Institute
and Faculty
of Actuaries

Understanding blockchain for insurance use cases

A practical guide for the insurance industry

Zhixin Lim
Chadwick Cheung
Darko Popovic

03 February 2020

Contents

1. Introduction
2. Blockchain 101
3. Insurance use cases
4. Risks and challenges
5. Guide to adopting blockchain solutions

Disclaimer: The views expressed in this publication are those of invited contributors and not necessarily those of the Institute and Faculty of Actuaries or the employers of the contributors. The Institute and Faculty of Actuaries and employers of the contributors do not endorse any of the views stated, nor any claims or representations made in this publication and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this publication. The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this publication be reproduced without the written permission of the Institute and Faculty of Actuaries.

Institute
and Faculty
of Actuaries

Introduction

03 February 2020

Introduction to the working party

“Risk Management in a Digital World” Working Party

- Formed in 2018
- Focuses on researching and developing the risk management practices and capabilities for assessing and managing risks associated with InsurTech activities

Working Party members

- Darko Popovic (Chair): Director, FTI Consulting
- Carole Avis: CRO, L&G Insurance & General Insurance
- Matthew Byrne: Chief Actuary, NFU Mutual
- Chadwick Cheung: Manager, EY
- Martin Donovan: Head of Actuarial and Finance, ExO Hub Irish Life (IRL)
- Yiyi Flynn: ERM Manager, Prudential
- Craig Fothergill: Deputy Chief Actuary, Assurant
- Zahra Hossein-Zadeh: Actuarial Advisor, Accident Compensation Corporation New Zealand (NZ)
- Jinal Shah: Incubation Manager, JITO JIIF (IND)
- Zhixin Lim: Senior Manager, HSBC

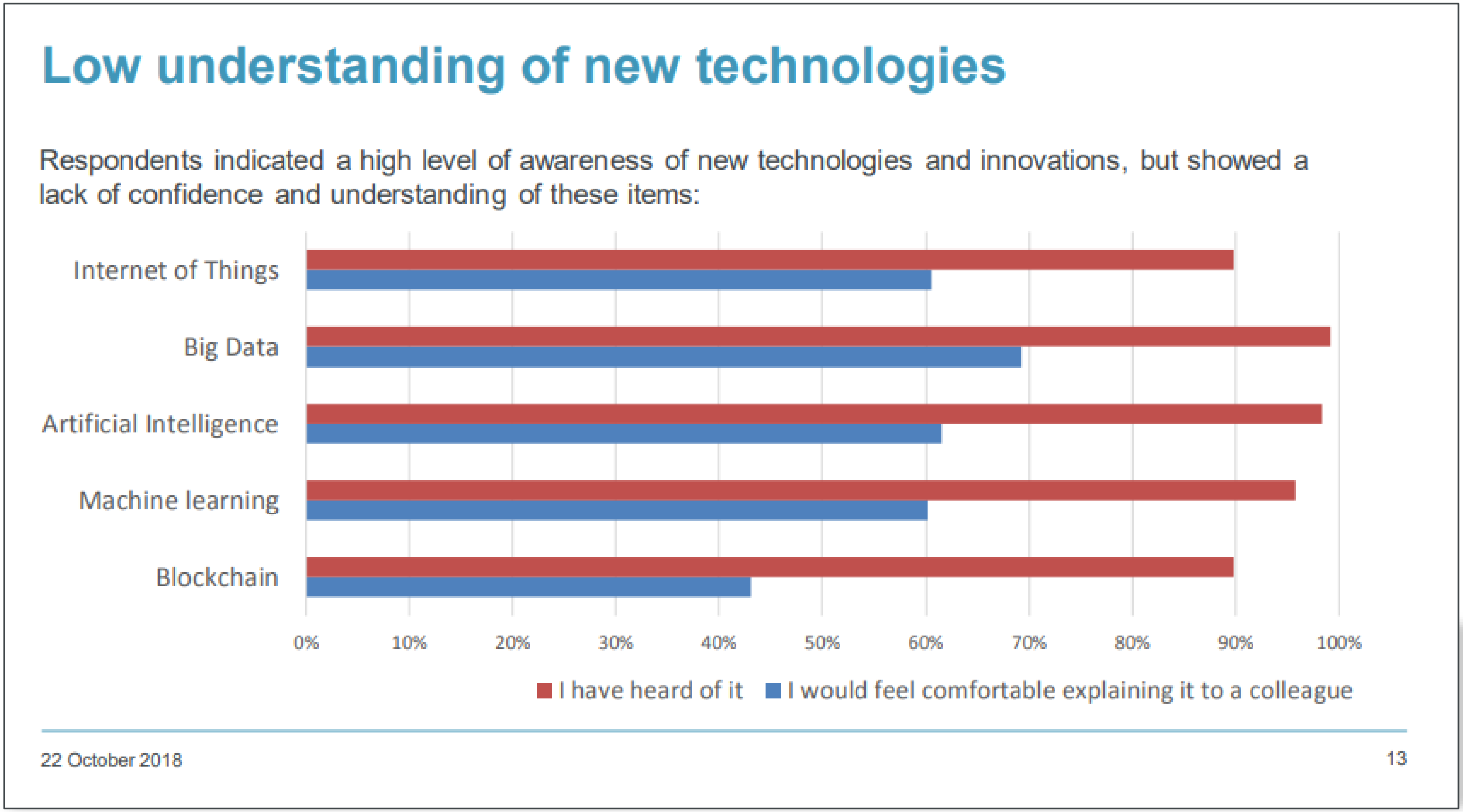
Previous output (Phase 1)

