Institute
and Faculty
of Actuaries

Understanding blockchain for insurance use cases

A practical guide for the insurance industry

by D. Popovic, C. Avis, M. Byrne, C. Cheung, M. Donovan, Y. Flynn, C. Fothergill, Z. Hosseinzadeh, Z. Lim*, J. Shah

Presented at the Sessional Meeting of
the Institute and Faculty of Actuaries [Staple Inn]

03 February 2020

Understanding blockchain for insurance use cases

Authors

D. Popovic, C. Avis, M. Byrne, C. Cheung, M. Donovan, Y. Flynn, C. Fothergill, Z. Hosseinzadeh, Z. Lim*, J. Shah

Abstract

Insurance industry practitioners have deep knowledge of their industry but there is a lack of a simple-to-understand, practical blueprint on applying distributed ledger technology (DLT) solutions, including blockchain. This paper provides a practical guide for actuaries, risk professionals, insurance companies and their Boards on blockchain, including an education piece to provide an understanding of the technology. Examples of real-world applications and use cases in insurance are provided to illustrate the capability of the technology. The current risks and challenges in adopting the technology are also considered. Finally, a checklist of issues to consider in adopting a blockchain solution for insurance business problems is provided.

Keywords

Blockchain; Distributed ledger technology; InsurTech; Insurance blockchain use cases; Risk management; ERM framework

Correspondence details

Z. Lim, 8 Canada Square, Canary Wharf, London E14 5HQ. E-mail: zhixin.lim@hsbc.com

Table of Contents

1 Executive summary

The Risk Management in a Digital World Working Party undertook an industry survey in December 2017 to better understand the views and activity in relation to InsurTech, along with the practice and capability in assessing risks emerging from InsurTech. Out of a number of "hot topics" in the context of digital innovation in the insurance industry, blockchain was identified as a subject matter that respondents were least comfortable explaining to a colleague. This highlighted a lack of understanding of blockchain, and the associated opportunities and risks.

The objective of this paper is to provide a practical guide to blockchain in the context of solving insurance business problems. The paper is divided into three broad sections. Firstly, the paper covers an education piece to provide an understanding of the technology and what sets it apart from existing solutions.

This is followed by examples of real-world applications and use cases in the insurance industry to illustrate the capability of the technology. The working party has also considered the risks and challenges of adopting the relatively new technology.

Finally, the working party has used its "*Guide for Risk Considerations During the Innovation Journey*"[1] in order to create a checklist of issues to consider in adopting a blockchain solution for insurance business problems. The checklist represents a suite of issues to consider at each stage of the adoption journey, phrased as questions. These are mapped to components of a typical enterprise risk management (ERM) framework.

2 Introduction to blockchain

Interest in blockchain has risen and then waned as it failed to gain mass adoption. However, the intellectual capital, and collective energy invested in the development of blockchain means that a tipping point is inevitable. This is the so-called Amara's law[2] which states that "*we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run*". As has the internet done for the exchange of information, blockchain is an infrastructure technology that will enable a peer-to-peer instantaneous exchange of value. Once mature and adopted en masse, it has the potential to be disruptive to the insurance industry's existing business and operating models. For example, the pooling/aggregating and transferring of risk could be achieved between end users (individuals, communities, corporations etc.) without (re)insurance/broker companies acting as intermediaries.

2.1 What is blockchain?

There is no single definition of blockchain; any attempt at a definition often spirals into semantic disputes. For the purpose of this paper, the working party uses the following definition to set a baseline and common understanding.

> *Blockchain, a variant of Distributed Ledger Technology (DLT), is a shared database/ledger on which the state (i.e. the current snapshot of data) is confirmed and verified without the need for a trusted centralised authority.*

[1] Bruce, *et al.* (2019)
[2] Amara (2006)

At its most basic level, blockchain is a database which is shared by multiple participants. Data is verified by multiple entities instead of a single organisation. The data is then propagated and stored by each participant.

The focus of this paper is less on the technical definition of blockchain and more on how it could be useful in solving insurance business problems. This paper uses the terms “blockchain”, “distributed ledger technology (DLT)”, “database”, and “ledger” interchangeably as umbrella terms. The working party also recognises that blockchain is a variant of DLT, and that there are technical differences in various DLT platforms.

2.2 How is blockchain different?

The defining features of blockchain/DLT that set it apart from existing technologies are:

- It provides a single source of truth – this enables the exchange of value digitally without the need for a central authority, who often acts as an intermediary. An intermediary typically extracts value from transactions to the detriment of the end users;
- Smart contracts deployed on a blockchain can automate business logic – this has the potential to reduce operational frictions and costs, and hence improve business process efficiencies.

2.2.1 Single source of truth

Blockchain-based solutions could serve as the single source of truth as they have the following characteristics:

- Distributed – verified data is propagated to participants on the blockchain network so that multiple parties have the same record. This solves the problem of data existing in silos and removes the need for reconciliation between multiple parties;
- Decentralised – in addition to data being propagated to and stored by multiple participants, the maintenance of the network, including data verification, does not depend on a centralised authority. This removes a central point of failure;
- Tamper-resistant – verified data is cryptographically secured, making it resistant to malicious alterations. This provides a high degree of data integrity and immutability;
- Transparent – the blockchain is fully auditable for those with access.

Conventional, tried-and-true database solutions may have some of these characteristics; what sets blockchain apart is that it is designed from the ground-up with all of these characteristics in mind.

2.2.2 Smart contracts

Smart contract is an umbrella term for self-executing code deployed on the blockchain, analogous to software that runs on a computing platform. When pre-defined criteria are met, smart contracts execute a set of business logic as agreed by participants involved. While they may not be “contracts” in a legal sense, they could be utilised to implement the automatic execution of a legal contract or agreement.

Self-executing code is not new; smart contracts are innovative in that they act on dependable data within the blockchain (on-chain data). Where data is not available on the blockchain, off-chain data

from external sources known as “oracles” (e.g. market data provider for financial contracts, weather data provider for weather-related insured events etc.) could be used to trigger the pre-defined action(s).

Smart contracts are important as they extend the functionality of blockchain as a shared database to that of a platform for building a wide array of applications (see examples of insurance use cases in Section 3.1).

2.3 How does it work? A non-technical overview

Blockchain is a convergence of multiple disciplines, including programming, information security, cryptography, distributed systems, peer-to-peer networks etc. To fully grasp its inner workings, one needs a fundamental understanding of these subject matters, which is beyond the scope of this paper.

Instead, the paper provides a high-level overview by focusing on:

- the trade-offs in blockchain design choices – this section provides an overview of the design considerations when choosing the most suitable blockchain solution for a given use case;
- the key components of blockchain/DLT technology – this section introduces the components of blockchain. A basic knowledge of these is useful in developing blockchain applications. However, like web application developments, an extensive knowledge of the underlying protocols is not required.

Readers are referred to Nakamoto (2008), Buterin (2013), Hearn & Brown (2019), Amsden, *et al.* (2019) for further reading.

2.3.1 Trade-offs in design choices

There are two broad classifications of blockchains as shown in Table 1.

	Access	**Examples of platform**
Permissionless blockchain	Anyone can participate in, maintain, and secure the network.	Ethereum
Permissioned blockchain	Only authorised entities can participate in the network with various degrees of read-write-validate access.	Corda, Hyperledger Fabric, Libra

Table 1: Broad classifications of blockchains

The differences are born out of design choices and trade-offs that favour certain features over another. This, in turn, may give one platform an edge over another in specific use cases.

The key trade-off between permissionless and permissioned blockchain is that of access vs. privacy. Permissionless blockchains provide frictionless access i.e. anyone can participate in the network as opposed to the need to set up governance around the rules of participation in a permissioned blockchain. More importantly, anyone can develop applications (via smart contracts) on

permissionless blockchains, potentially increasing the pace of innovation. However, transactions or changes to the database are transparent to all participants; this may not be acceptable in business use cases which require confidentiality.

