonomous Organization (DAO) hack in 2016 is a classic case of smart contract bug exploitation. The DAO, a venture capital fund implemented on the public Ethereum blockchain, hosted a voting mechanism for investors to decide on money allocation. Unfortunately, an attacker exploited a flaw in a smart contract governing the DAO and stole more than $60 million worth of cryptocurrency. The hacker kept requesting money from accounts without the system registering that the money had already been withdrawn. In January 2019, Ethereum came close to a reoccurrence of the DAO case. One day prior to a software release, Ethereum developers were told that the upgrade would leave some contracts on the blockchain vulnerable to the same kind of bug that had led to the DAO incident[11]. Permissioned DLT, however, unlike blockchains, can limit the execution of smart contracts to selected, authorized parties and are therefore less exposed to exploitations.

10 A computer program is deterministic if, given specific input and initial state, it will always generate the same output.
11 Once hailed as unhackable blockchains are now getting hacked, MIT Technology Review, 2019.

1.3 Pros and cons of DLT applications

Although some of the mentioned applications could be created without a DLT, they tend to be associated with DLT.

INSURANCE VALUE CHAIN

Claims management

- ✓ Better customer experience (shorter processing times, payments are automatically executed, eliminate the trust issue)
- ✓ Fraud reduction
- ✓ Cost reduction because of reduced or removed manual intervention
- × Significant investment for existing insurance companies to migrate from existing processes and systems to automatic claims processing

Reinsurance

- ✓ Reduce manual records and address current inefficiencies and weaknesses
- ✓ Simplify sharing of data like bordereau and claims databases
- × Has value when used by multiple parties and integrated with other company systems

Marketing and distribution

In private DLT, customer on-boarding: Know Your Customer (KYC), Anti-Money Laundering (AML)

- ✓ Cost reduction
- ✓ Fraud prevention
- × Has value only when used by multiple parties to share client information and evidence of validation

Distribution: P2P insurance

- ✓ Reduced cost for sharing risk between participants
- × Has value only when used by multiple participating parties willing to share risk

Pricing and underwriting

- ✓ Better pricing (real-world data about insured goods or individuals)
- ✓ Flexible and personalised insurance products and risk management
- ✓ Reduce paperwork, time inefficiency and risk of omissions
- × Assumes data sharing mechanisms and willingness of parties to contribute

Product design: Smart contracts / Automated parametric insurance

- ✓ Policy Contract is automatically executed at the occurrence of an insured event, triggered by an external oracle, or multiple oracles
- ✓ Payments are automatically executed
- × Dependency on oracles / external data feed (sensitive to hacking)
  No reverse option
- × No data privacy in case of public blockchain, data is accessible by everyone
- × Basis risk in parametric insurance payments (the actual loss amount is not checked anymore as the role of the adjusters to determine the amount of the actual loss or whether non-covered, concurrent causes of loss, were contributing factors, is taken out)

2 The role of Risk Management

The insurance and re-insurance businesses are increasingly interested in DLT solutions because of their high potential to transform interactions with partners, customers and regulators.

Despite this promise, DLT and similar other recently developed technologies present new challenges for corporations and for most functions within. The decentralized nature of DLT and its applications leads necessarily to a risk profile that is different from the one that arises from centralized solutions.

The traditional roles of Risk Management become therefore highly valuable also with regards to DLT and DLT based projects. Risk Management must play a key role to permanently challenge DLT related projects throughout the full project lifecycle. This requires involvement of CROs in such initiatives and potentially some knowledge built up within Risk Management itself.

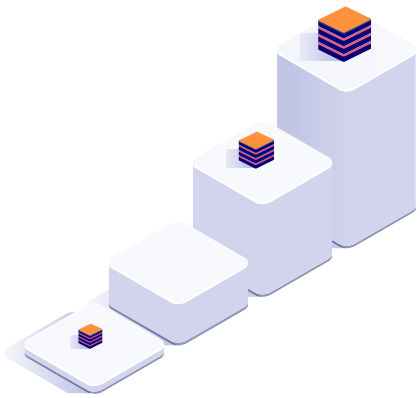
To ensure that such a key role is properly fulfilled, Risk Management should consider, on a broader level, the following questions:

- Are risk managers involved in the overall DLT vision and strategy definition, including DLT project selection and other related processes/ discussions?
- How can the CRO help define and continuously improve the overall strategy around DLT?
- Is Risk Management involved in the choice of the technical solutions, including the integration of DLT and non-DLT architectures? Considering the characteristics of DLT it is not adapted to all use cases.
- Are the technologies understood? Both by risk managers so that they can challenge the use of DLT, as well as by IT and business users who are responsible for conducting DLT projects.
- How can risk managers help business users and IT to reduce DLT-related risks in their projects?
- Is there a business case? Are DLT acceptance and monitoring criteria defined?
- How is appropriate governance ensured around emerging complex technologies such as DLT?
- Are data and algorithm sharing criteria and policies defined?
- How is it ensured that all relevant risks (in connection with new technologies, e.g. DLT) are identified and managed?

The first crucial assessment to be done regarding DLT and DLT based initiatives, though, is evaluation of the necessity and applicability of a DLT approach. Risk Management can provide valuable input to this strategic decision, for instance by means of a framework upon which to base the assessment.

2.1 Applicability of DLT

Before deciding on building or investing in a DLT solution, insurers should make the following key considerations regarding the potential DLT solutions:



	KEY CONSIDERATIONS	KEY QUESTIONS
Applicability compared to other technologies	• DLT is likely to increase the solutions' technical complexity. It might not be necessary if the requirements can be fulfilled without DLT.	• Is DLT necessary? • Could the same problem be solved without DLT? • Are non-DLT solutions possible / available? • Will DLT bring significant benefits compared to non-DLT solutions?
Feasibility considering the DLT network participants' technical capabilities and their willingness to collaborate	• DLT requires data, communication and process standards, if such standards do not exist then the participating companies need to develop one. • DLT as an emerging technology requires specialized technical and business expertise. • Companies must have sufficient IT infrastructure that enables them to participate in DLT networks.	• Do you have the necessary IT infrastructure and technical skills to operate the DLT solution? • Are there common data and communication standards available, accepted by all network participants? Or do the participants need to develop new standards? • Do you have sufficient resources to integrate the DLT solution into your IT landscape?
Profitability including operational expenses, in comparison with non-DLT solutions	• DLT can enable companies to automate cross-company processes and reduce administration / reconciliation costs but increased IT expenses could wipe out savings. • If standards are not available or not widely adopted by the network participants, then developing and integrating standards could have a significant impact on the solution's profitability.	• Do you have a clear business case considering potential IT costs? • Does the business case include a realistic estimate of operational costs after going live? • Did you consider the necessary IT integration and change management costs? • If standards are not available, did you budget the potential effort needed to develop one?