“Improving the Success of InsurTech Opportunities”

- Including “Guidelines for risk considerations during the innovation journey”
- Sessional event October 2018, Edinburgh
- BAJ paper
- SAI event early 2019

- Relied on output from our survey on risk management in a digital world…
- …and interviews with senior stakeholders in industry

Phase 2: Why focus on Blockchain?



Low understanding of new technologies

Respondents indicated a high level of awareness of new technologies and innovations, but showed a lack of confidence and understanding of these items:

22 October 2018

13

Phase 2: Objectives

Objectives:

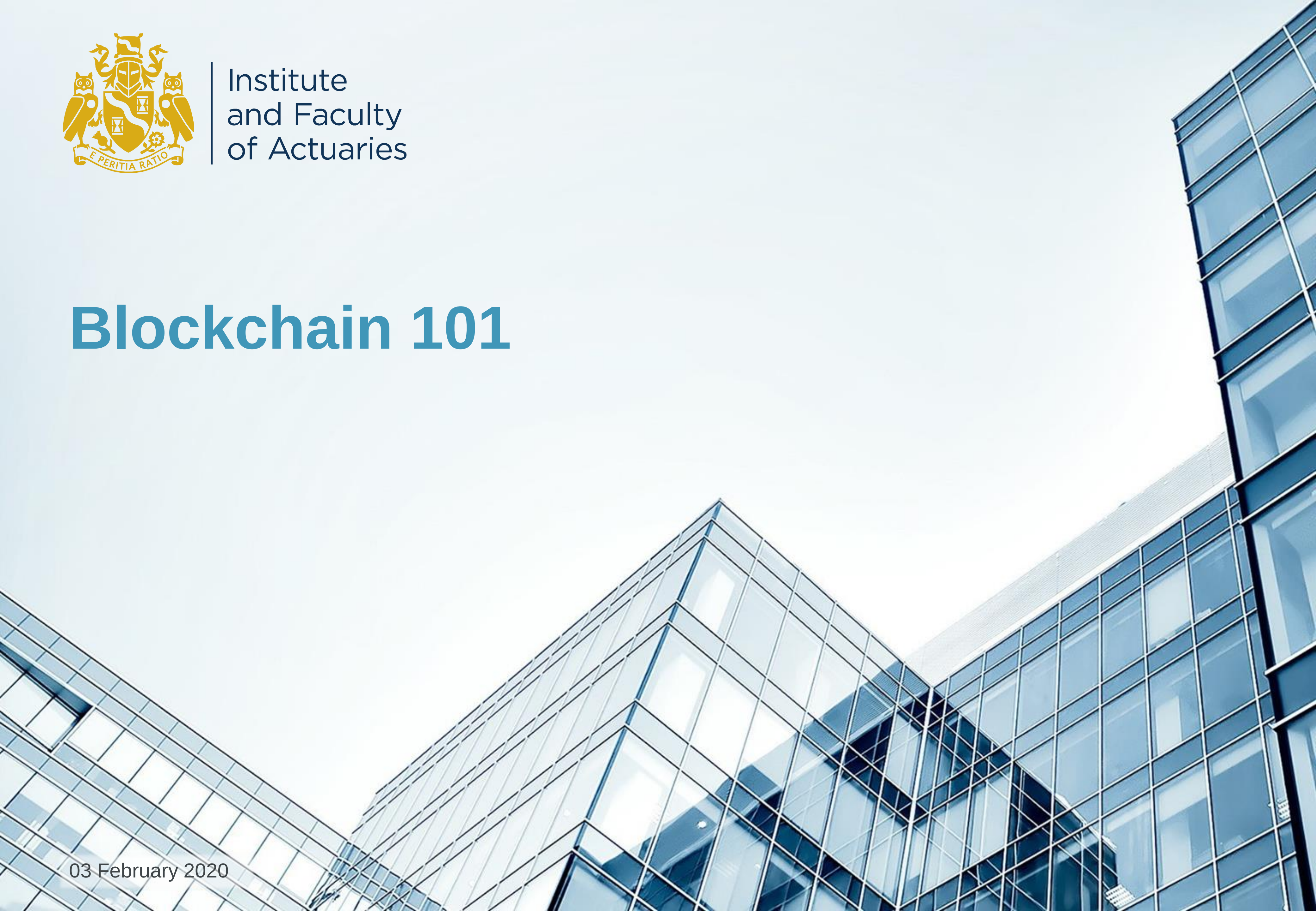
- Explain to colleagues what blockchain is and how it works
- Have an initial discussion on potential use cases
- Consider the risks and opportunities at a high level
- Have a framework in place if deciding to pursue blockchain development opportunity

