British Actuarial Journal (2020), Vol. **25**, e21, pp. 1–15
doi:10.1017/S1357321720000203

ABSTRACT OF THE LONDON DISCUSSION

Understanding Blockchain for insurance use cases: a practical guide for the insurance industry

[Institute and Faculty of Actuaries, Sessional Research Event, London, 3 February 2020]

The Chair (Miss J. K. Grewal, F.I.A.): Tonight's session will be on "Blockchain for Insurance Use Cases: a Practical Guide for the Insurance Industry", as written by the Risk Management Digital World Working Party.

To start, I will briefly introduce myself. My name is Jasvir Grewal and I will be chairing tonight's event. I am a general insurance actuary working for Arcus 1856, which is a Lloyd's of London syndicate backed by Credit Suisse ILS. I am also a member of the Institute and Faculty of Actuaries (IFoA)'s Risk Management Board, which is what brings me here today.

The Risk Management Board promotes, supports and champions the interests of members working in risk management, whether in traditional roles or wider fields. A key part of this role is supporting and promoting the work done by working parties such as the one presenting today.

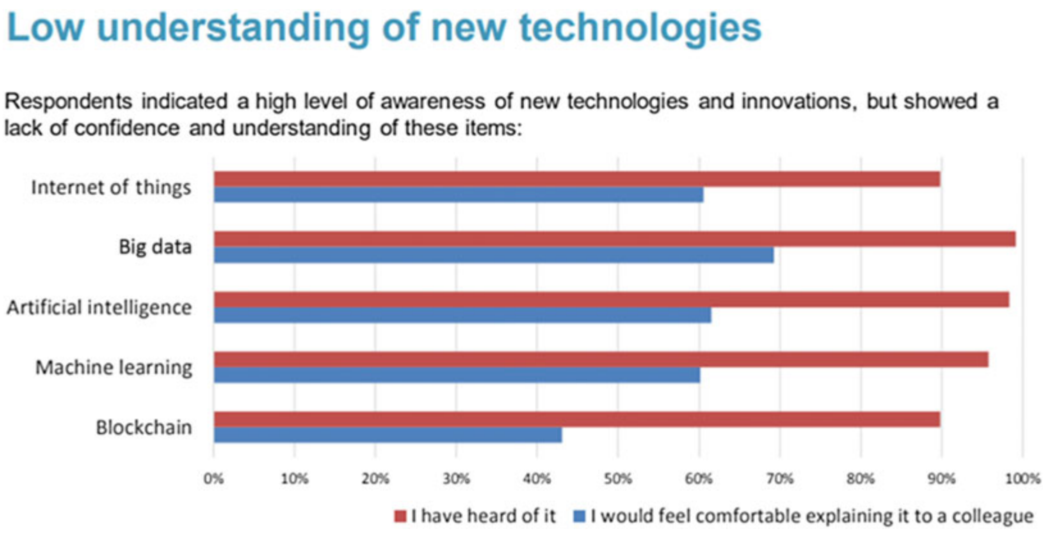
I would now like to introduce our three speakers for this evening. The first will be Darko Popovic. He is an actuary with extensive insurance industry experience, predominantly in risk and actuarial areas, gained through a mix of in-house and consultancy roles. He has worked across Europe, North America and South Africa. He is currently a director at FTI Consulting, focusing on M & A transactions, business transformation, and strategy. He is the current chair of the IFoA Risk Management in the Digital World Working Party.

Following on from Darko, we will hear from Chadwick Cheung. Chad is a life actuary with consulting and industry experience. He currently works at EY as a consultant and focuses on actuarial transformation, modelling and M & A transactions. He is also a member of the Risk Management in the Digital World Working Party and one of the main authors of the paper being presented this evening.

Our final speaker is Zhixin Lim. He is an actuary specialising in asset liability management, model risk management and investment risk. He is currently a senior manager at HSBC, providing investment risk oversight on retail and institutional investment funds. Zhixin led the Blockchain workstream on the Risk Management in the Digital World Working Party and is one of the main authors of the paper being presented this evening. He became interested in Blockchain while working on a Central Bank sentiment analysis model for the Modelling, Analytics and Insight from Data Working Party and has continued to closely follow the area.