Governance clarifying roles and responsibilities in operating and maintaining the DLT network	• DLT enables decentralized governance but certain centralized roles (i.e. software provider) are still required for efficient coordination. • The responsibilities of the network participants and central providers need to be clearly defined.	• Who is the software provider? What is their responsibility? • Who makes the decisions regarding product roadmaps and release cycles? • Who operates the network? • Are all network participants responsible for operating their own node? Who is responsible for troubleshooting?
Security assessing and mitigating cyber risks	• DLT projects, like any IT solutions, have their specific security risks, requiring mitigation. • DLT nodes can execute smart contracts which were developed and deployed by third parties.	• Does your company have the necessary skills to conduct regular security assessments and penetration testing on the DLT solution? • Do you have the chance to review every software update in a staging environment? • Do you have a clear understanding of the sensitivity of your data and business logic stored on the DLT platform? • Can you verify if the platform is configured properly and your data is only shared with the intended parties? • How are participant identities managed by the DLT platform? Are they stored by the network operator?

2.2 Risk identification and monitoring

Assessments by risk managers should start with an understanding of the technical and business context and the role of the DLT in the process. To have an overview on the context, characteristics and components of the use case need to be considered[12]:

- Insurance sector;
- Line of business;
- Product description;
- Type of operations performed.

Technical characteristics:

- Type of platform;
- Mode of operations;
- Type of consensus protocol and type of smart contract, where applicable;
- Programming language;
- Use of native cryptocurrency or not;
- Cryptographic method.

The choice can be made to use:

- A risk catalogue, i.e. a predetermined risk list, mix of a standard taxonomy-based risk list and a specific DLT risk list (please refer to the Appendix for a sample risk catalogue);
- A mapping between the process and the risk matrix.

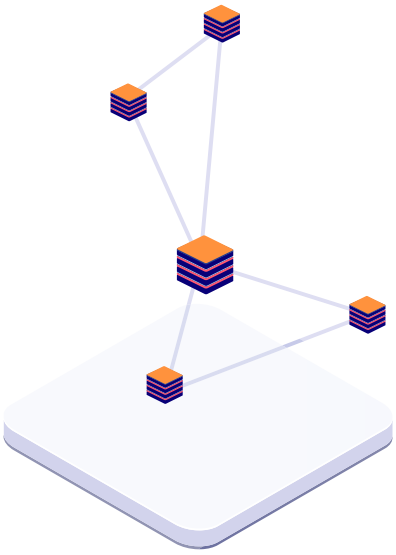
Once a risk assessment has been undertaken, the risk monitoring phase is essential to track risks over time. The risks may change as the technology continues to evolve at a fast pace. As the changes in the risk profile can be faster than those associated with more mature technologies, it is therefore highly recommended for organizations to frequently refresh the risk evaluation and closely monitor risks.

Events that should trigger a new assessment include the following:

- Implementation of new features or an extension of the DLT product to new markets;
- Participants with a significantly different risk profile joining the network;
- Changes in the business process based on DLT;
- Regulatory changes with impacts on DLT;
- Changes in the cost of DLT solutions;
- Major cyber incidents impacting the DLT in use or other events/failures/threats related to a DLT component (e.g. violation of cryptographic systems);
- Increase in the gap of skilled resources;
- Technological evolution (e.g. a new emerging platform).

Due to these changes, the efficiency and effectiveness of the controls mitigating these risks could also evolve rapidly. The status of the controls should also be assessed and reported regularly.

As is the case for other risk areas, key risk indicators should be in place when organizations are exposed to significant DLT risks, in order to gain insight into the effectiveness of the implemented controls and track the overall risk exposure. They can also help drive appropriate risk response activities (please refer to Appendix for selected risk mitigation options).



2.3 How CROs can engage beyond the insurance industry

DLT influences a number of functional domains like IT, operations, product, pricing and distribution that require risk management, controls and auditability. CROs can therefore enable risk-savvy, successful DLT adoption by safeguarding strategy and governance, as well as execution, while informing functional delivery. An in-house capability to strengthen DLT enablers becomes valuable as soon as DLT adopters start engaging and using DLT. In general, however, DLT adoption is likely to develop through additional and potentially overlapping stages that will uncover new specific risk management engagement opportunities beyond the boundaries of insurance undertakings.

While pursuing DLT opportunities, insurance groups and their CROs are likely to come across advocacy opportunities that will enable policy frameworks and regulation, notably to inform standards for:

- Internal policies informing DLT adoption as well as negotiations for the governance and implementation of decentralized insurance networks;
- Adopting DLT specific risk management measures as outlined in the Appendix of this paper;
- Developing smart legal contracts;
- Securing the usage of oracles;
- Managing digital identities;
- Decentral data sharing, maintenance and disclosure;
- Automating the secure processing of transactional data via smart contracts (without reversal);
- Safeguarding contract certainty and confidentiality, cryptographic safety and sound decentral governance;
- Safeguarding regulatory approval and avoiding regulatory arbitrage;
- Automating audit trails and verifications;

12 See also Understanding and managing the IT risk landscape: A practitioner's guide, CRO Forum, 2018.

• Leveraging regulatory sandboxes, confirming and recycling legal and sound DLT codes.

CROs are also likely to work on larger scale adoption of specific DLT products across consumers, DLT manufacturers (the insurer), and DLT ecosystems (all technology partners) by:

• Safeguarding customer-centric transparency with effective risk governance, addressing emerging risks and relevant DLT development trends;

• Proving customer benefits and trusted efficiencies that are equitable, fair, effective and safe, and as needed explaining the extent to which automation might produce trade-offs.

Eventually, DLT users and DLT platform operators might integrate robust insurance use cases with applications across financial and non-financial services. Time horizons for this phase may exceed the next few years and thus be outside of active planning horizons. Nevertheless, to inform and achieve strategic objectives, it is worth capturing a few long-term actions, including:

• Demonstrating the ability to deliver beneficial, fair, transparent, sustainable and trusted DLT benefits;

• Managing collaborative DLT evolutions in robust and predictable governance models;

• Analysing local and global insurance market needs with DLT's decentralized capacity deployment;

• Managing and monitoring performance and transformation capacity;

• Showcasing the sound co-existence of DLT and non-DLT ecosystems with managed risks.

Overall, sound DLT risk management can leverage several enablers:

• Deliver well-defined industry DLT issues and narratives;

• Propose feasible DLT solutions;

• Build strong, trusted DLT and advocacy capability;

• Encourage DLT leadership and champions;

• Inform and mobilize public and customers;

• Establish clear path and resource for implementation;

• Influence, support, shape and inform DLT coalitions.

There are still vast areas to be explored around DLT including, and certainly not limited to, legislative and regulatory gaps. As of today, it is not even possible to discuss DLT and blockchain using a commonly accepted taxonomy. In this respect, a joint effort among risk management, legal, compliance, security, and technology experts (along with business specialists) will help institutions and authorities accelerate the journey towards the productive phase of DLT. The CRO's attention to such points is supportive within regulatory regimes aiming at encouraging impactful innovation, fostering technology neutral choices, and identifying progressive standards for the development and adoption of DLT ecosystems.