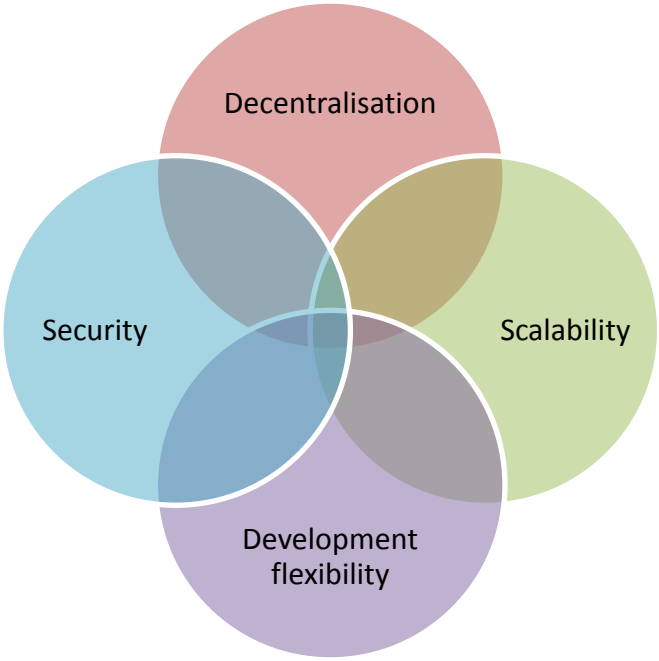

Figure 1: Examples of design trade-offs

Other important (but non-exhaustive) design trade-offs, as shown in Figure 1, include:

- Decentralisation vs. scalability/speed – To maximise the benefits of decentralisation (i.e. where the ownership and maintenance of the network, including data verification, does not depend on a trusted centralised authority), scalability/speed of the network needs to be sacrificed in favour of a robust decentralised consensus mechanism;
- Scalability/speed vs. security – To maximise throughput (i.e. the number and speed of transactions), certain design sacrifices need to be made to the rules that determine how data is verified and added to the shared database, potentially introducing vulnerabilities;
- Development flexibility vs. security – To maximise the flexibility in developing applications, restrictions on smart contracts may need to be minimised, potentially allowing malicious actors to exploit software bugs in smart contracts.

2.3.2 Components of blockchain

Components of blockchain are not new; the main innovation is in the mixing and aggregation of existing technologies such as cryptographic hash functions, digital signature, Merkle tree (or its variants) data structure, and consensus mechanism in a distributed system. These components are described further below.

2.3.2.1 Cryptographic hash function

Cryptographic hash functions are used extensively throughout a blockchain system to secure and authenticate data. A cryptographic hash function is a "*mathematical algorithm that maps data of*

arbitrary size (often called the "message") to a bit string of a fixed size (i.e. the "hash" or "digest") and is a one-way function, that is, a function which is practically infeasible to invert"[3].

A small change to the input, as shown in Figure 2, would change the hash/digest that the new hash appears uncorrelated with the old hash. The only way to find the input that produces a given hash is to attempt a brute-force search of possible inputs to see if they produce a match.

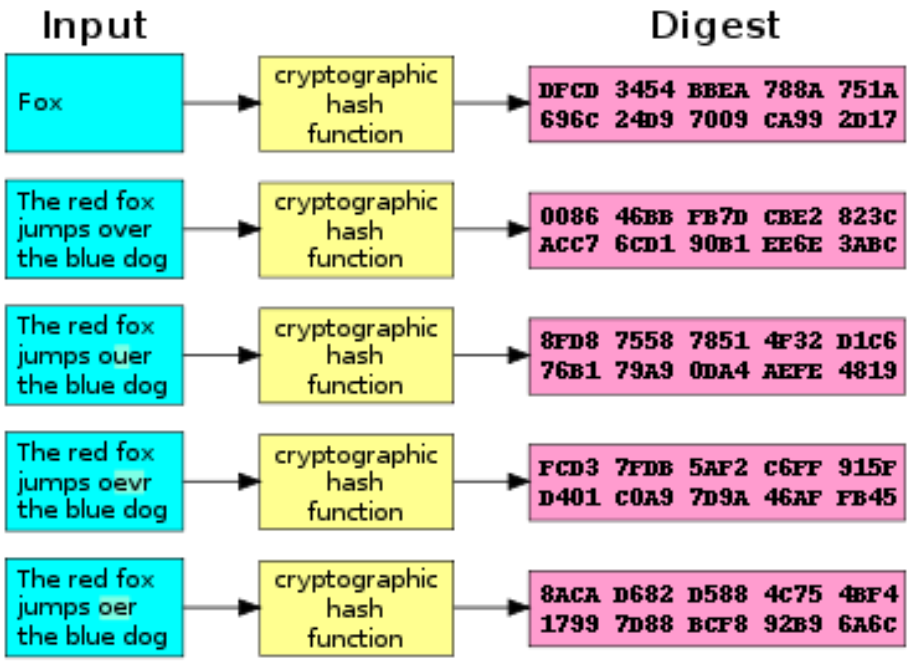

Figure 2: A cryptographic hash function (i.e. SHA-1) at work (Wikipedia, n.d.)

2.3.2.2 Digital signature

Digital signature, which serves as a unique fingerprint, provides the assurance that the proposal to change the state (i.e. the current snapshot of the data) of the blockchain originates from a network node that is authorised to do so. This is achieved using asymmetric cryptography, where a pair of "keys" – one public, and the other private – could be used to encrypt and decrypt data as shown in Figure 3.

[3] Wikipedia, n.d.

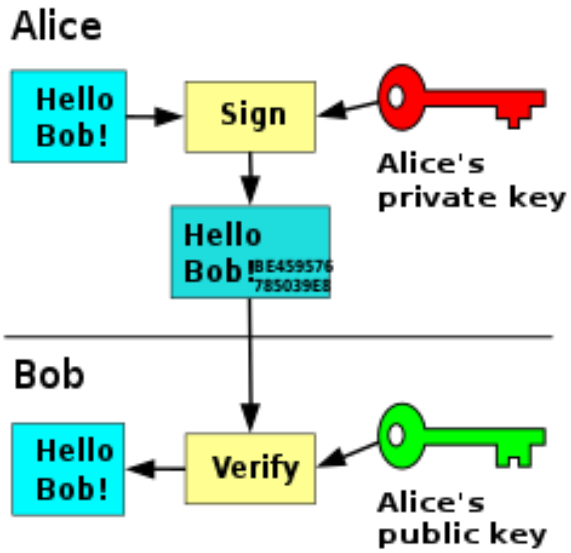

Figure 3: Example of digital signature in the context of signing a message from Alice to Bob, and used to verify the message (Wikipedia, n.d.)

An overview of how this works is as follows:

- The proposal is "signed" with the node's private key using a digital signature algorithm. The private key is known only to the node;
- The signed proposal can be verified to have originated from the node by using the node's public key and digital signature algorithm;
- A digital signature is unique to each state change request thereby adding extra security (i.e. the same signature cannot be re-used).

2.3.2.3 Merkle tree-type data structure

Merkle trees allow for efficient verification of data integrity. A Merkle tree is a tree of hashes constructed from the bottom up as shown in Figure 4. Each leaf node[4] is a hash of data (e.g. transactions), and each non-leaf node is a hash of its child nodes, culminating in the top node (i.e. the root hash or the Merkle root).

Such a data structure optimises the storage and verification of data in a blockchain. Data storage is optimised because only the hashes need to be saved and the root hash is the fingerprint of the entire data set. Data verification is optimised because only a small part of the tree needs to be traversed in order to check where changes have occurred.