Mr D. Popovic, F.F.A.: Before we start, I have to point out the usual disclaimer that these views are the views of the working party rather than the views of the IFoA or our employers.

I want to spend 5 minutes giving an introduction about who we are and why we are presenting on Blockchain. Our working party has been around for a couple of years. We focus on where risk management intersects with Insurtech. We have a mix of IFoA members and non-actuaries. Also, we are not just UK-based. We have members from Ireland, New Zealand and India. I strongly suggest that there is a lot of value in having international people on working parties for the additional perspective they bring.



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:

Figure 1. Low understandings of new technologies.

If you have seen some of us before, it is probably because we had a sessional event in October 2018 regarding our first phase of work. We believe that relevant frameworks have developed quite significantly over the past 10 years or so, mainly due to Solvency II in Europe but also across the rest of the world. At the same time, there has been a huge increase in investment in Insurtech and in focus on digital technology.

Our initial question was whether the development of Ethereum (Blockchain-based distributed computing) frameworks was facilitating, or in any way contributing to, the development of Insurtech.

We produced a report which you are welcome to download. I think that there is also a recording which can be used for Continuing Professional Development (CPD). It is entitled “Improving the Success of Insurtech Opportunities”. There are also some guidelines there about risk considerations relevant to these types of activities.

We carried out a survey across the industry and also relied on interviews with industry experts. I have taken the first graph from a presentation on that study because it shows what led us to focus on Blockchain Phase 2. Figure 1 shows a list of new technologies such as AI and machine learning, big data and Blockchain, among others, about which we asked two questions.

Firstly, we asked whether you have heard of these concepts? Secondly, would you be comfortable explaining them to your colleagues or to a group of your peers? The survey was predominantly sent out to the IFoA community. As you can see from the figure, for the majority of the topics, almost everyone had heard of the concept. For example, 9 out of every 10 respondents had heard of Blockchain at that time.

But when it came to whether respondents felt comfortable explaining the concept to a colleague, the numbers dropped substantially. For Blockchain, in particular, there was a considerable decrease, far more than for any other concept. Only about 40% of the respondents felt that they could explain this to colleagues. It should be noted that this was among a self-selected group who were sufficiently interested to complete a survey on Insurtech and hence represents a likely overestimate versus the actuarial community at large.

So we thought we should try to address this issue in Phase 2. We have not followed the approach of a normal sessional event which tends to have a hypothesis and some results and then a conclusion. Instead, our aim is that after reading our paper, IFoA members will be able to explain

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

to colleagues what Blockchain is and how it works. The paper has a focus on insurance and will cover some other elements more broadly.

We also want people to have the ability to consider the various opportunities and risks involved, at least at a high level. In addition, if they do choose to pursue an opportunity with this technology, at least to have some sort of framework in place that can help them to make the right decisions in this area.

That outlines the broad context of our work. We are going to follow the areas detailed in our paper tonight in this presentation.

If you download the paper, please feel free to store it in the knowledge repositories in your companies and share it more broadly with your colleagues. This research is only worthwhile it if its message is spread and helps people. With that in mind, we will start with the educational aspect.

Mr K. C. C. Cheung, F.I.A.: Just to set the scene and expectations, the purpose of this section is not to deliver a crash course on Blockchain in under 15 minutes. That would be impossible. What I would like to do is to demonstrate how a Blockchain works, highlight the key differences between a Blockchain and a database, and also introduce the key components in a typical Blockchain.

You will have come across many different similar definitions of Blockchain, all of which involve jargon that is difficult to understand. But in plain English, a Blockchain is made up of multiple and identical copies of the same ledger shared by multiple parties.

The status of the ledger is verified and agreed by all parties with a trusted intermediary. I think it is still very difficult to visualise what it is and how it works. So I would like to demonstrate how it works with a very simple example.

In the interests of time, I have preselected three volunteers to help me with this demonstration. The goal is very simple: three of you (the volunteers) are to try to maintain a set of records in this network. The records in this example are solutions to very simple arithmetic questions which I will read out. But there are rules as to how the records can be updated.

What you will do is to compete to be the first person in the network to solve this problem. Once you have solved this problem, put your hand up. I will invite you to announce a solution. You then agree among yourselves if you agree with the proposed solution. Once you have reached agreement, you will then commit this solution to your Notepad.