Chief Risk Officer (CRO)

• Act as a critical enabler in vision, strategy and project portfolio definition of DLT initiatives;
• Inform internal governance around DLT, including acceptance and monitoring criteria as well as third party management;
• Ascertain the risk profile of DLT initiatives, including risks, opportunities and trade-offs;
• Support the creation of integrated risk management frameworks; among DLT networks participants
• Contribute to wider ecosystems by informing policy, standards and regulation.

3 Risks in using a private DLT. Catastrophe Excess of Loss (CAT XL) re-insurance

USE CASE

B3i's CAT XL[13] solution, apart from CAT modelling and risk pricing, implements the whole underwriting process in smart contracts on DLT. This involves the pre-placement phase where the cedant creates the insurance portfolio to be reinsured, followed by sending the information package to a broker and requesting a price indication. The broker forwards the package to selected reinsurers starting an iterative negotiation process. This includes many conversations between all involved parties and performed via the B3i platform built on R3 Corda technology, and eventually ends in final reinsurance agreements.

Most of the DLT specific risks may arise out of the proper mapping and implementation of the business process on the DLT system. The application steers and stores the whole reinsurance underwriting process. This starts with the cedant uploading relevant data (e.g. a primary insurance portfolio to be reinsured), continues with the intermediary (broker) selecting and approaching the proper reinsurance candidates, and ends with reinsurers providing prices and writing/signing lines of non-proportional layers.

Key technological aspects, useful for understanding the risk profile

B3i's CAT-XL use-case is based on the R3 Corda DLT platform, which has no concept of blocks or chain, but rather handles data as peer-to-peer transactions among participating parties. As a private and permissioned DLT platform, it provides its own centrally steered identity and authorization management on different authorization levels. Further, Corda is not tied to any particular consensus algorithm nor to a specific smart contract language.

Contrary to a classical blockchain implementation, Corda applications do not rely on a public consensus algorithm and are therefore not vulnerable to common blockchain limitations like slow performance or low scalability. Due to its design, Corda is not exposed to a 51% attack either, where parties with the majority of the calculation power can hijack and compromise the single version of the truth. Corda's notary services validate transactions and sign or reject them (e.g. notaries reject transactions with missing signatures). Only the presence of a notary signature indicates transaction finality.

Unlike Ethereum or Bitcoin, Corda is designed to build up a private network amongst a number of peers. Corda can dynamically create sub-networks for

13 Catastrophe excess of loss (CAT XL) reinsurance is made of covers triggered "per event" and over a specific threshold. They include all the individual losses that are attributable to one cause and therefore form an accumulation loss.

each transaction, only accessible by the authorized counterparties specific to that transaction. The technology behind B3i's CAT XL use case can thus be considered as a secure network among counterparties involved in specific transactions.

Risk assessment

We have separated the risks associated with the B3i DLT solution into the following three categories:

- Risks prevalent in all secure IT solutions;
- Risks common to the use of automated systems;
- B3i specific risks arising out of re-building the legacy business process.

Risks prevalent in all secure IT solutions

• Information security risk - Broken cryptographic protection
The development of quantum computing is going ahead and there is a noteworthy probability that in five to ten years a feasible quantum computer exists, which could be able to break today's common cryptographic algorithms. For common symmetric algorithms, quantum computing doubles the length of secure cryptographic keys. This means for future applications that a minimum length of 1024 or 2048 bit should be considered secure. Asymmetric algorithms, which use generally one-way functions based on the factorization of large prime numbers, will not be considered secure anymore, as soon as quantum computing has been developed.
A mitigation of this risk is possible by applying a quantum-proof/safe cryptography (which has until now not been fully developed) or by retaining the option of changing the cryptographic system over time without disrupting the DLT network ("Crypto-Agility").

• Information security risk - Compromised participant devices
This risk arises not directly from the DLT itself, but rather from the participant devices. In B3i terminology, both the "nodes" (servers) and the corresponding clients running the DLT applications could be vulnerable to typical IT security risks such as unauthorized access, virus attack, missed security patches etc., with the consequence that those devices

constitute vulnerabilities for the whole DLT network. Therefore, those devices have to be treated in at least the same way, in terms of IT security measures and controls, as a company's other highly exposed web-facing devices.

• Information security risk - Malicious content in the DLT
A risk could arise from "poisoning" the content of the ledger by bringing malicious content into it, such as infected code snippets which install back doors for other malicious applications and/or provide access to unauthorized users. As a mitigation measure, and to avoid such software vulnerabilities, a regular code review and regular penetration testing applying the most up-to-date techniques is required in order to cope with current vulnerabilities and exploits.

• Compliance risk - Risk of non-compliance with privacy regulation does not apply
It is in the nature of a blockchain that data, once in the blockchain, cannot be deleted anymore. This generally gives rise to a risk of being non-compliant with the European General Data Protection Regulation in terms of the customer´s right to be "forgotten" and right to be "deleted". However, in contrast to traditional blockchain solutions, where "deletion" can only happen by reversing entries, the B3i solution shares data only on a need-to-know basis and only between the involved parties, plus R3 Corda allows the data to be physically removed from the underlying enterprise database systems. As a consequence, there is no increase in risk compared to a traditional storage of information such as in the way of emailing and storing the data in file shares.

• Strategic risk - Technology change in the DLT environment
The whole technology of DLT is still in a development phase and thus cannot be considered mature at this point in time. Therefore, a risk of fundamental changes within this technology exists. In the B3i CAT-XL use case, this applies to the fact that B3i recently switched from the Hyperledger protocol over to R3/ Corda. If this or similar happened when a productive network already existed and real data was being handled, all data would have to be migrated to the new protocol, with resulting risks stemming from data migration (loss of data, loss of integrity, loss of availability, loss of confidentiality).

• Other operational risk - Human resources and personnel-related risk
As with any enterprise system, specific knowledge and experience are required. In particular, setting up and reviewing the data and the smart contract within the DLT environment, as well as maintaining the Corda nodes and certain system settings, require specific knowledge. This knowledge includes IT administration as well as business-related professional knowledge. Currently, only very few people have this very specific know-how. As a consequence, risks may arise from insufficiently qualified in-house personnel as well as from so-called "head monopolies". Mitigating these risks requires suitable staff development measures and management instruments, as well as succession planning.

• Business continuity risk
The B3i application and the Corda network need to be continuously available. Unavailability of any part of the network for any reason could potentially cause financial loss due to the fact that important contractual transactions (e.g. signed lines, written lines, offers) or any written communication cannot be executed. This could potentially happen through internet outage, cloud outage if the B3i application runs in the cloud, outage of a notary service in the Corda network or other internal or external events. However, there may be particular time slots during the year (renewal seasons) where the availability requirements could be higher. At least for those time slots mitigation measures such as redundancy, backups or even parallel processes should be considered.