[4] "Nodes", when used in the context of a Merkle tree, refer to hashes. This is not to be confused with a "node" in the blockchain network i.e. a participant in the network

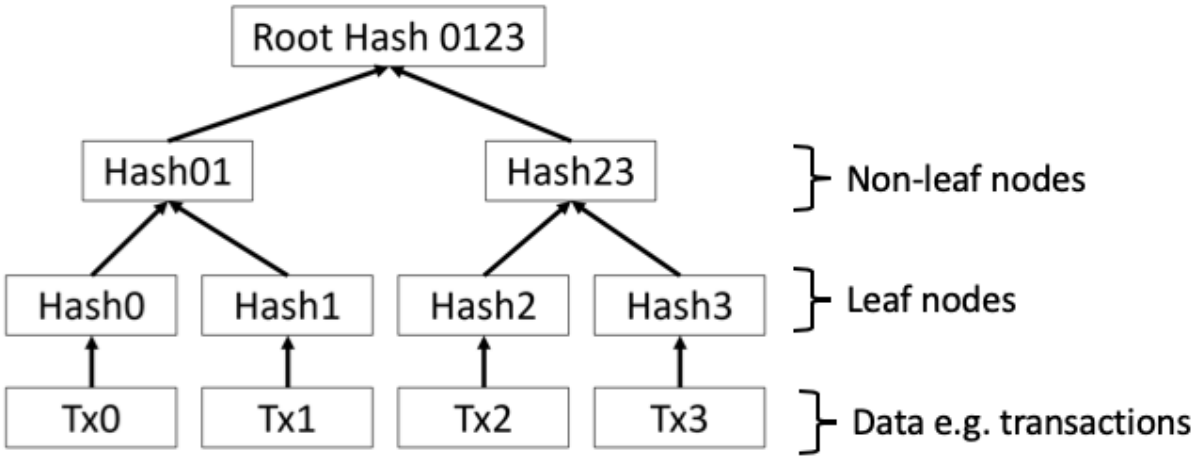

Figure 4: Transactions hashed in a Merkle Tree (Nakamoto, 2008)

The root hash/Merkle root, the fingerprint of the entire data set, forms part of the block header on the blockchain. Another component of the same block header is the hash of the previous block. This unique data structure, where blocks are chained together as shown in Figure 5, is a distinctive feature of blockchain that makes it tamper-resistant. This is because a data change would cause the block hash to change, making it incompatible with the block header in the next block. Therefore, an adversary who wishes to change the state of a particular block would need to change all subsequent blocks. In a proof-of-work (PoW) consensus mechanism (see Section 2.3.2.4), this would require more than half the computing power of the whole blockchain network (known as the 51% attack).

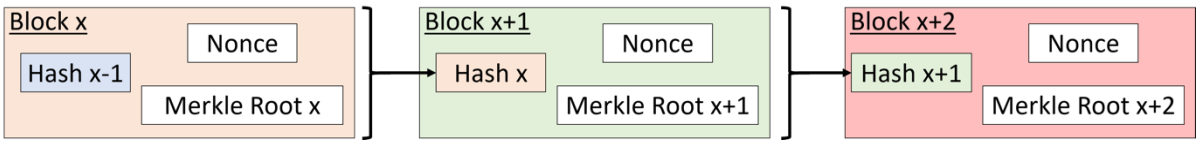

Figure 5: Previous states are linked to the current state (Nakamoto, 2008)

2.3.2.4 Consensus mechanism

The consensus mechanism is a set of rules that determine how data is verified, how conflicting information is resolved, and how agreement is reached on committing changes to the blockchain without a trusted centralised authority.

By utilising cryptography and behavioural economics, the mechanism ensures that participants are strongly incentivised to maintain and secure the network. Examples of consensus mechanism are summarised in Table 2:

Consensus mechanism	High-level method	Typical blockchain type	Incentive	Key pros and cons
Proof-of-Work (PoW)	Requires solving cryptographic puzzle by brute computational force for a state change to be	Permissionless	"Miners" who provide computational power are rewarded and paid transaction fees (in the form	• Pros: Has the longest history in production use (i.e. it has been used in real-world adversarial

	committed to the blockchain		of the digital currency/token native to the blockchain) on successful commitment of state changes to the blockchain	conditions); vulnerabilities are relatively well-known and could be mitigated against • Cons: Significant electricity usage/wastage
Proof-of-Stake (PoS)	Unlike PoW where miners compete to commit state changes to the blockchain, PoS selects from a pool of validators who hold a certain amount of the digital currency/token native to the blockchain (i.e. the stake)	Permissionless	The validator who is selected is rewarded on successful commitment of state changes to the blockchain but risk losing a portion of their stake otherwise	• Pros: Significantly less electricity usage • Cons: It is at a proof-of-concept (PoC) stage and has not been rigorously tested in real-world conditions
Proof-of-Authority (PoA)	Trusted entities vote on whether to commit the state changes to the blockchain	Permissioned	The governance set up for the permissioned blockchain would agree on the penalty to be imposed on non-performing entities	• Pros: High throughput and low latency (i.e. high number and speed of transactions) • Cons: Effective only in a closed, permissioned blockchain.

Table 2: Examples of consensus mechanism

3 Insurance use cases

Compelling use cases in the insurance industry arise when there is a need to:

- Remove intermediaries in the process of value transfer/exchange;
- Produce a shared tamper-resistant record that is trusted by multiple participants and all stakeholders;
- Reduce operational frictions and costs in the value chain.

Figure 6 summarises examples of real-world[5] use cases. The potential application of blockchain technology is evident throughout the insurance value chain i.e. from the underwriting and pricing of products, their sales and distribution, through to the ongoing management of product, and claims processing. The examples below are not exhaustive and, in some cases, the use of blockchain technology may not be strictly required. However, blockchain could be an enabler and catalyst to accelerate digitisation, shift the mindset towards change and transformation, and foster further innovation.

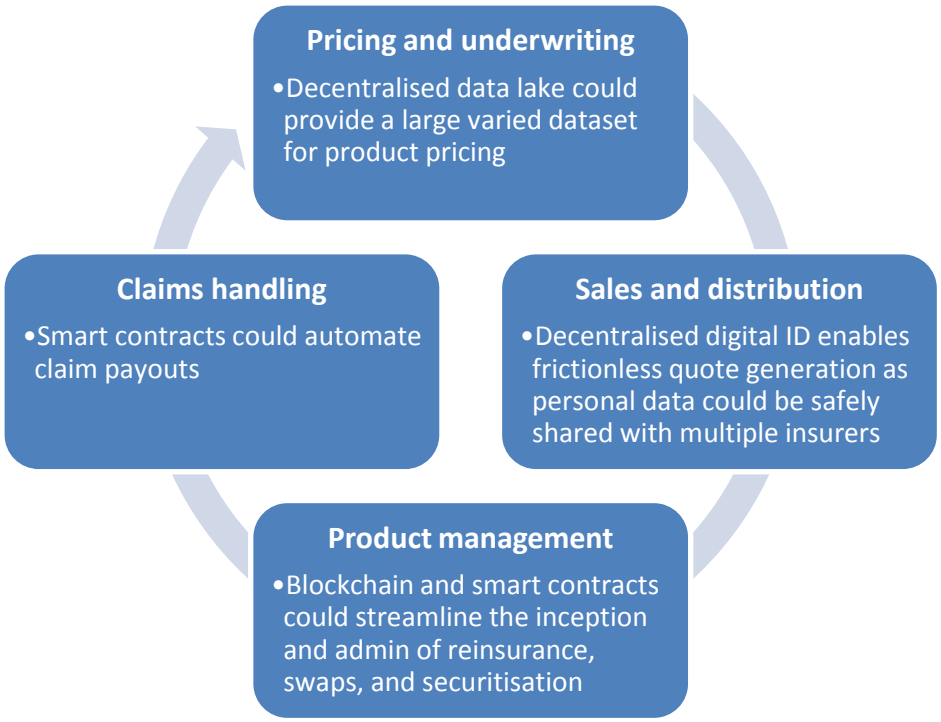

Figure 6: Examples of use cases across the insurance value chain

The following sections discuss the use cases in more detail, covering the problem statement, a high-level description of the use case, main beneficiaries of the use case, the benefits (other than cost savings), and challenges preventing adoption. Many of these use cases are work-in-progress, and are ordered roughly by time to adoption (imminent to long-term).