So, here goes. Trust me, they are not differential calculus!

The first question: what is the answer to $25 + 58$?

83. Do we all agree?

Okay, we now have a consensus. So let us write this down in your notebook.

The next question: what is 12×11?

132. Do you agree? If you do not agree, we will reject this solution and we will try again.

You all agree so let us commit to the record.

The last question: what is the square root of 169?

13. You all agree so let us write this on the Notepad.

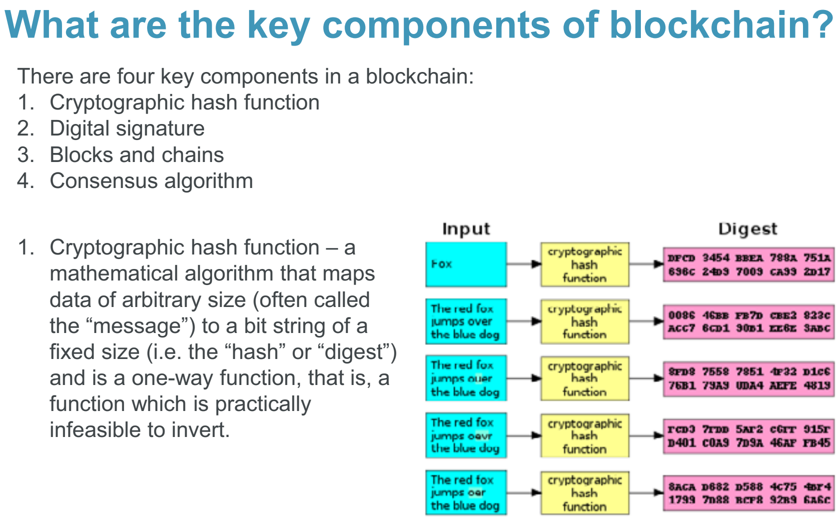
I think this illustrates the point around Blockchain.

What we have done is maintained a shared ledger among the participants of the network. In this example, each volunteer is what we call a node in the network. They also happen to be a miner because they do work to maintain this ledger. Each Notepad is a ledger or a database, if you like, that stores the record. Each person writes to their own ledger, which is identical to any of the other ledgers.

Every ledger is the same and it is shared among all of you. This is a distributed ledger system. Contrast this to a database. In a database, usually one person would hold just one set of master records. They are the administrator and only they can grant access and write on this database.

An important concept is that there is no one single person or entity in a shared ledger network with sole responsibility or authority over how the data are recorded.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press



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 7FDD 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

Figure 2. Key components of Blockchain.

This is decentralisation because the responsibility of maintaining this ledger is shared among all the participants in this network.

This can be contrasted with a database which is a centralised model.

Remember that each participant in this network tries to maintain common sets of records by following predefined rules. These rules are what we call consensus algorithms. In the example, we have illustrated a simplified version of a proof of work (POW) consensus algorithm where each person tries to solve a mathematical problem in order to win the right to commit to the ledger.

Contrast this to a traditional database. You do not need this consensus algorithm because the administrator has the right to grant you access to write to the database.

The downside of a decentralised model is that the network is usually slow. In a database, centralisation means that it is usually much faster and more scalable.

I preselected three volunteers to participate in this network. This is an example of a private Blockchain where the participants are known and trusted to participate in this network. If there were many more people in this network over whom I had no control, then that would be a public Blockchain because everyone would have access to the database of the shared ledger.

Another thing to point out is that we demonstrated a permissioned Blockchain where only selected parties were allowed to write to this ledger. Contrast this to a permissionless Blockchain where everyone is allowed to maintain the ledger.

What the example did not show is how data are secured, which I will explain in the next section.

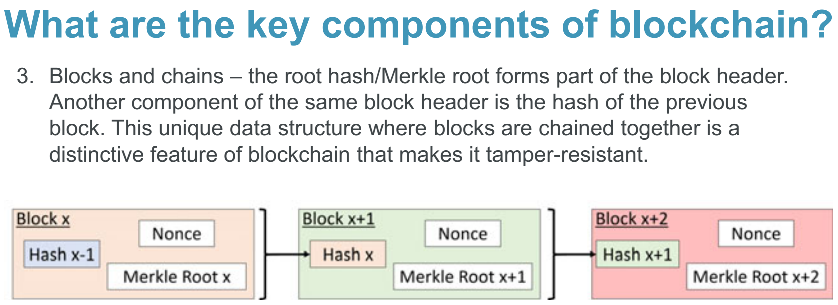
Perhaps the first component of Blockchain that I need to demonstrate is what is called a cryptographic hash function. The hash function is basically a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size which is called a hash.