Risks common to the use of automated systems

• Smart contract and data quality risks
Especially in the beginning phase, when users (client managers, underwriters and brokers) are not fully used to the system, there is an increased risk of data input failure. If contract data is forgotten, wrongly entered or misinterpreted, users may work with the smart contract not fully reflecting the policy terms & conditions, or a wrong premium calculation.
As a standard risk mitigation procedure, a tight four-(or multi-)eyes principle should apply, especially in the early days of any new system. This control would increase the complexity of the business process along with the B3i solution, at least temporarily.
Note that, as with paper contracts, in the event of an error, whether technical or human in nature, mitigation measures are in place by means of contract amendment / endorsement. A further mitigation measure, more effective and in line with the technology, is the introduction of validation rules within the application logic, thus enabling the possibility that potential anomalies or mistakes can be identified automatically.

• Risk of overreliance on technology
With any new technology there is the risk that users over-rely on its failsafe mechanisms and skip certain key checks and balances that were part of the legacy process. Users should keep in mind that, until the technology has solidly proven that checks and balances have become redundant, these checks need to be executed. A partial mitigation measure is the introduction of validation rules within the application logic enabling certain checks to be executed automatically.

• Interoperability risk - Risk due to lack of Corda integration in the customer´s legacy system environment
At the current stage of the B3i use case, supported steps include uploading a primary insurance portfolio over to broker(s), finding reinsurers to negotiate a price, and finally writing a binding line. Before the upload, the portfolio must be defined. This could happen simply via Excel, but also with highly specialized software. Several activities will be, in the initial phase, carried out externally to the DLT infrastructure, such as pricing of an exposure portfolio, balance sheet accounting of the signed reinsurance contract, claims management and administration. All these potential process steps have their own highly specialized software deployed at the insurer and / or reinsurer, and such software needs to interface to the B3i application. Missing standard interfaces generate a risk of a high effort to self-develop integration applications. For standard applications such as SAP, interfaces could be developed in cooperation with software vendors.

• Vendor and service provider risk
Customers may fear the dependency on one single supplier (B3i) for the administration of reinsurance business among different stakeholders. To mitigate the risk of supplier default, an exit strategy (for an unplanned exit) should be defined. Additionally, a plan in case of a regular contract termination (the contract with B3i) should be available. Whilst in the second case the customer/member has enough time to get back its contract data or set it up in its legacy systems, there might be not enough time in the first case. For this reason, a back-up and disaster recovery strategy must be prepared. Apart from supplier default or regular contract termination, the dependency on one single supplier may also to a certain extent influence the negotiation position in terms of functional requirements as well as in roll-out and error correction issues.
The choice to go along with only very few specific platform providers, such as Corda as provider of the underlying network and B3i as software provider, should be considered a strategic long-term decision. It is important for B3i customers to get into a position to participate in important decisions within the governance of both providers.
R3 provides a set of governance guidelines for the Corda Network Foundation[14]. It provides a framework for the Foundation's Board, to steer and govern the Corda Network effectively to realize its potential. The governance guidelines recommend that the users (which in our case is B3i, not B3i customers) vote for a chair in the Corda foundation board. One representative of B3i and two representatives of insurance companies participating in B3i are present at this board.
B3i, at the time of writing this assessment, does not have its own published governance guidelines.

14 Governance Guidelines, Corda Network Foundation, 2019.

B3i specific risks arising out of re-building the legacy business process

• **Risk of shadow administration**
Currently, smart contracts are not yet accepted as legally enforceable instruments. There is no overall maturity in the regulatory frameworks of smart contracts - among different legal environments - to enforce digital signatures. Customers may not trust the use of smart contracts alone, and so build a shadow administration, which is the "old-fashioned" way of underwriting with paper slips and paper contract copies, as well as storing contracts and account data in the customer's systems outside the DLT. Although this will provide legal safety, it counteracts the idea of process simplification and cost reduction.

A short-term mitigation of this risk is currently possible neither through technical nor organizational measures. A customer should be aware of it, make the risk transparent and thus accept it consciously. Looking at the longer term, once DLT and smart contract adoption reach a substantial level, regulators and legislators shall be sensitized to release some of the restrictions and enable new frameworks to support the adoption of smart contracts.

Technical features

DLT Platform – R3 Corda

Corda is a distributed ledger for contracts, tailored for use by financial institutions. Transactions/agreements are only visible to parties with whom the data has been deliberately shared (e.g. contract counterparties), including a definable regulator. In this setting, the regulator could be an authority such as the European Banking Authority or an industry body defining a set of standards to which market participants are required to adhere. Corda has no cryptocurrency, as these parties alone are also the validators of the agreement taking place, with multiple consensus mechanisms potentially being used. Corda aims to provide a global network of distributed ledgers, where transactions serve as authoritative and binding facts to ascribe contractual obligations to counterparties[15]. To this effect the behaviour of the system is designed in code and backed by a legal framework which outlines the obligations of participants. Corda is designed to allow a number of financial transactions, including enabling financial institutions to issue digital fiat currency to counterparties. In turn, these blockchain-based funds can be used for trading and settlement.

B3i Platform

Membership of the B3i business network will provide access to a number of B3i and 3rd party applications for transacting with other members, and services and components that can be consumed to rapidly build new shared applications. The security framework allows for members to use their existing identity management and authentication infrastructure and avoid bleeding individual identity and management of users and roles into the B3i platform or B3i applications. Functional authorisation privileges (the things that a user can do) are managed externally and propagated into the B3i in the signed user identity token. Members manage user privileges using the application function list published for each B3i application.

Interoperability

The B3i business network will operate as a business network on the global Corda Network to facilitate interoperability between other business networks in other industries. Within the B3i network, application interoperability will be DLT native and based on the implementation of an insurance industry data standard.

B3i Network Architecture

The B3i ecosystem forms a permissioned business network that provides foundational services required for the operation of an insurance value chain business network. The network comprises member companies (e.g. brokers, insurance and reinsurance companies), B3i and 3rd parties providing services (e.g. oracles). Each member has their own node on the network on which their Corda instance and chosen shared applications can execute. As the Business Network Operator (BNO), B3i will also operate their own node for shared network services such as the membership service. Participation in the network is only possible once a new member has been issued a certificate by the doorman service and the member has been registered in the membership and network map services as part of the on-boarding process. All nodes, notary and oracle services communicate securely via point-to-point Transport Layer Security (TLS) connections.

15 Corda: An Introduction, R. G. Brown et al., 2016.

4 Risks in using blockchain. Parametric flight delay insurance

USE CASE

The use case analyses a fully automated parametric flight delay insurance product where contracts are partly processed and stored in the public Ethereum blockchain. Claim settlement is automatically triggered upon the occurrence of an event.
Traditional insurance claim settlement is triggered by an actual loss or damage, whereas parametric solutions are triggered by an event occurrence exceeding a pre-defined parametric threshold (for example: an earthquake of minimum magnitude of 7.0 within a defined area). The triggering event is that a flight is late by more than two hours.