Key sections for today’s session:

1. Education piece
2. Consideration of insurance industry use cases
3. Consideration of risk and challenges
4. ERM Framework checklist in the context of a blockchain solution to further pursue an opportunity

Institute
and Faculty
of Actuaries

Blockchain 101



03 February 2020

What is blockchain and how does it work?

For the purposes 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.*

At its most basic level, blockchain is a ledger 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.

Let's demonstrate how this works in a simple exercise, and it will introduce some of the key concepts of blockchain technology, including:

- Distributed ledger
- Decentralisation
- Consensus
- Permissionless vs. permissioned; public vs private
- Miner

How is blockchain different?

The key difference between a blockchain and a traditional database is (de)centralisation.

Database	Feature	Blockchain	
Client-server architecture	Topology	Peer-to-peer network	1
Centralised	Authority	Decentralised (if permissionless)	2
Transparent to the extent approved by the administrator	Transparency	Fully transparent (if public)	3
Create, Read, Update, Delete	Data operation	Read and Write only	4
Relatively easier to compromise	Security	Much harder to compromise	5
Much faster and more scalable	Performance	Scalability is constrained by decentralisation or security	6

1. Distributed – verified data is propagated to participants on the blockchain network so that multiple parties have the same record.
2. Decentralised – the maintenance of the network, including data verification, does not depend on a centralised authority.

How is blockchain different?

Database	Feature	Blockchain	
Client-server architecture	Topology	Peer-to-peer network	1
Centralised	Authority	Decentralised (if permissionless)	2
Transparent to the extent approved by the administrator	Transparency	Fully transparent (if public)	3
Create, Read, Update, Delete	Data operation	Read and Write only	4
Relatively easier to compromise	Security	Much harder to compromise	5
Much faster and more scalable	Performance	Scalability is constrained by decentralisation or security	6

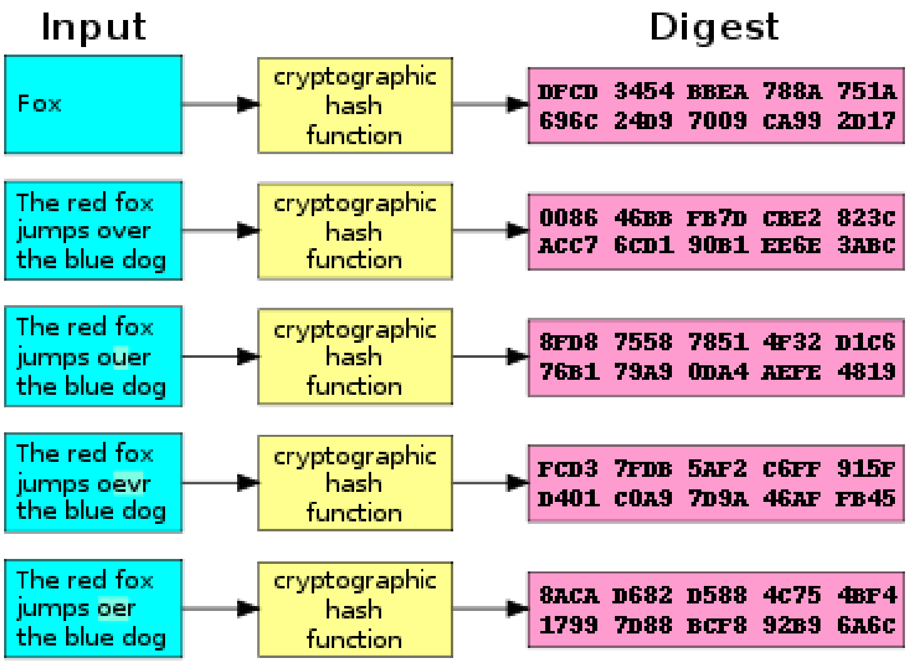
3. Transparent – data on the blockchain is fully auditable for those with access.
4. Read / Write only – (almost) impossible to delete once written on the blockchain.
5. Tamper-resistant – verified data is cryptographically secured, making it resistant to malicious alterations.
6. The “Impossible Triangle” – a (conventional) blockchain is (for now) only able to have two of these attributes, namely scalability (defined as throughput), decentralisation and security.