This is practically a one-way function because it is nearly impossible to invert. If we start with the hash on the left-hand side of Figure 2, it is really difficult to reverse-engineer to find out what the inputs were.

One benefit of using hash functions in a Blockchain is that you can secure data by hashing it. If there was a change to the input data, everyone would know because the hash would be different.

The second very important component of Blockchain is digital signatures. Hash functions and digital signatures are not new, but it is the first time in history that they have been brought together. A digital signature adds another layer of security because it delivers a unique fingerprint

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press



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.

Block x
Nonce
Hash x-1
Merkle Root x

Block x+1
Nonce
Hash x
Merkle Root x+1

Block x+2
Nonce
Hash x+1
Merkle Root x+2

Figure 3. Key components of Blockchain (2).

and provides the assurance that the proposal to change the state of the Blockchain originates from a network node that is authorised to do so.

It makes use of two keys, a private key and a public key. For example, if you wanted to sign off on a transaction, you would need your private key and your data (the transaction) and would put these into a digital signature algorithm. The other party could verify that it came from you using the public key which is known to the whole network. There are various digital signature algorithms, one of which is the Elliptic Curve Digital Signature Algorithm (ECDSA), used by the Bitcoin network.

Data are encapsulated within the Merkle route. A Merkle route is basically a hash of many hashes of data. You can imagine it as a tree where at the very bottom you have data. You hash the data, these hashes come together, and you then go to the very top with one hash. This is stored within the block header. Each block has a Merkle route hash.

Figure 3 shows how blocks are linked together. If we take the Block X + 1, for example, another component within this block header is the hash Block X. In Block X + 2, there is a hash of Block X + 1. They are all chained together. There is another component called Nonce, which stands for "Number Only Used Once". This is just a random number that the miner guesses that will solve the POW mathematical problem. All of these together form the header of the block.

Imagine that we are trying to change something in Block X + 1. For example, that block contains a transaction of £10 and you want to change it to £12. As we said earlier, each hash coming out is different which means that the Merkle Root X + 1 is different. Because the whole thing, hash plus one, is fed into Block X + 2, it is no longer compatible with the POW done in X + 2.

You would immediately see that there is something wrong in Block X + 2. Therefore, to solve this problem, you would need to do POW again on this block and so on and so forth until you have done all subsequent blocks. This would be impossible because of the amount of computation power required.

Finally, POW is not the only consensus algorithm. There are many more, such as proof of stake, proof of authority, proof of disc space, and so on. Each of them functions in a different way. For example, POW is not particularly environmentally friendly because it burns a lot of electricity in order to solve the mathematical problem. Proof of stake does not have this problem as it uses a different mechanism. I am not going to go deeply into these algorithms. I will leave the readers of this paper to investigate further.

Mr Z. Lim, F.I.A.: Before I delve into the cases, I want to present some background information. I was here about 3 years ago presenting a machine learning case study on utilising text data to predict central bank sentiment. I spoke about how influential central banks are. They control the supply of money through monetary policies, and through quantitative easing they create money out of thin air.

Such is their influence that the tone or sentiment in central banks' communications set expectations in financial markets. My model classifies central banks' communications into one

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

of three categories: dovish, neutral or hawkish, with reasonable accuracy. It turns out there is a way to get 100% accuracy in predicting central banks' sentiment.

In December 2019, *The Times* newspaper reported that some traders had access to audio feeds from Bank of England briefings several seconds earlier than the wider public. That was enough to give them a market advantage. The lengths to which some traders would go, and the ethical and legal lines they are willing to cross underscore the influence that central banks have. Each word and each nuance moves the market.

So what is the connection between central banks and Blockchain? If we are going to talk about Blockchain, we should at least touch on Bitcoin – that infamous cryptocurrency. Bitcoin was born out of a response to the influence that centralised authorities have over our monetary system.