In addition to letting the customer query the blockchain to confirm policy existence, the product uses the blockchain to handle insured events through a smart contract. In particular, a parametric smart contract is triggered by an oracle based on FlightStats, an external data source. The transaction validation process relies on the Proof of Work consensus protocol.

The product was developed to help solve some customers' pain points including:

- Eliminate exclusions that are encountered in classical insurance products. Cover against flight delays is provided regardless of the reason: e.g. weather, strikes, mechanical or technical issues;
- Automate compensation with parametric features and blockchain;
- Eliminate the classical claims process which can be cumbersome, involving contacting the airline to provide proof and sending it over to the insurer;
- Increase the immutability and transparency of insurance policies by using the Ethereum blockchain;
- Reinforce insurer/insured trust as it is a non-human third party (the smart contract), unrelated to the insurer and through a public code, that decides whether or not the insured should be compensated.

The functional scope of the product is detailed in three steps:

1. Quote – The user visits the insurer's website or a partner of the insurer (flight companies after buying a flight ticket). He/she enters flight details and then chooses the level of protection needed (for example: €8 premium for €150 compensation in case of a delay of more than 2 hours).

2. Subscribe – After selecting a protection level, the user signs in with personal information (email, password, first and last name and country).

3. Compensate – In case of a flight delay, compensation is automatically triggered. The customer receives a payment on the credit card used for subscription.

Risk assessment

As a consequence of the overall application architecture, the risks specifically stemming from DLT are really few and immaterial. This also means that DLT-related risks, if needed, can be easily mitigated by switching the DLT part of the process onto the insurer's own, non-DLT, systems. Had the insurer fully relied on the blockchain, it would have been exposed to the general DLT risks that will be considered in the following paragraph.

• Consensus protocol and scalability risks
The blockchain-related part of the solution is hypothetically vulnerable to problems arising from the consensus protocol, like slow performance or low scalability, since a consensus protocol (Proof of Work) is used to validate new blocks of data and so determine which state of the database can be considered valid. However, very little information is used in the validation process, thus reducing validation time. To mitigate the impact of this issue further, the insurer has the option to obtain higher performance by paying more for the mining ("fuel for mining").

• Information security - Consensus protocol hijack
Slow performance, with the possible effect of a denial of service, in a DLT architecture can also be the consequence of a cyber-attack, for instance spam transactions.
In particular, due to its design, the product is theoretically exposed to a 51% attack, where a majority of peers or one peer with the vast majority of calculation power hijacks the eventual single version of truth of the blockchain. The Ethereum Classic cryptocurrency (not used in this case) has recently been affected by this kind of attack.
A possible consequence can be the blockage of correct transactions or the validation of undue payments. Off-chain monitoring of due payments, as well as ongoing reporting on the events registered by FlightStats and on the number of transactions per flight, as already implemented, are solutions to promptly identify such cases. A parallel traditional claims process management could be a solution to work around a 51% attack.

• Information security - Broken cryptographic protection
Another DLT vulnerability, which is generally applicable to secure IT solutions, is the breach of the cryptographic protection system, for instance through quantum computing. This risk could become a threat in the near future, considering that IBM has recently announced the first commercial quantum computer "Q system One". The implications of such a data breach can be manifold, ranging from data integrity to data confidentiality issues. A complete mitigation of the risk is currently not possible, since quantum-proof cryptography has not yet been fully developed. In any case the insurer has limited the data privacy breach risk (in the DLT part of the process) by avoiding the storage of client personal data on the public blockchain and keeping on Ethereum only a minimum set of transaction information.

• Information security - Key management and other traditional IT issues
More generally, other traditional IT risks exist, which are not necessarily brought by DLT itself. Examples of IT risks are key management (e.g. key storage, key loss, key theft, key generation) or information transfer (e.g. communication between the oracle Flightstats and the blockchain, or between the blockchain and the insurer's legacy systems). Traditional IT security measures and controls are valid mitigations. Clients are not required to have direct interaction with the blockchain (although they can see their transactions on the blockchain) and therefore key management risk is limited.

• Information security - Malicious content in the DLT
Another typical IT risk is the risk of "poisoning" the ledger by bringing malicious content into it. A possible point of attack would be the smart contract that can be potentially affected by malicious software spread, bugs/errors or a 0-day vulnerability. Recurring code reviews and penetration tests, as already performed by the insurer, reduce this risk. Engaging with white hat hackers and creating bug bounties are additional options to further harden applications.

• Smart contract risks
The smart contract could be also affected by the more general risk of unwanted behaviour of the smart contract itself, due to a programming error in the development phase (rather than fraudulent external attack). This risk is higher in the case of complex algorithms. However, the smart contract used by this product is simple and easy to monitor, update and maintain. In any case, an undue payment or a mistake can be managed by a traditional parallel process, which is still in place.

• Interoperability risks - Technology change in the DLT environment
Apart from the smart contract, since the whole DLT is still in its development phase, there is a risk of fundamental changes within the very technology stack. If that happens, it will require software developments or migration with possible problems related to data in terms of availability, integrity and confidentiality. The product relies on the current main public platform, Ethereum and a recovery plan, consisting of migrating the DLT part of the process to a non-DLT solution that already exists and would not imply material impact on the overall service. Despite this, failure to control change due to ongoing developments and frequent updates is still a possibility.

• Vendor and service provider risks
Another risk arises from the dependency on an external platform (Ethereum) and an IT supplier for the development of the DLT part of the process. Also in this case, the insurer's exit strategy would be changing the platform and technology for this part of the process. This aspect reduces the negotiation power of the outsourcer. The risk of insufficient in-house skills is negligible at the moment and easy to tackle. Vendor risk may also apply to the use of Flightstats.

In conclusion, most of the risks of the product DLT part of the process are traditional IT risks or general DLT risks, due to the lack of technology standards and maturity. However, since the role of the blockchain is limited in the overall product and mitigation controls have been implemented, the residual risk is very low.

Technical features

In this use case, the parametric flight delay insurance uses a widely-distributed blockchain platform called Ethereum that combines a generalized peer-to-peer networking platform with next-generation blockchain architecture to deliver a decentralized, consensus-based, full-stack platform for developing, offering and using distributed application services.