What are the key components of blockchain?

There are four key components in a blockchain:

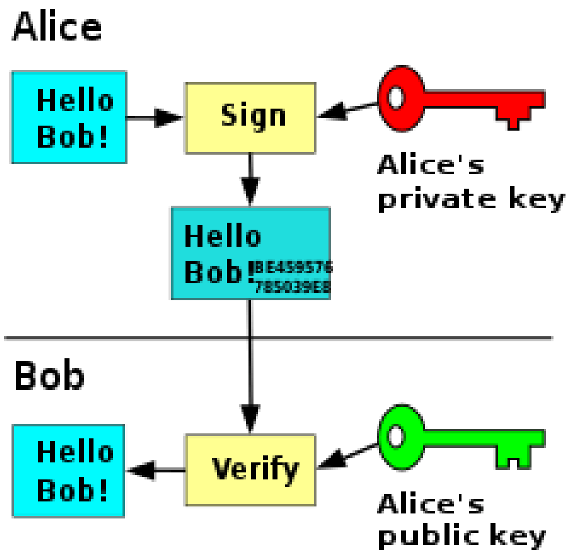
1. Cryptographic hash function
2. Digital signature
3. Blocks and chains
4. Consensus algorithm

1. Cryptographic hash function - 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.


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

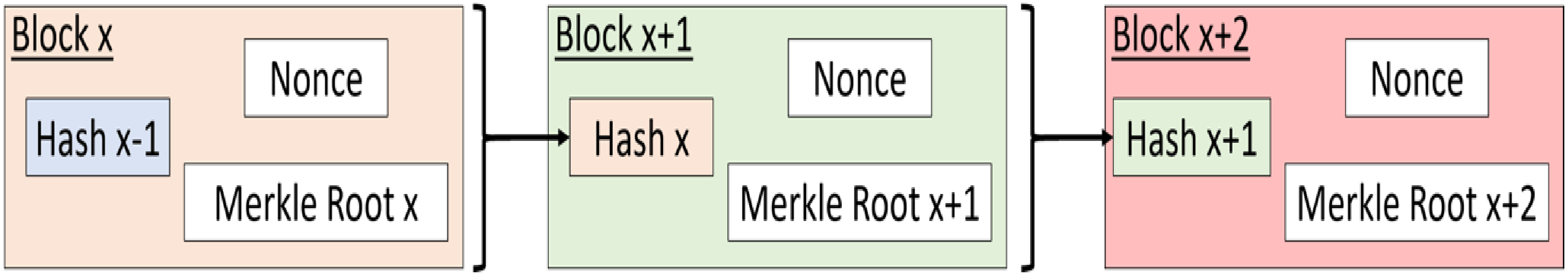
What are the key components of blockchain?

2. Digital signature – it serves as a unique fingerprint and 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.



What are the key components of blockchain?

3. Blocks and chains - the root hash/Merkle root forms part of the block header. Another component of the same block header is the hash of the previous block. This unique data structure where blocks are chained together is a distinctive feature of blockchain that makes it tamper-resistant.



What are the key components of blockchain?

4. Consensus algorithm - 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. Here are some examples:

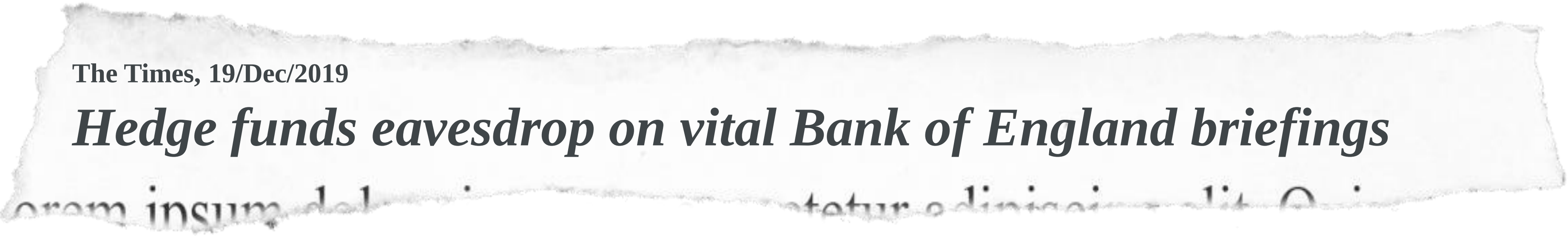
Consensus algorithm	High-level description
Proof-of-Work (PoW)	Requires solving cryptographic puzzles by brute computational force for a state change to be committed to the blockchain.
Proof-of-Stake (PoS)	Unlike PoW where miners compete to commit state changes to the blockchain, PoS selects from a pool of validators who hold a certain amount of the digital currency/token native to the blockchain (i.e. the stake).
Proof-of-Authority (PoA)	Trusted entities vote on whether to commit the state changes to the blockchain.