When I first heard of Bitcoin I dismissed it, as most people do. I mean, what is this magic Internet money that needs to be mined using electricity? It is not an easy or intuitive concept to grasp. It turns out there is no magic or witchcraft. It is pure innovation, combining various existing technologies into what is now known as Blockchain.

Blockchain has often been conflated with cryptocurrencies, so it is probably worth reiterating that cryptocurrencies are the first application of Blockchain. The technology could be and has been co-opted by the insurance industry for various use cases. Compelling use cases arise from a need to (1) produce a tamper-resistant record that is shared by multiple participants and all stakeholders; (2) reduce operational frictions and cost in the insurance value chain; and (3) remove intermediaries.

The working party paper explores examples of use cases throughout the insurance value chain including data sourcing for pricing purposes, on-boarding customers using digital identity, product management using Blockchain-based securitisation and reinsurance platforms and automatic claims processing using smart contracts.

The paper provides a structured description of these use cases. For each of them there is a problem statement, a description of the Blockchain solution, the benefit of using Blockchain and the main challenges to adoption.

I will be the first one to admit that although these are interesting use cases, they represent only incremental improvement over existing business and operating models. The real game changer of Blockchain for the insurance industry is the pooling of risk between end users without intermediaries. This use case is best explained using the concept of decentralised finance (DeFi) and insurance. DeFi is a loosely defined concept. It is often described as peer-to-peer financial services built on permissionless Blockchain.

Let us unpack that description. By peer-to-peer, we mean there is no middleman in the inception and administration of insurance policies. Under the existing business model, policyholders pay a premium to an insurer, who is trusted to prudently manage a reserve and to pay out claims.

In a peer-to-peer business model, individuals pool resources and enter into a direct agreement with each other to insure against an event, all without the need for a trusted centralised authority.

In terms of permissionless Blockchain, there are two aspects to this: (1) permissionless innovation where anyone can design, build and distribute insurance products; (2) permissionless access where anyone with an Internet connected device would have access to these insurance products. The end result is a wider variety of insurance products that are more transparent, more affordable and more accessible.

To be clear, it is too early to know how this will play out. There are a number of challenges preventing mainstream adoption. Chad (Cheung) is going to speak on the risks and challenges of adopting Blockchain, but there are two main challenges specific to DeFi.

The first challenge is that Blockchain is a relatively new technology. The main tenet of DeFi is that it eliminates centralised authority. You do not need to trust a single organisation or regulator. However, it is necessary to trust the software. Because the technology is so new, smart contracts not performing as intended is still a major risk.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

Additionally, the infrastructure required to support a decentralised insurance system is still not fully built. There is a lack of trustworthy oracles, which are sources of external data, and a lack of a digital identity platform. As a result, decentralised insurance products available now are relatively simple and generally do not need to comply with "know your customer" (KYC) rules.

An example of a product that is suitable for Blockchain is flight delay insurance. It is a relatively simple product which automatically pays out without the customer having to make a claim, using a reliable source of flight delay data.

Another hurdle to mainstream adoption is user experience. While much has been done to make interactions with DeFi apps as simple as possible, these apps are strictly for those who know what they are doing.

For example, consider opening a savings account on a DeFi application built on the Ethereum Blockchain platform. Users first need to obtain a stablecoin, a cryptocurrency that is stable in value. They then need to acquire Ether, the native currency on the Ethereum Blockchain, to be able to pay for transaction fees in sending the stablecoin to the smart contract.

On top of all that friction, users are fully responsible for access to their wallets. Losing access means losing their funds. There is no "forgotten your password" button to resolve these problems.

All of that trouble will earn you perhaps 6% in annual interest. It is not too bad in a low interest rate environment, but probably not worth the trouble for the masses.

So what does the future hold? Despite these challenges, it is far too early to write off the possibility of a highly disruptive Blockchain use case. It is difficult to predict what the killer application is for Blockchain. Human creativity is such that many applications cannot be predicted in advance.

Just think of when Apple paved the way for writing applications for mobile phones. Who would have thought that one of the most popular applications would be a way for you to share colour-graded photos to a group of followers? Now, Instagram is worth more than the original Facebook.

Mr Cheung: I will focus on a few risks and challenges that I find quite interesting.