1

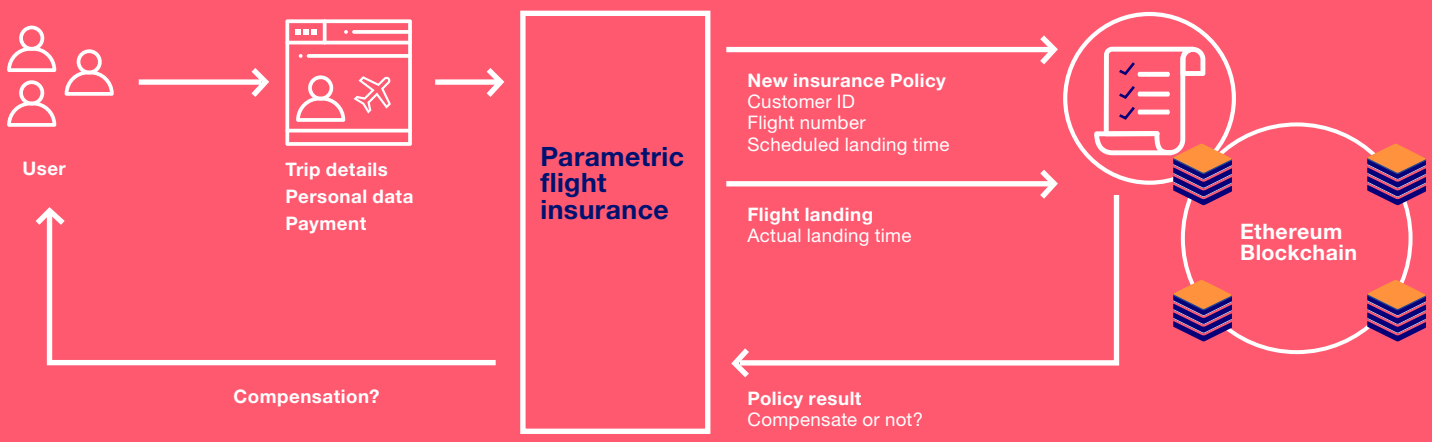
In step 1 the solution uses the insurer's internal pricing system to display a quote for the customer. No blockchain interaction is initiated at this stage; data provided by the client (including personal data) are stored internally. Flight date and destination are also processed internally by a proprietary algorithm that analyses historical data in order to evaluate the risk of delay and calculate premiums for each coverage level.

2

Interaction with the Ethereum blockchain begins in Step 2 after the user chooses a coverage level and pays the insurance policy. The policy is appended to Ethereum thanks to a dedicated smart contract. The customer is notified upon the creation of the transaction in Ethereum: a notification email is sent containing the link of the corresponding transaction. No one except the customer and the insurer can associate the transaction to the insured party, since the transactions do not contain any personally identifiable information.

3

In step 3 after the flight landing, the actual landing time is sent to the smart contract within the Ethereum blockchain. The actual landing time is automatically retrieved using public flight data and the internal system is notified in case a policy applies for compensation. In such cases, the customer receives a payment on the credit card used for subscription.



Conclusions

In the making of this paper, the CRO Forum has reviewed existing DLT insurance and reinsurance solutions to share a risk manager's perspective and forward-looking advice on DLT adoption. To date, no truly mature DLT-based insurance solution has been identified and DLT, although very promising, clearly ought to be classified as an emerging technology. Consequently, not only the potential of, but also the risks related to, DLT continue to evolve. Key paper findings address the early stage of DLT-based solutions. Without standardization, adopters face uncertainty, as well as strategic risks, even when selecting a DLT platform and code base. This evolving situation is reflected in the two use cases analysed in this paper. Flight insurance administrators would be ready to by-pass any major blockchain problems by moving production onto traditional non-DLT systems. B3i, on the other hand, is currently keeping certain strategic participants' assets such as pricing rules outside the DLT. Somehow the insurance industry seems to be waiting for the technology to mature.

A decentralized system, like for example blockchain, must not be considered inevitable; it may rather be considered appropriate where numerous independent parties wish to maintain common data, particularly if there is a concern about a single party managing or 'owning' the data. In many cases, however, it is natural for a central authority (e.g. a government, bank or healthcare provider) to maintain and secure information. While decentralization offers benefits, such as resilience against certain forms of cyberattacks, there are other technical solutions that offer the same benefits without the use of DLT.

As for risks, the analysis of the two use cases indicates that many of the challenges of adopting DLT solutions are pretty much like the ones linked to the adoption of traditional IT (e.g. security, continuity, scalability, privacy). Smart contracts, on the other hand, create valuable opportunities, but current applications are still relatively simple. Smart contracts' logic needs to be validated thoroughly and, when oracles are used, data availability and integrity can be critical. Since nearly every DLT and blockchain platform is in active development, interoperability can be a challenge both among DLT applications and between DLT and legacy systems. Specifically for blockchain, scalability and performance are still considered relevant issues.

Based on the currently available use cases in insurance, there seems to be a trade-off between using more features of the emerging technology and limiting risk. At the same time, although the potential of DLT is high, traditional insurance solutions and processes might need to be transformed to fully exploit the new technology and its benefits, for example in terms of process efficiency.

Ultimately, DLT lies in a line of technology developments that will require the focus and understanding of the entire C-suite, as business models and markets evolve. CROs and financial executives should continue to periodically evaluate both the latest DLT developments and how those developments could directly impact their business and financial objectives. Senior decision-makers should also continue to evaluate their growth investment opportunities as technology continues to drive the risk of business disruption ever higher. Firms may wish to evaluate strategic DLT partnership opportunities - either within their own industries or with DLT thought leaders like technology companies, specialized consortia and startups[16].

It may also be possible to draw some conclusions on how to perform a risk assessment on a DLT-based application. First, a thorough understanding of the technology and its place in the insurance process is a prerequisite for any meaningful evaluation. Some of the necessary questions to be answered before starting the analysis should focus on which part of the process DLT is used for, which DLT components have been used and the possibility to replace any technical components with more mature, and therefore safer, ones.

When dealing with evolving technology, involving new solutions and/or regulations, risk management activities must be agile and assessments must be refreshed often. This ensures that insurers keep track of the latest technical developments and potential vulnerabilities. To cover all kinds of risks and ensure that a solution provides the expected benefits in a timely manner, it is key not only to involve risk managers at a very early stage in projects, but also to keep them involved throughout the development and maintenance phases. In such a dynamic environment, CROs are well positioned to play a critical role and strengthen innovation initiatives.

16 Blockchain and the decentralization revolution, JP Morgan, 2018.

Appendix
Risk catalogue and good practices

The following catalogue introduces risks and respective possible mitigations.
The catalogue has been prepared based on CROF internal workshops as well as by reviewing literature[17], but is not fully exhaustive and may not account for all possible use cases or adopters' circumstances. Furthermore, for the sake of simplicity, risks are not further categorized to distinguish between DLT and blockchain applicability, unless otherwise specified.

GOVERNANCE & STRATEGY

Strategic Risk

Risk description

(1) Firms need to evaluate whether they want to be at the leading edge of adoption or wait to adopt until the technology matures. Each of these options has varying levels of risk.

(2) Given the peer-to-peer nature of DLT technology, it is important for entities to determine the right network to participate in, as their business strategy could be impacted by the different entities participating in the chain. For instance, "the idea of sharing data as part of a distributed ledger could hinder participation of entities that might worry about competitive implications" (see JP Morgan, Blockchain and the decentralization revolution, 2018).