Institute
and Faculty
of Actuaries

Insurance use cases

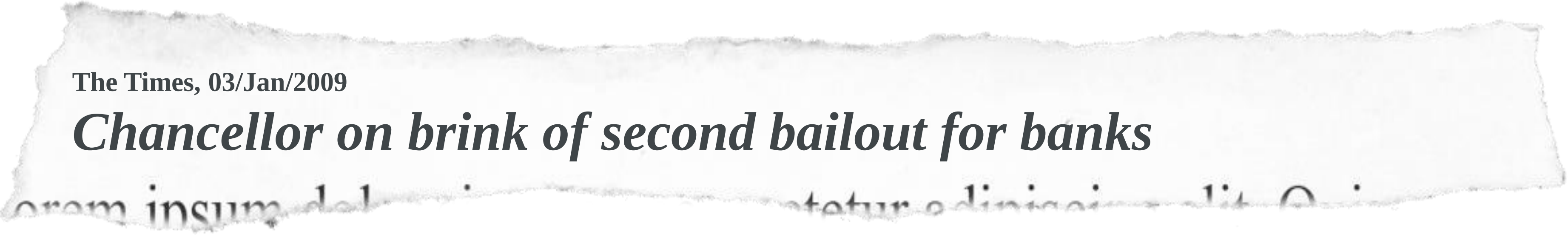
03 February 2020

Brief context on blockchain



The Times, 19/Dec/2019

Hedge funds eavesdrop on vital Bank of England briefings



The Times, 03/Jan/2009

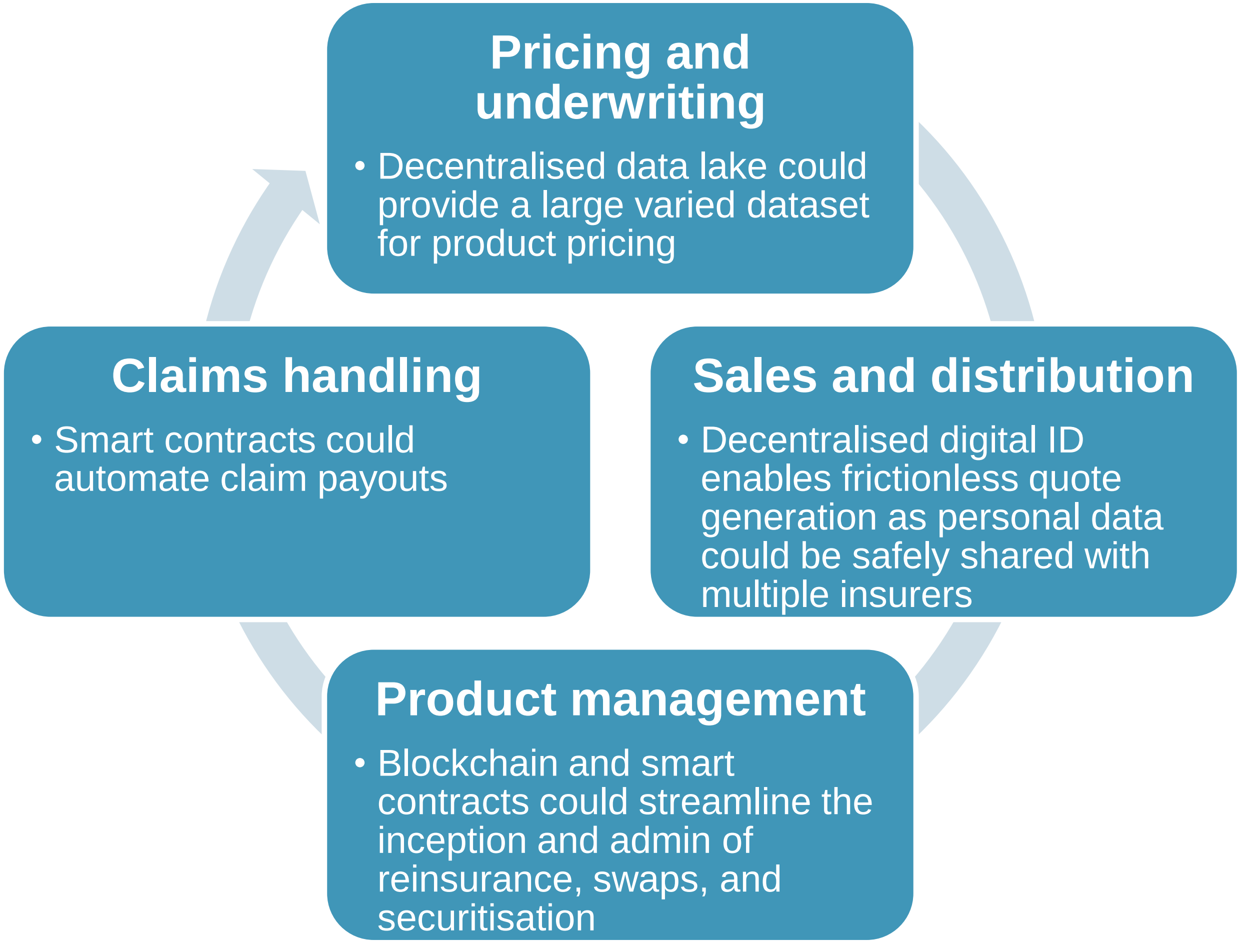
Chancellor on brink of second bailout for banks