One of the risks is the cost of adopting Blockchain. Blockchain is a fairly new technology so platforms are still emerging. It means that you need investment and to wait for a while before you see some real benefits.

Another cost is that of finding the right talent. I think it is fair to say that Blockchain talent is rare these days. Universities and education providers are only just starting to educate people in the subject. Depending on the type of Blockchain, there are some specific challenges. These may relate, for example, to the ownership of intellectual property or what it takes to have mass adoption.

Security is a major issue – hacks and mistakes on Blockchain may require drastic measures to make things right. For example, you may need to hard-fork your Blockchain. Forking refers to the branching out of the original Blockchain. If it is a hard-fork, then the new branch takes over to become the permanent Blockchain.

Vulnerability in software code can be exploited. For example, in smart contracts, codes might be badly written. Criminals could steal money from people using malfunctioning smart contracts.

Another security risk is around the data feed into the Blockchain. If it does not originate from within the Blockchain, that is if it comes from outside sources such as an Internet of Things sensor, there is a chance that data on the sensor may be corrupted. This is what is known as the "Oracle Problem".

There are some issues relating to General Data Protection Regulation (GDPR), particularly in relation to the right to be forgotten.

As we mentioned, you can only write on Blockchain and not delete. So how do we deal with the right to be forgotten? There are at least two solutions, the first of which is a traditional one, which is to not store personal data on a Blockchain. The second one is to store hashed values of personal

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

data on a Blockchain, in which case personal data are anonymised. This means there is a case for arguing that this does not fall within the scope of GDPR.

There is also a lack of clear guidance on accounting and solvency capital treatment of cryptoassets, such as cryptocurrencies or asset-backed tokens or utility tokens. For example, how do you find a fair value of a utility token if there is no liquid market? What is the "one in 200" scenario for a utility token? More work needs to be done in this area.

There are lots of legal questions to consider. For example, can smart contracts be recognised as a legal form of contract? Are cryptocurrencies protected by existing regulations or laws?

Finally, in this paper, we have highlighted the challenges around the change of mindset necessary to use Blockchain. Blockchain can be regarded as analogous to a team sport. You need the support of your own organisation and support from across the value chain in which you operate. It is a transformation which is difficult to achieve. This is one of the reasons why there are not many successful real-life use cases. It is not because the technology does not work, but because of issues related to politics and business strategy. In addition, there are always risks in sharing your own data, which may lead to the commercial advantage of others.

Mr Lim: Blockchain is a solution looking for a problem. In most cases, Blockchain is not required and is ill-fitted to the business problem. It is an ingenious piece of technology, but it is being used in a very immature way. Even when Blockchain fits the business needs, its implementation is not well thought through.

With that in mind, the working party has created a guide to Blockchain adoption. The guide is in the form of a timeline and checklist. The timeline represents the key life cycle stages of a Blockchain adoption journey, starting from identifying the opportunities and running a pilot all the way to embedding it as the "business as usual" process.

The checklist represents a suite of issues to consider at each stage of the adoption journey. These are components of a typical enterprise risk management (ERM) framework. There are more than 60 questions to consider. In the limited time available this evening, I am going to focus on two questions and consider them in detail.

The first and most obvious question is: do you need Blockchain? Blockchain is potentially useful if you are looking for a solution that provides a single source of truth among multiple stakeholders. Even so, there is a need to consider whether using existing technology is more cost-effective and easier to implement solution.

For example, could you use Application Programming Interface to make your connections and to collect data from multiple data sources? Why delve into the scary world of Blockchain adoption if you can accomplish the same thing with tried and tested solutions?

The main tenet of Blockchain is decentralisation. Specifically, the maintenance of the shared database and data verification does not rely on a single entity. Do you really need decentralisation? In most cases, you do not. For example, when multiple parties in your shared database are regional entities within a larger global organisation, a centralised solution is a much better choice.

Once you have established that Blockchain is the most appropriate solution, another important consideration is which platform you should implement the solution on. The first decision is whether you require a permissioned or a permissionless Blockchain. On a permissioned Blockchain, you can restrict who sees particular transactions, which is much harder to do on a permissionless Blockchain.

If you need transactions to be observable on a need-to-know basis, a permissioned Blockchain is potentially more suitable. That said, there are clear benefits to permissionless Blockchains. The main benefit is that anyone can join the network easily. This will be useful when you are introducing clients to your solution.