(3) The choice of the underlying platform could lead to limitations in the services or products that can be delivered via this platform; projects can fail due to a wrong platform choice.

Good practices and mitigation

(A) Evaluate whether your organization will position itself as an early adopter or wait until the technology matures.

(B) Assess your need for a DLT/blockchain by involving enough stakeholders and experts (e.g. security, privacy, technology/business architecture, risk management).

(C) Monitor market for different DLT/blockchain solutions.

17 Distributed Ledger Technology & Cybersecurity, Enisa, 2016.

Governance Risk

Risk description

(1) Governance needs careful attention as DLT thrives on collaboration, meaning thought is needed when deciding on how to accommodate operational developments or when responding to legal changes. Decentralized ownership can cause unresolved disputes among parties and means that no one person is in charge of distributed ledgers; there is no central authority to take responsibility or resolve disputes between participants (e.g. defects and corrupted messages).

(2) Decentralized ownership can also cause failures to create, maintain, implement and execute efficient controls in a distributed environment.

(3) Blockchain relies on a consensus algorithm that needs to be specified and configured or implemented before go-live. The algorithm might change or evolve over time, but depending on the platform, changes might require significant investment from the participants.

Good practices and mitigation

(A) Select a managing entity qualified to manage the network and exercise appropriate oversight consistent with project expectations. In particular, there is 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.

(B) Define service-level agreements (SLAs) between participating nodes and the administrator of the network, in addition to SLAs with service providers that will need to be monitored for compliance.

(C) More generally, integrate DLT/blockchain as well as emerging risks in your risk management practices and update existing policies and procedures to reflect changes introduced by DLT/blockchain in business processes.

COMPLIANCE

Compliance Risk

Risk description

(1) Distributed ledgers have no specific location: this creates a problem in terms of jurisdiction and applicable law, as each network node/computer could be subject to different legal requirements.

(2) Furthermore, regulators across the world are taking different approaches to how they regulate DLT, meaning it will be difficult to determine whom you answer to and how they will supervise the system going forward.
The result could be non-compliance with anti-money laundering and anti-fraud regulations or financial regulations (e.g. Crypto-currencies can be illegal in some jurisdictions).

Good practices and mitigation

(A) Pay attention to all relevant legal issues in the design phase. This includes setting standards in code or pure executions, methods for dealing with issues that cannot be captured in code, specific legal requirements, and more general legal questions (liability, applicable law, jurisdiction, general principles, dispute resolution, privacy and digital identity).

(B) Monitor regulatory developments and evolutions in market standards.

(C) Reviewing broader regulatory requirements and standards, including both industry-specific and generally applicable rules.

Compliance Risks – Focus on Privacy

Risk description

Data is accessible to everyone in a public, permissionless blockchain: the effect of this can be non-compliance with Privacy Regulations such as the European General Data Protection Regulation, in particular with some of the following key issues:

(1) Right to Erasure. One key feature of blockchain is that information cannot be removed from the ledger, being part of an immutable record. However, if there is personal data on the ledger, individuals may have the right to have their data 'erased'. It is hard to reconcile these two principles.

(2) Re-identification and Singling-Out. When the public key is visible, it could be possible to attain information that enables an individual to be identified. At that point, all transactions that the relevant individual has made are publicly available and the individual can be re-identified. The cost and amount of time required for re-identification, the available technology at the time of processing and technological developments should be taken into account.

Good practices and mitigation

(A) Dealing with privacy, in general it is important to identify data that will remain outside public DLT/blockchains: there will be some data that cannot be uploaded to a public DLT (such as personally identifiable information or medical records). One solution that has been proposed for privacy issues is "Hawk", in which users can hide the details of their transactions but still convince the rest of the network that the transactions are valid. While useful, Hawk is specific to Ethereum and makes use of fairly advanced cryptography.

(B) Dealing with the use of public keys, some newer DLTs permit the public key not to be published.

Compliance Risks Focus on Intellectual Property Rights (IPR)

Risk description

(1) DLT solutions in the insurance sector will require navigation of a complicated landscape for intellectual property rights (IPR). For example, 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.

Also 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 can all be protected by copyright. Smart contracts may be copyright protected too.

Good practices and mitigation

(A) Avoiding, if possible, data subject to copyright.

IT & OPERATIONS

Information Security and Business Continuity risks

Risk description

(1) Failure to protect against and detect cyber-attacks. The best known attack in public, permissionless blockchains is the 51% attack; it consists of controlling the majority of the computing power on the network (applicable only to public blockchains) and can enable the attacker to alter the blockchain.
Another issue can be network overload due to a distributed denial of service attack: spam transactions can be massively introduced for validation.
Furthermore, one possible issue is the broken cryptographic protection.

(2) Key Management. Loss of assets associated with private keys due to a failure in key management and protection.

(3) Compromised participant devices. An attack on a single participant could affect the integrity of the entire blockchain.

(4) Malicious content in the DLT. “Poisoned” content of the ledger due to malicious code, such as infected code snippets that install back doors for other malicious applications and/or provide access to unauthorized users.

(5) Business Continuity. Blockchain technologies are generally resilient due to the redundancy resulting from the distributed nature of the technology. However, business processes built on blockchains may be vulnerable to technology and operational failures as well as cyberattacks. Unavailability of any part of the network for any reason could potentially cause financial loss due to the fact that important contractual transactions (e.g. signed lines, written lines, offers) cannot be executed.

Good practices and mitigation

(A) In general, conduct extensive penetration tests on the blockchain application.

(B) Dealing with business continuity, define a robust business continuity plan and governance framework to mitigate such risks. Additionally, blockchain solutions shorten the duration of many business cross-strategy processes, and business continuity plans should account for a shorter incident response and recovery time.

(C) Designing the system with the requirement to change the cryptographic system in production systems over time without impacting the DLT network (“Crypto-Agility”).

Interoperability risks

Risk description

Many blockchain platforms are still under development, with incomplete features in active development. This can bring risks in terms of interoperability:

(1) Within DLT. Lack of implementation standards specific to blockchain can cause unstable and difficult-to-maintain IT solutions. This can also bring lock-in or service interruption due to lack of interoperability between blockchain protocols: exchanging data will require translation of formats and protocols which is currently in a very early stage.

(2) Between applications built on the same DLT. Risk of creating countless new silo-ed solutions based on different standards and with significant reconciliation challenges.

(3) Between DLT and legacy systems.

Possible consequences can be also:
(4) Failure to control change due to ongoing developments and frequent updates.

(5) Risk of shadow administration in order to react to the lack of interoperability.

Good practices and mitigation

(A) Select widely used DLT/blockchain platforms to maximize resilience and select, when possible, DLT/blockchain platforms that support popular programming languages such as Java.

Consensus protocol and scalability risks

Risk description

(1) Mining and fuelling costs. Cost inflation due to excessive computational power and energy consumption: some consensus protocols used by public blockchains require significant computational power to verify and confirm each block.