Drivers for use cases in insurance

Compelling use cases arise from a need to:

- Produce a shared tamper-resistant record
- Reduce operational frictions and costs
- Remove intermediaries

Examples of use cases



Pricing and underwriting

- Decentralised data lake could provide a large varied dataset for product pricing

Sales and distribution

- Decentralised digital ID enables frictionless quote generation as personal data could be safely shared with multiple insurers

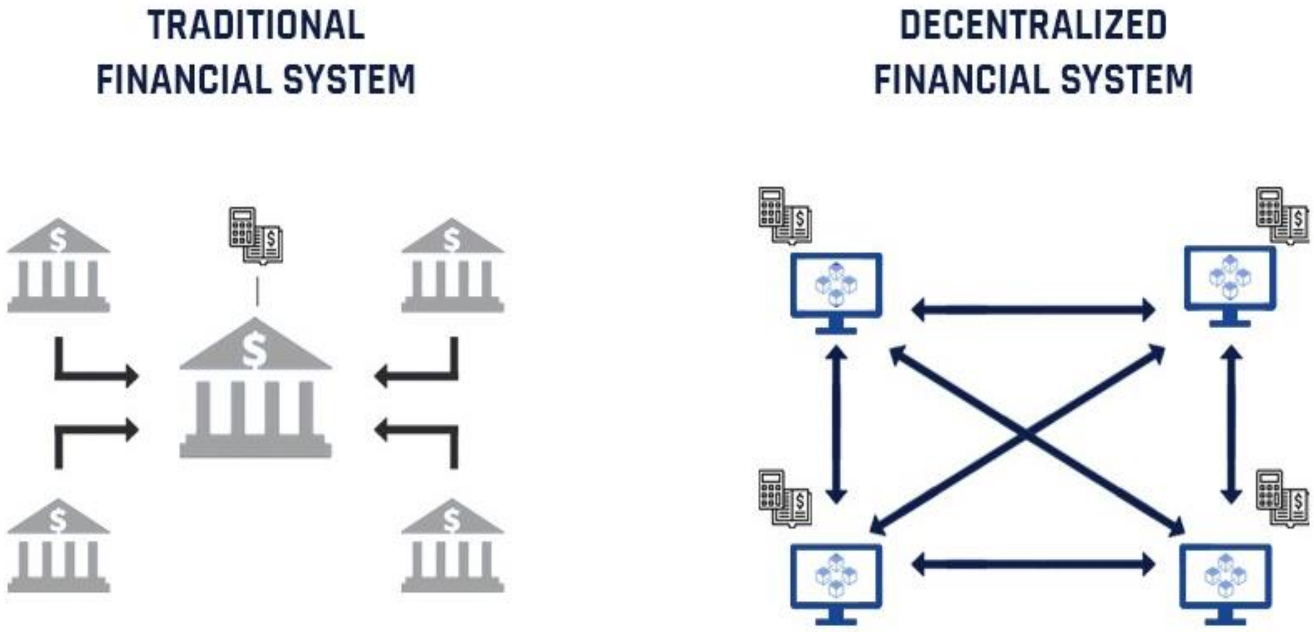
Product management

- Blockchain and smart contracts could streamline the inception and admin of reinsurance, swaps, and securitisation

Claims handling

- Smart contracts could automate claim payouts

Decentralised finance (DeFi) and insurance



Key characteristics:

- Peer-to-peer
- Permissionless

Current limitations:

- Relatively new technology
- User experience

Institute
and Faculty
of Actuaries

Risks and challenges

03 February 2020

Top risks and challenges to consider

Costs of adoption

- Blockchain is a nascent technology as standards/platforms are still emerging
  - While many concepts have been proven, most PoCs failed to progress further
  - One exception is a catastrophe excess of loss (Cat XoL) reinsurance application launched by an industry blockchain consortium
- Blockchain solutions development requires an understanding of multiple disciplines such as mathematics, cryptography, computer science
  - Talents are hard to find and usually a diverse team is needed
  - Blockchain is allegedly the most in-demand skill in 2020 according to a professional social media site
- There are specific challenges depending on the type of blockchain
  - In the case of permissionless blockchains, mass collaboration and adoption (i.e. network effect) is required to reap the full benefit
  - In the case of permissioned blockchains, intellectual property (IP) might be owned by a select few which might deter new entrants from joining the network