3.1 Claim processing

Problem statement	• The insurance claim process is a series of manual steps e.g.

[5] As it is not possible to identify an exhaustive list of companies and projects working on these use cases, companies/projects are not named in this paper to avoid implicit endorsement. Additionally, the success rate of these projects is low historically; any named project may not exist or be relevant after the paper is published.

	1. The policyholder fills in a form or makes a phone call to report the claim; 2. The insurer asks for and verifies proof of insured event. Insurer might also need to send out an adjuster to quantify the damage; 3. The insurer receives all the details and pays out the claim. If there is a dispute, the process will take even longer. • The required data for processing a claim might be stored in silos which do not communicate with each other; • Fraud is a potential issue as the policyholder could take advantage of weaknesses in the claim process (information asymmetry and data silos); • For the insurer, it might be a costly process because of manual administration, reconciliations, settling disputes etc.; • For the policyholder, claiming in times of need or distress is an inconvenience.
Blockchain solution description	• The terms of the insurance product are written into a smart contract which automatically pays out claims upon receiving the right parameters. This is feasible for simple "parametric" insurance products where the claim trigger event is easily verifiable from trustworthy publicly available data e.g. flight delay, extreme weather, natural catastrophes, or death of a person (via ubiquitous biometric sensors); • Claims are recorded on the blockchain for auditability to prevent multiple claims on the same insured event.
Main beneficiaries	Incumbents, start-ups, customers
Benefits	• Improves customers' experience; • Prevents insurance fraud by eliminating double-claiming on the same event.
Main challenge to mass adoption	• No proven standards or platform; • The lack of trust-worthy third-party (i.e. oracles) data to trigger a claim on more complex insured events; • Automatic processing/settlement is not new; blockchain and smart contract may not provide a clear benefit over existing technology.

3.2 Reinsurance and swaps

Problem statement	• A typical life reinsurance account takes 2 to 3 months to settle i.e. from the point the insurer pays out a claim to when it receives recovery from the reinsurer. This is mainly due to the time required to gather claims data, calculate reinsured claims / premiums, reconcile claims / premiums, settle disputes, etc.; • There are multiple parties trying to work on the same data but data is stored in silos. This slows down the reinsurance process and is prone to errors; • When trying to make a deal (e.g. bulk annuity), considerable time is spent on cleansing data which could mean missing an opportunity to close a deal if the data is not ready; • Transactions involving collateral require third party to manage the collateral assets. This involves costs, and these assets may be double-pledged; • For bulk annuities, it is difficult to track deferred lives because of a lack of shared data; • For longevity risk transfer, it is generally difficult to novate swaps because new transacting party does not usually have full view of past claims history.
Blockchain solution description	• Reinsurance treaties / swaps terms are written into a smart contract which automatically executes payments (premiums and claims) to/from reinsurers when pre-determined conditions are met; • Experience data is recorded on the blockchain which is tamper-resistant and immediately auditable; • All parties (i.e. insurers, reinsurers, third-party data providers, asset managers, consultants etc.) record data on the blockchain so everyone has access to a single version of the truth; • For bulk annuity deals, cleansed data could be stored on the blockchain which is tamper-resistant and all participants could see what changes have been done; • All transactions (reinsurance premiums and claims) are recorded on the blockchain for visibility to future transacting parties.
Main beneficiaries	Incumbents, start-ups

Benefits	• Reduces complexity of contracts (simplification is by necessity as contract rules are coded rather than in legal prose);
	• More liquid and transparent market for reinsurance deals;
	• Facilitates a secondary market of insurance-linked securities;
	• In the longer-term, once a standard/platform has emerged, standardised data collection and verification will lead to:
	  ○ More reliable data;
	  ○ Reduced lead time from data submission to price quotes;
	  ○ Simplified regulatory reporting requirements.

Main challenge to mass adoption	• No proven standards or platform. However, industry consortia, such as B3i (Blockchain Insurance Industry Initiative) are working to establish an enterprise blockchain standard.

3.3 Tokenisation of insurance risk (i.e. securitisation on the blockchain)

Problem statement	• Intermediaries extract fees from securitising insurance risk, reducing the capital raised; • Insurers incur costly expenses in the administration of the securitised book of business; • Investors often do not have a transparent view of the underlying insurance risk.
Blockchain solution description	• Blocks of insurance business are escrowed on the blockchain, and smart contracts are used to trigger payments to investors when pre-determined conditions are met. This is similar to the reinsurance use case but applied to the capital market; • The insurance-linked security (ILS) is packaged into a "token" i.e. a digital representation of the ILS, potentially widening the investor base (subject to regulatory constraints).
Main beneficiaries	Incumbents, start-ups, investors
Benefits	• A cost-effective way of raising capital and to transfer risk i.e. no fees to intermediaries (e.g. investment banks); • Increases information flow to investors i.e. cashflows arising from the block of business are recorded on the blockchain, and are auditable;

	• Improves liquidity of the ILS market via informed price discovery as a result of the increased information flow to investors.
Main challenge to mass adoption	• No proven standards or platform; • Security laws and regulations around digital representation of assets are not clear.

3.4 Decentralised digital identity

Problem statement	• Compliance to data protection and Know-Your-Customer (KYC) regulations is costly and onerous; • Customers have no control over their personal data and to whom it is shared with.
Blockchain solution description	• Customers' private information is owned and stored locally by customers; blockchain acts as a trusted conduit of data from customers to insurers; • Regulatory Know-Your-Customer (KYC) requirements are codified into a smart contract and automated.
Main beneficiaries	Incumbents, start-ups, customers

Benefits	• Insurers could choose not to store customers' private data. Hence:
	  ○ Limits the attack surface i.e. reduces data breach risk;
	  ○ Reduces the onus of complying with data privacy rules.
	• Customers retain full ownership of their data and control with whom they share what data;
	• Customers could share the same data with multiple insurers, enabling frictionless quote generation;
	• Any changes to personal data could be passed on to insurers in real-time;
	• Advanced encryption techniques such as zero-knowledge proofs mean that customers could share minimal personal data for KYC checks.

Main challenge to mass adoption	• The enabling technology is only just emerging; digital identity is a public good; private enterprises are least incentivised to develop the infrastructure necessary for the technology to work;

	• Insurers need to change the way they consume data as data is not stored by the insurer; • Customers would need to change their mindset with regards to how they manage and possibly monetise their personal data. They need to have the confidence and incentive to share their personal data in return for more benefits, e.g. cheaper premium, personalised products, faster underwriting, etc.

3.5 Decentralised data lake

Problem statement	The proliferation of sensors and connected devices has led to a rise in digital data. These are often in siloed data lakes managed disparately by numerous entities (with various degree of data security processes).
Blockchain solution description	Data from sensors and connected devices is recorded directly on a blockchain-based platform. A data marketplace can be created to incentivise the collection and sharing of data.
Main beneficiaries	Start-ups, customers
Benefits	• Tamper-resistant, verifiable data source; • Democratise access to advantageous pricing data. For example, incumbent insurers have access to customers' wearable data collected over the years. The creation of a decentralised data market place where such information can be sold directly by customers, and purchased by start-ups will level the playing field.
Main challenge to mass adoption	The technology is available but such a market place is ahead of its time; adoption will require a cultural shift.