(2) Slow performance due to complex consensus algorithms: The network must reach consensus to add each transaction, and the number of validated transactions per second is limited. The consequence is that processing time could increase due to scalability issues: with every transaction and user that joins the network, the blockchain history grows constantly and can become a bottleneck.

Good practices and mitigation

Possible solutions/trade-offs to partially mitigate the risk, depending on the specific purposes of the use case, include:

(A) Store only the headers of blocks on the blockchain, rather than their full content (useful also for Privacy issues).

(B) Build a “Lightning network” solution: a recent and increasingly active line of research that allows two parties to open a payment channel. Using such a channel, a single pair of transactions can be placed in the ledger—that, respectively, serve to open and close the channel—but many individual payments can take place.

(C) Shard the ledger. If implemented in a certain way, participants do not need to store (or even hear about) transactions that are irrelevant to them: each participant sees transactions only within a given shard (e.g., in Corda, participants need to achieve consensus only on transactions that are directly relevant to them, and in Certificate Transparency there is similarly no global consensus on ledger content). However, these solutions raise questions about verifiability of fully decentralized solutions.

(D) More generally, after selecting a specific platform, set up close monitoring of the consensus model.

Smart contract risks

Risk description

Smart contracts can be affected not only by classical IT external risks (such as cyber-attacks), but also internal risks. Here are some examples:

(1) Contract enforcement and validity: Currently there is no legal precedent around the enforcement of a smart contract in lieu of a physical contract.

(2) Bugs. Algorithms can contain bugs, caused by human error in programming.

(3) Unwanted behaviour. Contracts may not always perform as the parties had intended because of complexity. For example, contracts may be difficult to develop and implement where the situation calls for:
- Reversibility of transactions;
- Subjective analysis (how much flood damage was there on the second floor of building?);
- The programming of excessively complex or nebulous principles into smart contract code (e.g. interpretational standards, such as “reasonableness”);
- Extensive interaction between a blockchain and the outside world (i.e. data input from outside the ledger or an impact on the outside world by events on a ledger).

Good practices and mitigation

(A) In general, define robust incident management processes to identify and respond to glitches in smart contract operations.

(B) Smart contracts may require new types of due diligence by lawyers to provide comfort that the code is enforceable and embodies intended provisions.

Oracles risks

Risk description

(1) Oracles can be a point of failure in DLT architecture. The problems can be both in oracle data quality and in failures during communication with the blockchain (e.g. messages transmitted over the internet can be delayed or interrupted, and data can be corrupted in transit).

Good practices and mitigation

(A) The outside actor must be a trusted third party and must preserve the integrity of the smart contract by transmitting accurate and trustworthy data in a secure manner.

Vendor and service provider risks

Risk description

(1) The technology might be sourced from external vendors and hence organizations may be exposed to third-party risks (due to lack of adequate IT Skills for example).

Good practices and mitigation

(A) Using different vendors (if possible) is a defence against vendor lock-in.

(B) Applying a vendor risk management framework including information security, operational resilience and data privacy risk assessments.

Other Operational risks

Risk description

(1) Poor Data Quality. DLT validates data through consensus protocols, but if a protocol does not appropriately address data quality it might lead to a massive integration of poor quality data. The problem can be related both to internal and external poor data quality and lack of data standards.

(2) Human resources issues. Inadequate IT skills to manage blockchain technology or lack of skills on the market.

Good practices and mitigation

(A) Ensure that the data validation rules in place match business requirements: generally, DLT/ blockchain solutions provide consistency checks over data. Ensure the entity applies additional validation rules to ensure the accuracy of the data coming in.

(B) Establish a baseline of skills and capabilities that are in line with DLT/blockchain strategy.

(C) Leverage internal teams through dedicated awareness/training sessions.

(D) Partner with specialized vendors when needed.

FINANCIAL RISKS AND OTHER RISKS APPLICABLE ONLY IN CASE OF USE OF CRYPTOCURRENCY

Volatility risks

Risk description

(1) For crypto-currency applications on blockchain (e.g. Bitcoin): volatility risk due to the lack of maturity of both the market and blockchain technology.

Good practices and mitigation

(A) Traditional mitigation of volatility risks.

Liquidity risks

Risk description

(1) The adoption of DLT, such as the blockchain, may introduce new liquidity risks. In current business models, intermediaries typically take on the counterparty risks and help resolve disputes.

Good practices and mitigation

(A) Dispute resolution in a distributed trust environment is a requirement to tackle by design through preordained liquidity arrangements.

Wallet[18] risks

Risk description

(1) While blockchain technology provides transaction security, it does not provide account/wallet security. The distributed database and the cryptographically sealed ledger prevent any corruption of data. However, value stored in any accounts is still susceptible to account takeover (see information security risks).

Good practices and mitigation

(A) Make sure the software for the wallet does not leave the key accessible in plain text outside the application.

(B) Require the implementation of recovery keys.

18 According to bitcoin.org, wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet.

Acknowledgement

The CRO Forum would like to acknowledge with much appreciation the collaboration with B3i, The Blockchain Insurance Industry Initiative. B3i was formed in late 2016 as a collaboration of insurers and reinsurers to explore the potential of using Distributed Ledger Technology within the industry for the benefit of all stakeholders in the value chain. The incorporation of B3i Services AG was completed in March 2018 in Zurich.

Consultation sources

Blockchain and the decentralization revolution, JP Morgan, 2018

Blockchain/DLT in the Insurance Sector, Hogan Lovells, 2017

Blockchain risk management, Deloitte, 2017

Blockchain's Occam problem, McKinsey & Company, 2019

Corda: An Introduction, R. G. Brown et al., 2016

Cryptocurrency Deals Can Always Be Erased for a Price, Bloomberg, 2019

Distributed Ledger Technology & Cybersecurity, Enisa, 2016

European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains, 2018

Governance Guidelines, Corda Network Foundation, 2019

Hi-Tech Crime Trends 2018, Group IB, 2018

Insight report on distributed ledger technologies, Lloyd's Register Foundation, 2017

Machine Decisions: Governance of AI and Big Data Analytics, CRO Forum, 2019

The Myth of Easy Interoperability, R3 Reports, 2017

Once hailed as unhackable blockchains are now getting hacked, MIT Technology Review, 2019

Securing the chain, KPMG, 2017

Smart Contracts: 12 Use Cases for Business & Beyond, Chamber of digital commerce, 2016

Smart contracts as a specific application of blockchain technology, Dutch Blockchain Coalition, 2016

Top Ten Obstacles Along Distributed Ledgers' Path to Adoption, R3 Reports, 2018

Understanding and managing the IT risk landscape: A practitioner's guide, CRO Forum, 2018

The 4 Phases of the Gartner Blockchain Spectrum, Gartner, 2019

5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, Gartner, 2018

Disclaimer

The CRO Forum is supported by a Secretariat that is run by KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org