Top risks and challenges to consider

Security

- Immutability of blockchain can be a double-edged sword
  - Hacks/fraud/mistakes on the blockchain cannot be reversed easily and may require drastic measures, e.g. hard-forking
- Vulnerability in software can be exploited e.g. bugs in smart contract code can lead to financial losses
  - The infamous hard-fork of the Ethereum blockchain, i.e. the "Decentralised Autonomous Organisation (DAO) fork" in July 2016, serves as a cautionary tale
- 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
  - 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. This is known as the "Oracle Problem"

Top risks and challenges to consider

Regulation

- Data protection laws, e.g. GDPR pose challenges but there are solutions:
  - 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
  - Only store the hash value of the personal data on the blockchain. It may be argued that the hashed data is anonymised hence does not constitute personal data
- There is a lack of clear guidance on the accounting and solvency capital treatment of cryptoassets, e.g. cryptocurrencies, asset-backed tokens, utility tokens, digital collectibles
  - 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? What is the “1-in-200” scenario?
- It is unclear whether smart contracts would be recognised as a formal legal contract, and which regulation cryptoassets fall under
  - The UK Jurisdiction Taskforce published its legal statement on their status under English and Welsh law in Nov 2019 and concluded that smart contracts are legally enforceable, and that cryptoassets should be treated as property (but not legally binding)

Top risks and challenges to consider

Business strategy and culture

- No companies are prepared to share commercially sensitive data
    - One solution that is generating a lot of attention is zero-knowledge proof (ZKP) which allows data to be shared between two parties without revealing the data
    - 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
- The lack of support from within the organisation due to a natural reluctance to change
    - Creating a culture which encourages innovation and continuous improvements is no small task and will take time
    - One approach is to allow transformation to take place in a gradual and ring-fenced manner by establishing a new brand under the parent company

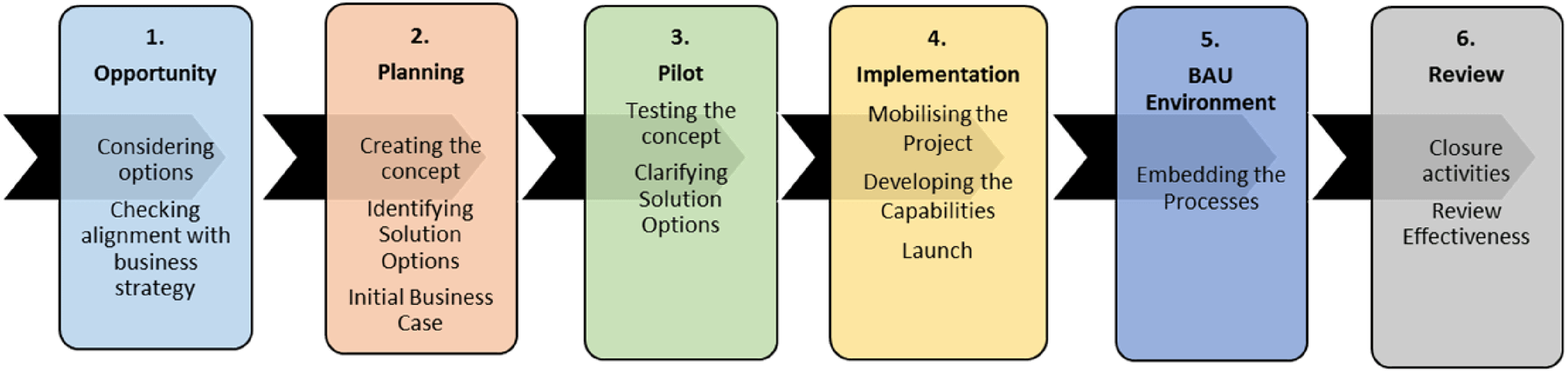
Institute
and Faculty
of Actuaries

Guide to blockchain adoption

03 February 2020

A solution looking for a problem?