3.6 Decentralised Autonomous Insurer (DAI)

Problem statement	The existing insurance business and operating model is not optimised for the benefits of policyholders due to the need to return capital to shareholders and high operating costs.
Blockchain solution description	DAI is a convergence of various technological trends (Big Data, AI, Blockchain) once they reach a mature stage: • Insurance products are priced using Big Data by AI-based algorithms;

	• Automatic compliance to Know-Your-Customer (KYC) rules via decentralised digital identity; • Peer-to-peer pooling of risk via blockchain i.e. individuals, communities, corporations can share/transact risk directly; • Premium and claim payments are managed using smart contracts; • Reserves are calculated and invested by AI-based algorithms; • All transactions/data are recorded on the blockchain and made available to the regulator.
Main beneficiaries	End users/customers. This could be highly disruptive to existing business model.
Benefits	• Reduced prices to customers arising from lower operating costs, and the removal of high profit margins priced into insurance contracts; • Communities who are otherwise denied the opportunity to purchase insurance covers due to under-developed business environments or infrastructure could have access to protection via the peer-to-peer business model.
Main challenge to mass adoption	The technology has not reached a mature/steady state.

4 Risks and challenges

As is the case with adopting any new technology, there are risks and challenges that need to be considered when adopting blockchain as an enterprise solution. These issues are not only related to technology, but also business strategy and culture, processes, regulation and financial costs.

4.1 Costs of adoption

Blockchain is potentially disruptive but it may not make commercial sense to be a first mover in adoption for the following reasons:

- Blockchain is a nascent technology as standards/platforms are still emerging. The hype is ahead of development; it will take time for the technology to mature, become cost-effective for mass adoption, and more importantly, to be tested under real-world adversarial conditions. Companies across the insurance industry had piloted proof-of-concepts (PoC). Most of these failed to move to the production stage. One notable exception is a catastrophe excess of loss (Cat XoL) reinsurance application launched by an industry blockchain consortium after 2 years of trial and development;
- Blockchain solution development is an area where mathematics, cryptography, economics, data structure and computer science skills overlap. It is rare to find experienced developers

who tick all boxes. It is even more challenging to find business subject matter experts in the insurance industry with these skill sets;

- In the case of permissionless blockchains, mass collaboration and adoption (i.e. network effect) is required to reap the full benefit. Currently, only cryptocurrencies as a use case have this level of scale whilst other use cases receive little adoption. In the case of permissioned blockchains, intellectual property (IP) might be owned by a select few (e.g. the founding member firms) which might deter new entrants from joining the network, thus hampering adoption. A real-world example is the case of a blockchain-based marine insurance solution co-developed by a container shipping company. Other major marine cargo carriers had reservations about participating in the blockchain solution over concerns that they did not own the IP.

4.2 Security

Trust placed on a centralised authority is replaced by trust that the underlying cryptography and consensus mechanism are fit for purpose. There are a number of known potential security issues with blockchain technology that need to be considered:

- Immutability of blockchain can be a double-edged sword; hacks/fraud/mistakes on the blockchain cannot be reversed without drastic measures i.e. “hard-forking” the blockchain (creating a permanent divergence in the blockchain), rendering the new and old versions of the blockchain incompatible;

- Vulnerability in software e.g. smart contract codes can be badly written and exploited just like any other computer programs. The infamous hard-fork i.e. the “Decentralised Autonomous Organisation (DAO) fork” of the Ethereum blockchain in July 2016 serves as a cautionary tale. The DAO was a blockchain-based venture capital fund built on the Ethereum blockchain. Hackers were able to siphon a substantial amount of Ether (the token native to the Ethereum blockchain, worth more than USD 50 million[6] at the time) by exploiting vulnerabilities in the DAO smart contracts;

- Data recorded on the blockchain is not inherently trustworthy unless data is native to the blockchain (i.e. “on-chain” data created within the blockchain). In particular, smart contracts often rely on external data feed (i.e. off-chain data) from sources known as “oracles”. Oracles ore often data silos operating in a centralised fashion, creating a single point of attack. Smart contracts are not inherently “smart” enough to determine the credibility of data feeds. This introduces a new challenge widely known as the “Oracle Problem”, whereby the execution of smart contracts could be compromised by unreliable external data feeds. This is one of the major obstacles hindering the mainstream adoption of blockchain and smart contracts.

4.3 Regulation

The adoption of blockchain-based solutions and the issuance of tokenised assets (see Section 3.3) represent unprecedented regulatory issues that governments, regulators, enterprises and investors need to assess.

[6] Popper (2016)

4.3.1 Data privacy rules

Data privacy issues have become a hotly debated topic in the blockchain space. The General Data Protection Regulation (GDPR), specifically, the right to be forgotten, is inherently at odds with the immutable nature of blockchain. This is an example of existing regulations having centralised data storage architecture in mind, where it is feasible to request the data processor to delete personal data when instructed to do so. There are at least two possible solutions around this piece of legislation:

- The first and most conventional solution is to not store any personal data on the blockchain. Instead, pointers are used on the blockchain to refer to where personal data is stored off the blockchain, which can be readily deleted;
- The second solution is to only store the hash value of the personal data on the blockchain. It is probabilistically impossible to reverse-engineer a hash value (assuming quantum computing technology is not mature yet to break hash functions) and reveal the original input (i.e. the personal data). It may be argued that the hashed data has become anonymised data and hence does not constitute personal data.

4.3.2 Accounting and capital treatment of cryptoassets

Blockchain is well-known largely due to Bitcoin, a type of cryptoasset. Cryptoasset is an umbrella term for cryptocurrencies, asset-backed tokens (see Section 3.3), utility tokens, digital collectibles etc. There is a lack of clear guidance on the accounting and solvency capital treatment of these assets. Given a particular cryptoasset, the following considerations are likely to present challenges:

- What is the accounting definition of the asset?
- Which area of existing accounting standards is most relevant for the treatment of the asset? If not fit for purpose, are new accounting standards required?
- What is the fair value of the asset if it is not traded in deep and liquid markets?
- What are the key risks associated with the asset? Are there new types of risks that are not associated with conventional assets?
- How does the asset behave under stress? What is the "1-in-200" scenario?

4.3.3 Legal status of smart contracts and cryptoassets

Legislation and regulation have generally not caught up with developments in the blockchain space. It is unclear whether smart contracts would be recognised as a formal legal contract. Similarly, it is not immediately obvious which legislation or regulation cryptoassets fall under. Jurisdictions around the world recognise the need to address this legal uncertainty. In November 2019, the UK Jurisdiction Taskforce[7] (UKJT) published its legal statement on the status of smart contracts and cryptoassets under English and Welsh law. The landmark statement concludes that smart contracts are legally enforceable, and that cryptoassets should be treated as property[8].

[7] The UKJT is one of the six taskforces of the LawTech Delivery Panel, an industry-led group that is tasked with supporting the digital transformation of the UK legal services sector.
[8] UK Jurisdiction Taskforce (2019)

Although the legal statement is not legally binding, it is influential and is an important step in providing confidence in the use of smart contracts and in the ownership of cryptoassets.

4.4 Business strategy and culture

A common feature amongst successful blockchain use cases is that business partners are willing to collaborate. Companies need to be prepared to both cooperate and compete on the same network so that everyone benefits i.e. game theory is at play. Many would struggle to embrace this new thinking and the challenges may include:

- The risk of sharing commercially sensitive data, leading to a loss in competitive advantage – This is one of the reasons companies are reluctant to transact with each other on a public permissionless blockchain (see Section 2.3.1). One area blockchain researchers have been focusing their effort on is the so-called zero-knowledge proof (ZKP). ZKP is an encryption technique which allows "*one party (the prover) to prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x*"[9]. A practical benefit of ZKP is that it allows data to be shared between 2 parties without revealing the data, potentially enabling private transactions on public permissionless blockchains;

- The lack of support from within the organisation due to a natural reluctance to change – New technology often means changing mindsets and existing processes. Creating a culture which encourages innovation and continuous improvements is no small task. One approach to adopting new technology is to allow transformation to take place in a gradual and ring-fenced manner by establishing a new brand under the parent company.