The second consideration relates to the adoption of the platform by the industry. A network is obviously only valuable if there are people on it. People adopt, say, "Whatsapp" over "WeChat" because their friends and families use it. Different Blockchain platforms do not necessarily work

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

with each other. If you are forced to choose a platform that has little adoption, you need to consider how this platform is going to be able to connect to other networks.

You heard about the trade-offs in Blockchain design from Chad (Cheung). The third consideration is whether the design trade-offs are suitable for your use case.

For example, if you need to be able to perform a high number of transactions per second, you need to choose a platform that favours high throughput over decentralisation.

The fourth consideration is the size of the developer pool. You need access to experienced developers who are familiar with the platform. Software platform wars are often won by the platform with the most developers using it for development. So that could be an indicator of the future level of adoption of your solution.

The last consideration is a very topical suggestion from one of the paper's peer reviewers. You have heard from Chad (Cheung) on the POW consensus mechanism. A massive amount of electricity may be wasted in a POW consensus mechanism, like the one used on a Bitcoin network. You need to consider whether adopting such a platform, which wastes electricity, would constitute a breach of your internal or external Environmental, Social and Governance requirements.

These are just examples of consideration that we have in the guide. There are many more, which hopefully will inspire your reasoning when doing an assessment about Blockchain adoption.

If there is one key takeaway from all of this it is that Blockchain is an infrastructure technology that will enable the exchange of value, just like the Internet enables the exchange of information. And, just like the development of the Internet, it is going to take many more years before the impact of Blockchain is felt.

The Chair: The discussion is now open to the floor.

I will start. In your experience, how much insight and input are actuaries adding to Blockchain discussions? If they are not, what is the value that actuaries could be adding here?

Mr Popovic: From what I have seen, “very little” is probably a fair answer. Conversations I have seen have tended to be very much on the technical end of the scale rather than about business decision-making and the use case.

I think that in many ways, actuaries are well placed to understand some of the technical aspects. I am not sure whether they are necessarily better placed than everyone else to undertake the technical work, which feels like a genuine IT problem.

Having said that, I think in our particular area of work, we should be able to assess the implications of some of this for our industry. In that area, I would definitely like to see more actuarial involvement.

The Chair: Would you say the actuarial involvement has been limited simply because risk management of this very new technology has been limited?

Mr Popovic: There are two types of people: those who have explored very deeply into the area in a technical sense and those who have stayed away. As actuaries, we probably have tended to fall into the second category. While we are not necessarily advocating diving right in, I think that there is a happy medium where we can understand how Blockchain works at a high level.

Mr Cheung: From what I see personally, unfortunately I feel that actuaries do not currently play a big enough role within the Blockchain space. There are good reasons for that. Firstly, there is a lack of understanding, which was the motivation for writing the paper that we are presenting. Secondly, the most compelling reason to use Blockchain is to resolve the lack of trust in some situations. Generally, lack of trust is not a major problem for actuaries in the way it can be for the IT department or for underwriters.

Actuaries have been dealing with imperfect data for centuries. They tend not to need Blockchain to solve the problems that they have. Hence, actuaries do not tend to be the first people to become involved in Blockchain.

Having said all this, my view is that actuaries should get more involved. There is good reason for this. Within a Blockchain project, there are many roles. There are roles for developers, roles for

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

testers, roles for project managers, and roles involving understanding the business problem and using the tools that Blockchain offers to solve the problem. Someone needs to sit between these professionals and I feel that actuaries should fill this role. Having spoken to many developers, they do not necessarily understand the insurance problems that we encounter.

On the other hand, there are very few actuaries who understand what Blockchain could offer. If actuaries are better educated in Blockchain, we are then likelier to see more actuaries involved.

Mr Lim: I agree with Chad (Cheung). As companies adopt this technology, especially insurance companies, they will need actuaries to be able to perform the role of a business translator, to be able to understand the technology and how to apply it.

We need actuaries to be able to design products on the DeFi system and to be able to understand the trade-off and the risks.

Dr L. M. Pryor, F.I.A.: I am coming to this as someone who some years ago did a PhD in computer science, in artificial intelligence in particular. Over my career, I have spent a lot of time between the software and actuarial worlds doing a lot of modelling and data analytics.