Guide to blockchain adoption



1. **Opportunity**

Considering options

Checking alignment with business strategy

2. **Planning**

Creating the concept

Identifying Solution Options

Initial Business Case

3. **Pilot**

Testing the concept

Clarifying Solution Options

4. **Implementation**

Mobilising the Project

Developing the Capabilities

Launch

5. **BAU Environment**

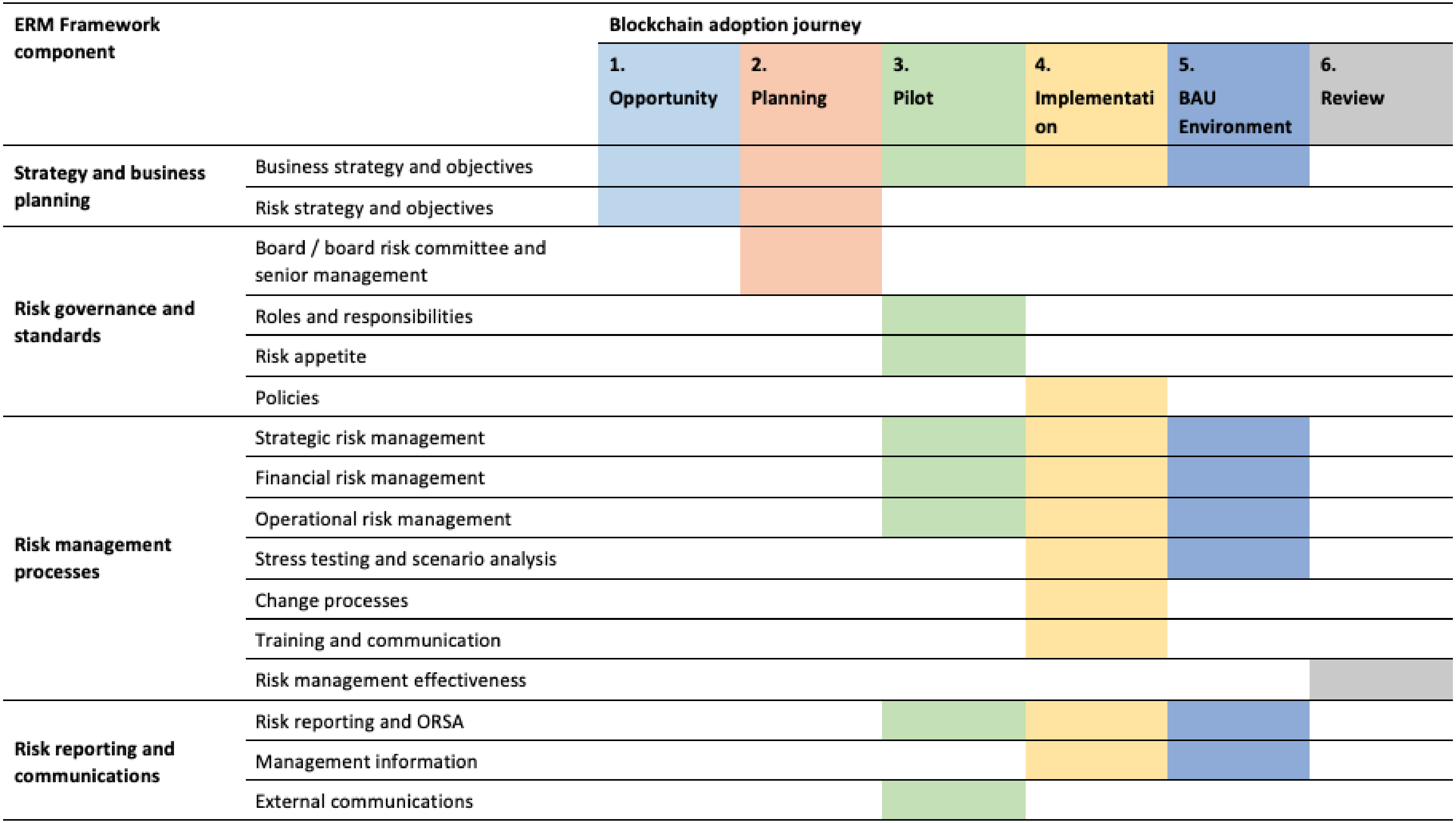
Embedding the Processes

6. **Review**

Closure activities

Review Effectiveness

Guide to blockchain adoption



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			●			

Examples of considerations

Do you need blockchain?

- Is there a need for a shared version of truth among multiple parties?
- Could a shared version of truth be achieved using existing technology?
- Is there a need for decentralisation?

Examples of considerations

Which blockchain platform to use for implementation?

- Permissioned or permissionless?
- Is the platform widely adopted within and outside of the industry?
- If not widely adopted, would there be interoperability issues with other platforms?
- Is the performance of the platform limited by certain design choices?
- Is there a readily available pool of developers for the platform?
- Does adopting a platform which uses Proof-of-Work (PoW) constitute a breach of ESG policy (due to its excessive use of electricity)?

Questions

Comments

The views expressed in this [publication/presentation] are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this [publication/presentation] and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this [publication/presentation].

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this [publication/presentation] be reproduced without the written permission of the IFoA [*or authors, in the case of non-IFoA research*].