5 Guide to adopting blockchain solutions

Blockchain is a means to an end; adopting blockchain only makes sense if there is a suitable and high impact business use case. The lack of understanding of blockchain technologies and the advantages over existing technologies gives rise to a risk of fitting blockchain to a problem, leading to failed projects and wasted investment. The following guide is provided with this in mind.

In the "*Improving the success of InsurTech opportunities*" paper (Bruce, et al., 2019), the working party created a timeline and checklist which considers how risk management activities can help with the implementation of InsurTech solutions. In this paper, considerations specific to the risks of adopting blockchain/DLT solutions are provided.

5.1 Timeline and checklist

The timeline represents the key lifecycle stages of a blockchain adoption journey, as set out in Figure 7.

[9] Wikipedia, n.d.

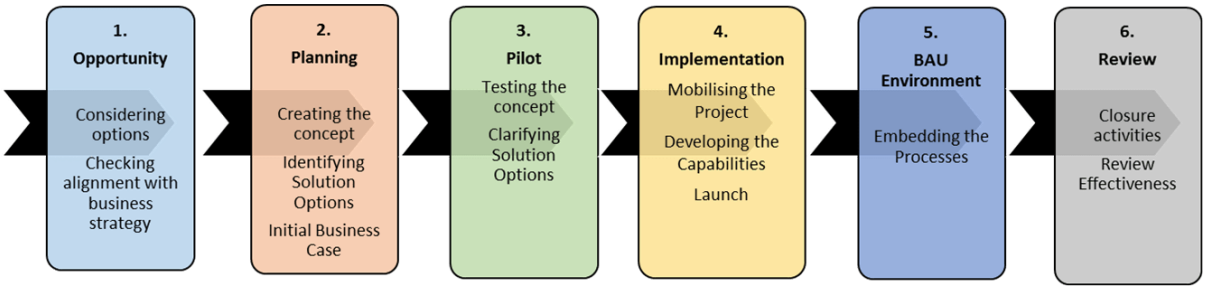

Figure 7: Blockchain adoption journey

The checklist represents a suite of issues to consider at each stage of the adoption journey, phrased as questions. These are mapped to components of a typical enterprise risk management (ERM) framework as shown in Figure 8.

ERM Framework component		Blockchain adoption journey					
		1. Opportunity	2. Planning	3. Pilot	4. Implementation	5. BAU Environment	6. Review
Strategy and business planning	Business strategy and objectives						
	Risk strategy and objectives						
Risk governance and standards	Board / board risk committee and senior management						
	Roles and responsibilities						
	Risk appetite						
	Policies						
Risk management processes	Strategic risk management						
	Financial risk management						
	Operational risk management						
	Stress testing and scenario analysis						
	Change processes						
	Training and communication						
	Risk management effectiveness						
Risk reporting and communications	Risk reporting and ORSA						
	Management information						
	External communications						

Figure 8 ERM framework applied to blockchain adoption

5.1.1 Stage 1: Opportunity

1. Opportunity	Considering options – Review and consider all potential options. Checking alignment with business strategy – Consider which options are strategically aligned.
ERM Framework component(s)	**Strategy and business planning**

Considerations: Strategy and business planning

Business strategy and objectives

1.1 How would blockchain solutions help you improve existing business processes? For example, would it allow you to move towards digitisation by leapfrogging away from legacy systems or paper-based processes?

1.2 How would blockchain solutions help you move into a new operating model? For example, would it provide you with a new way of raising capital, or a novel way of selling products?

1.3 What are your peers or customers doing in the blockchain space? Have they joined any industry consortia in developing a blockchain solution?

1.4 How would joining an industry blockchain consortium align with your business strategy?

1.5 How would you measure the return on investment (ROI) in adopting blockchain?

1.6 What is the risk of no action (including potential lost opportunity)?

Risk strategy and objectives

1.7 Has the full range of risks been considered and their potential impact on your risk strategy (see examples in Section 4)?

1.8 Is your current internal control framework sufficiently robust to mitigate key risks related to blockchain adoption?

5.1.2 Stage 2: Planning

2. Planning	Creating the concept – Take the core options and conceptualise them into real-life propositions that could sit in your business environment. Identifying solution options – Consider how best you are going to deliver into a live proposition – leverage existing technologies, develop new processes? What will the end solution look like? Initial business case – Produce a Business Case which validates the need, how it fits into the strategic direction and the proposed solution. Committee to approve or reject.
ERM Framework components	**Strategy and business planning**

Risk governance and standards

Considerations: Strategy and business planning

Business strategy and objectives

2.1 Do you need blockchain? Would other technology be equally suitable? Specific considerations are:

- Is there a need for a shared version of truth among multiple parties?
- Is there a need for decentralisation (i.e. where the consensus of the true state of the database does not rely on a centralised authority)? For example, where "multiple parties" are trusted entities within a larger organisation, centralised solutions which have the features of blockchain (i.e. distributed, tamper-resistant, transparent) could be more appropriate.

2.2 Which type of blockchain (i.e. permissionless, permissioned, or hybrid) best meet your business needs and requirements? Specific considerations are on design trade-offs between access and privacy (see Section 2.3.1):

- Access – Is there a need for frictionless access? For example, is an efficient, cost-effective customer on-boarding process a key driver for blockchain adoption?
- Privacy – Are transactions on a need-to-know basis? For example, do you need payments to/from a party to be viewable only to select participants?

2.3 Do you have previous experience of delivering blockchain/DLT solutions? What lessons have been learned?

2.4 What capability do you have to develop Intellectual Property (IP) in-house versus partnering with external firms, who may be able to reduce timescales and risk? Which approach is more aligned with strategic objectives and is owning the IP and retaining knowledge and experience key to the business strategy?

Risk strategy and objectives

2.5 Is adopting blockchain solutions in line with your risk strategy and objectives?

2.6 Has a high-level assessment been undertaken to identify the key risks arising from adopting blockchain solutions, including new risks introduced and/or changes to existing risks?

2.7 Do you have clear and rigorous decision-making processes to follow when choosing a blockchain solution?

Considerations: Risk governance and standards

Board / board risk committee and senior management

2.8 Does blockchain adoption need to be discussed at higher levels? Has the opportunity / business case been discussed with the Board? What key issues will the Board have?

2.9 Early discussion allows engagement to be more likely to result in internal acceptance. Specific issues are likely to be: meeting customer needs, confidentiality concerns, timescales, execution risk & cost vs benefits.

5.1.3 Stage 3: Pilot

3. Pilot	Testing the concept – Test that the solution proposed in the business case does what the business case states it will do.
	Clarifying solution options - Define the functional and non-functional requirements of the proposed solution.
ERM Framework components	**Strategy and business planning** **Risk governance and standards** **Risk management processes** **Risk reporting and communications**

Considerations: Strategy and business planning

Business strategy and objectives

3.1 Which blockchain platform should you use to implement the solution? Specific considerations include:

- Is the platform widely adopted by practitioners within and outside of the industry?
- Is there a chosen/recommended platform within the industry?
- Is the performance of the platform limited by certain design choices (see Section 2.3.1)?
- Would the solution be easy to implement on the platform? For example, is there an existing pool of talents who are familiar with the platform?
- Would there be interoperability issues with other platforms?
- Does adopting a platform which uses Proof-of-Work (PoW) consensus mechanism constitute a breach of internal/external Environmental, Social, and Governance (ESG) policy due to its excessive use of electricity and contribution to climate change?

Considerations: Risk governance and standards

Roles and responsibilities

3.2 Are the roles and responsibilities for all key participants agreed, documented and communicated?

Risk appetite

3.3 Has the risk appetite for digital innovations been defined? This may differ from other risk appetites in that it should recognise that failure of the innovation is a possibility.

3.4 Is blockchain/DLT adoption in line with any risk preferences that have been set by the Board? If the opportunity is outside of the existing preferences and limits, has this been explicitly discussed with and agreed by the Board?

Considerations: Risk management processes

Strategic, financial, and operational risk management

3.5 Has the full range of internal risks associated with blockchain adoption been identified? For example:

- Strategic risks;
- Financial risks;
- Operational risks, including reputational risk, regulatory changes, technology, cyber, data security etc.

3.6 Has the Risk Function identified and assessed risks to the business and communicated associated issues and actions? Have the material risks been quantified?

Operational risk management

3.7 Are contractual arrangements with any third parties in place, including deliverables, objectives and IP?

3.8 What are the biggest factors that may cause a blockchain consortium or third-party data providers (i.e. oracles) to fail?

- Do you have mitigation plans?
- Do you have plans to avoid significant loss if third parties fail?

Considerations: Risk reporting and communications

If relevant, have there been communications with the relevant regulators / supervisors?

5.1.4 Stage 4: Implementation

4. Implementation	Mobilising the project – Establish a team for delivering the proposed solution. Undertake more detailed planning.
	Delivering the capabilities – Putting in place processes and systems that will make the solution happen.
	Launch – Take the solution from a development environment through testing to a live environment.
ERM Framework components	**Strategy and business planning** **Risk governance and standards** **Risk management processes** **Risk reporting and communications**

Considerations: Strategy and business planning

Business strategy and objectives

4.1 How would a decentralised form of governance align with your business strategy? Specific considerations include but are not limited to:

- Would you have a leading role in making major policy or technical decisions?
- What are the contractually obligated resources (e.g. financial costs and time) required for the on-going participation and the maintenance of the blockchain network?
- To what extent are you willing to be open and collaborative with a potential competitor?

Considerations: Risk governance and standards

Policies

4.2 Have your firm's policies been reviewed and, where required, updated to reflect changes arising from blockchain adoption? Specifically, is the policy appropriate in relation to engagement with other participants on the blockchain network?

Considerations: Risk management processes

Strategic, financial and operational risk management, stress testing and scenario analysis

4.3 Has a full assessment been undertaken to identify and assess risks to the business, with associated issues and actions? Does blockchain adoption materially change your firm's risk profile, according to the following criteria:

- The potential change to your firm's risk profile arising from strategic, financial and operational risks;
- The regulatory risks from adopting blockchain-based solutions given the regulatory uncertainties (see examples in Section 4.3);
- Whether the risks associated with the project causes your firm to breach any risk appetite tolerance, limits or thresholds;
- The risks to delivering the benefits arising from the project, including the use of external third parties and outsourcing;
- Whether the project introduces a material new risk to your firm;
- Whether the project delivery methodology is 'tried and tested' within the firm and whether the Risk team has the skills and resources to engage effectively with the project at the right time;
- Whether the project is similar to, or introduces similar risks to, previous projects;
- The capital and financial impact.

4.4 Has your firm considered a set of sensitivities to the underlying assumptions, in order to understand what the key factors are which influence the ROI and the ultimate success of the investment?

4.5 Does the assessment consider a set of future scenarios of plausible events which may cause the investment to be less successful? What contingent actions arise from this analysis?

Operational risk management: People and organisation

4.6 How are leaders prepared to manage their functions' transitions to greater digitisation and automation?

4.7 How can your firm empower leaders to adjust processes and technology investments to respond quickly to new developments?

4.8 What challenges are there to processing new information and making decisions?

4.9 What criteria are required to consider whether to change course if necessary?

4.10 Which parts of the firm are able to move and adapt quickly - what characteristics drive this? Can these characteristics be used to assist the slower moving parts of the firm?

4.11 If the project displaces workers from their current roles, how can the organization effectively retrain them and/or move them to different roles?

4.12 How will staff collaborate on development activities?

4.13 How will your firm's recruitment plans change to acquire the new talent with the requisite skills to deliver the opportunity?

4.14 Does the operating model need to be enhanced? Is each function clear about its responsibilities and how these will be delivered alongside existing processes?

Operational risk management: Processes

4.15 What new processes need to be designed and implemented?

4.16 How do these new processes align to existing processes?

4.17 How will these new capabilities enable your firm to drive long-term growth?

4.18 Is there a feedback loop, and is it appropriate, to ensure that your firm can learn from successes and failures?

4.19 Are there opportunities for further efficiency gains?

4.20 What third party support is required to successfully run the processes and how are these to be engaged? For example, do you need oracles to provide off-chain data that smart contracts would rely upon to trigger pre-defined actions?

Change processes

4.21 Is the project fully established, with appropriate governance, project management disciplines etc.?

- Are the existing governance arrangements appropriate or do they need to be enhanced / amended?
- Have success criteria for the project been set and go / no-go gates been agreed in advance?
- Do the success criteria consider risk-adjusted return metrics?

4.22 Who will own the delivery of the digital opportunity?

Training and communication

4.23 What gaps, if any, exist in staff competencies and skills required to drive a digital strategy?

4.24 What training needs to be developed and delivered?

4.25 Is there the necessary skills and expertise in-house or is external expertise required?

Considerations: Risk reporting

Risk reporting and ORSA

4.26 Can your firm's current risk reporting and ORSA processes appropriately report risks arising from blockchain adoption?

Management information

4.27 What management information needs to be produced in order to be able to monitor progress?

4.28 Where and when will this new management information be reported?

5.1.5 Stage 5: BAU environment

5. BAU environment	Embedding the processes – Review the BAU processes and consider whether further changes required.
ERM Framework components	**Risk management processes** **Risk reporting and communications**

Considerations: Strategy and business planning

Business strategy and objectives

5.1 What further automation could be achieved in the processes?

5.2 Is the decentralised governance framework working? What needs to be improved?

Considerations: Risk management processes

Strategic, financial, operational risk management, stress testing and scenario analysis

5.3 Is there ongoing review, monitor and challenge of the risks to the business as well as issues and actions, covering for example:

- Strategic risks
- Financial risks
- Operational risks, including reputational risk, regulatory changes, technology, cyber, data security etc?

5.4 Is the quantification of material risks regularly reviewed? How often?

5.5 Are the stress tests and scenario analyses regularly reviewed and updated?

Operational risk management: Consortia and third parties

5.6 *Optimising consortia participation*: Is your firm continuously re-evaluating the relationship (openly) to ensure that the participation in any blockchain consortia is optimised to maximise the benefits as you learn more about each other?

5.7 *Scrutinising third party data providers (i.e. oracles):* Is your firm continuously re-evaluating the limitations of the off-chain data provided by oracles? Is there a range of potential alternatives given the execution risk and the diverse approaches to ensuring that off-chain data is accurate?

Considerations: Risk reporting and communications

Risk reporting and ORSA

5.8 Are the risks and opportunities regularly recorded and reported through the risk reporting & ORSA processes?

Management Information

5.9 Is appropriate management information produced, in order to effectively monitor progress?

5.10 Is the management information reported to the appropriate fora?

5.1.6 Stage 6: Review

6. Review	Closure Activities – Undertake review: What are the lessons learnt? Should changes be made to the processes? Feedback loop to Change Governance Framework.
ERM Framework components	**Risk management processes**

Considerations: Risk management processes

Risk management effectiveness

6.1 To what extent is the firm able to evidence that risk management has been taken into consideration appropriately throughout the decision-making process including challenge and review from relevant committees and stakeholders?

6.2 Has your firm undertaken a review of the blockchain solution implementation and the extent to which risk management activities have facilitated a better outcome? These learnings can then be taken forward to subsequent opportunities.

6.3 The review should include:

- effectiveness and engagement of key stakeholders with the risk process;
- updating of risks / issues / actions;
- whether actions were taken to mitigate or manage risks;
- reporting of risks to the appropriate person / committee;
- key learnings from the project.

6.4 This should also include consideration of whether the project:

- mitigated or managed risks
- increased risk
- introduced new risks.

6 Conclusion

This paper provides a practical guide to insurance industry practitioners on understanding, assessing and adopting blockchain. It covers the distinctive attributes of blockchain, real-world use cases currently in development, risks and challenges associated with adoption, and a guide to successful adoption of blockchain based on the framework proposed in the working party's Phase 1 output.

It is true that the excitement surrounding blockchain has not yet led to a tangible impact on the insurance industry. However, like most innovations, adoption does not happen overnight. Blockchain adoption is a team sport relying on the collaboration of multiple stakeholders. For example, governments and regulators, in consultation with the industry, need to provide regulatory clarity to spur further innovation. The insurance industry, in turn, needs to collaborate to formulate blockchain standards and to ensure interoperability between different solutions.

Where there has been adoption, the key driver is a need to replace paper-based processes, digitise end-to-end business processes and increase trust in the value chain. This only scratches the surface of what the technology is capable of.

As Tim Harford, the economist and journalist recounted, "*in 1881, Edison built electricity generating stations at Pearl Street in Manhattan and Holborn in London. Within a year, he was selling electricity as a commodity. A year later, the first electric motors were driving manufacturing machinery. Yet by 1900, less than 5% of mechanical drive power in American factories was coming from electric motors. The age of steam lingered.*" (Harford, 2017).

Slowly but surely, blockchain insurance applications and use cases will mature, and adoption will increase as mindset shifts, thus transforming existing insurance business and operating models.

7 References

Amara, R. (2006). *Roy Amara - Oxford Reference*. Retrieved October 2019, from https://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00018679

Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., . . . Dill, D. L. (2019). *The Libra Blockchain.* Retrieved October 2019, from https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf

Baliga, A. (2017). *Understanding Blockchain Consensus Models.* Retrieved October 2019, from https://www.persistent.com/wp-content/uploads/2018/02/wp-understanding-blockchain-consensus-models.pdf

Bruce, D., Avis, C., Byrne, M., Gosrani, V., Lim, Z., Manning, J., . . . Qin, W. (2019). *Improving the success of InsurTech opportunities.* Retrieved October 2019, from

https://www.cambridge.org/core/journals/british-actuarial-journal/article/improving-the-success-of-insurtech-opportunities/73FCA24E992D5B381DADBEBE256A38C2

But how does bitcoin actually work? (2017). Retrieved October 2019, from https://www.youtube.com/watch?v=bBC-nXj3Ng4

Buterin, V. (2013, December). *A Next-Generation Smart Contract and Decentralized Application Platform.* Retrieved December 2019, from https://github.com/ethereum/wiki/wiki/White-Paper

Buterin, V. (2014). *On Stake.* Retrieved October 2019, from https://blog.ethereum.org/2014/07/05/stake/

Buterin, V. (2017). *The Meaning of Decentralization*. Retrieved October 2019, from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Consensys. (n.d.). *Ethereum Smart Contract Best Practices.* Retrieved January 2020, from https://consensys.github.io/smart-contract-best-practices/

Curran, B. (2018). *What is a Merkle Tree?* Retrieved October 2019, from https://blockonomi.com/merkle-tree/

Harford, T. (2017). *Why didn't electricity immediately change manufacturing?* Retrieved December 2019, from https://www.bbc.co.uk/news/business-40673694

Hearn, M., & Brown, R. G. (2019, August 20). *Corda: A distributed ledger.* Retrieved December 2019, from https://www.r3.com/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf

How does a blockchain work - Simply Explained. (2017). Retrieved October 2019, from https://www.youtube.com/watch?v=SSo_EIwHSd4

Kannengiesser, N., Dehling, T., Lins, S., & Sunyaev, A. (2019). What Does Not Fit Can be Made to Fit! Trade-Offs in DLT Designs.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved October 2019, from https://bitcoin.org/bitcoin.pdf

Popper, N. (2016, June 17). *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency.* Retrieved January 2020, from https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html

Rauchs, M., Glidden, A., Gordon, B., Pieters, G., Recanatini, M., Rostand, F., . . . Zhang, B. (2018). *Distributed Ledger Technology Systems: A Conceptual Framework.* Retrieved from https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/#.XX48iZNKh0s

UK Jurisdiction Taskforce. (2019, November). *Legal statement on cryptoassets and smart contracts.* Retrieved January 2020, from https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf

Wikipedia. (n.d.). *Cryptographic hash function*. Retrieved October 2019, from https://en.wikipedia.org/wiki/Cryptographic_hash_function

Wikipedia. (n.d.). *Digital signature*. Retrieved October 2019, from https://en.wikipedia.org/wiki/Digital_signature

Wikipedia. (n.d.). *Zero-knowledge proof*. Retrieved January 2020, from https://en.wikipedia.org/wiki/Zero-knowledge_proof

World Economic Forum. (2018). *Blockchain Beyond the Hype: A Practical Framework for Business Leaders.*

8 Glossary

Centralised authority – A central governing organisation, typically (but not limited to) corporations or governments, which exerts control on a network or system

Consensus mechanism – A set of rules used to reach agreement on what is the authoritative version of record in a distributed database

ERM – Enterprise Risk Management

Fork – Divergence in the blockchain. Most forks are short-lived due to the difficulty of reaching fast consensus in a distributed system. Hard forks (i.e. protocol changes) are permanent and have been used to add new features to a blockchain, to reverse the effects of hacking, or catastrophic bugs

Node – A participant on the blockchain network

Nonce – An arbitrary random number which "miners" in a PoW consensus mechanism need to solve for (by using brute computational force) to be able to commit state change to the blockchain

On-chain data – Data created within the blockchain

Off-chain data – External data not created within the blockchain

PoW – Proof-of-Work consensus mechanism which requires solving cryptographic puzzle by brute computational force for a state change to be committed to the blockchain

PoS – Proof-of-Stake consensus mechanism where a pool of validators (who hold a certain amount of the digital currency/token native to the blockchain i.e. the stake) are selected to verify a state change and commit it to the blockchain

PoA – Proof-of-Authority consensus mechanism where trusted entities vote on whether to commit the transactions to the shared database

Smart contracts – An umbrella term for self-executing code that automates business logic on the blockchain

State – The current snapshot of the data on the blockchain

London

7th Floor · Holborn Gate · 326-330 High Holborn · London · WC1V 7PP
Tel: +44 (0) 20 7632 2100 · Fax: +44 (0) 20 7632 2111

Edinburgh

Level 2 ·Exchange Crescent · 7 Conference Square · Edinburgh ·EH3 8RA
Tel: +44 (0) 131 240 1300 · Fax +44 (0) 131 240 1311

Oxford

1st Floor · Park Central · 40/41 Park End Street · Oxford · OX1 1JD
Tel: +44 (0) 1865 268 200 · Fax: +44 (0) 1865 268 211

Hong Kong

2202 Tower Two · Lippo Centre · 89 Queensway · Hong Kong
Tel: +852 2147 9418 · Fax: +852 2147 2497

Beijing

6/F · Tower 2 · Prosper Centre · 5 Guanghua Road · Chaoyang District · Beijing · China 1000020
Tel: +86 (10) 8573 1000

Singapore

163 Tras Street · #07-05 Lian Huat Building · Singapore 079024
Tel: +65 6717 2955

www.actuaries.org.uk