I think the last two points that have been made are vital. It is really important to look at Blockchain not as a sexy technology, but to think of the business case for its use. As actuaries, I think that the idea of looking at whether to use Blockchain from a risk management point of view is vital.

There are risks involved with Blockchain. Anybody who has spent any time in the software industry knows that it is very difficult to produce a complex system that is bug free.

If the whole premise is that the computer is right and that you cannot question what the distributed ledger says, then you have a problem if it turns out that there were bugs in the system.

There is also a scaling problem related to computational complexity. We are talking about unmanageable complexity here. For anything distributed, you start getting exponential complexity, which is awful.

It is important to consider energy. I noticed that it was correctly pointed out that it was a problem, especially if you are using POW. In fact, as Blockchain is distributed and you have copies all over the place, you are automatically using more energy and creating more emissions.

Finally, of course, the really important risk is the trust issue. A shared version of truth is important but usually the problem with the shared version of truth is not what happens after the data are in the system. It is whether you are sure that the right data got in at the beginning, and Blockchain distributed ledgers can do nothing for that.

I just leave you with the thought that most of the distributed ledger systems we see in operation nowadays are not in FinTech, they are in the black market. They are for groups of criminals who do not trust each other.

I should like to think that even in the fast and loose world that is the modern financial services system, that there is a bit more trust around than that.

Mr Popovic: Thank you for those very interesting points. We have had a number of discussions around the trust point in particular. In many ways, I feel it probably requires a fundamental shift in the way that we see and feel about our own data before we can trust this.

I gained an interesting perspective on this using my bank account as an example. Right now, I hope that I am the only person, apart from the bank, who knows how much money is in my account. However, if something were to happen to that money, no one would know either, except myself and the bank.

Whereas imagine a situation where every single person in this room knows exactly how much money is in my account and receives an instant notification if someone is trying to steal my money. Would I prefer that? I do not know. Maybe if I had lots more money I probably would.

That is such a fundamental shift. Imagine millions of people knowing how much is in my account. I understand that there is encryption and all these sorts of things, but fundamentally I think this characterises the situation. There will need to be a big mindset change to viewing data from that perspective.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

Dr Pryor: The distributed ledger worries me because there is so much duplication and redundancy. From an environmental point of view, this will mean huge wastage.

I wonder if there is an opportunity for a halfway house solution where you have a distributed ledger system that is a lot less distributed, that would give you better replicability than standard database systems, and better robustness against network breakdown without the huge wastage that is involved with a fully distributed system.

Mr Cheung: I have not seen this argument before, but it is a very valid point to consider. Decentralisation for the sake of decentralising operations is wasteful and pointless. I think it comes to a point where more decentralisation is not helpful because there are only so many customers or validators in the network. I think there needs to be a limit to how many distributed and duplicated ledgers there are in the network. But we will see how the industry develops in this respect.

Mr Lim: I would disagree with that, to be honest. One of the main reasons why the system is distributed and decentralised is because that approach removes a single point of attack. There are a lot of redundancies, which is beneficial to the system.

Just think of a self-driving car. If it was not designed to have redundancies, would you take a ride in that car? So I would argue that redundancies in the design is one of the key points of adopting Blockchain.

Dr Pryor: In respect of wasting electricity, the problem is by no means just POW – every aspect of Blockchain uses electricity. If you are doing things a million times, when you could just do them 50 times, then that is a lot of wastage.

Mr Lim: If we are thinking in terms of the usage relative to current conventional databases, yes. But current conventional databases do not provide the features of Blockchain.

Dr Pryor: No, but Blockchain does not provide the features of current conventional databases either. I hope that I am not coming across as too critical. I thought that the arguments you made indicated that you have picked up on all these points.

Mr N. Montagni, F.I.A.: I just wanted to ask a basic question. What would you say if you had to explain to someone who has just a laptop with Microsoft Excel, Microsoft Outlook, and so on, what technical infrastructure is required to implement a Blockchain solution?

Mr Cheung: First of all, you cannot do it yourself. You need a team with the right expertise.

Mr Montagni: Would each stakeholder need to have a computer constantly running? Would it need to have text files for the shared data? Would there need to be some bespoke software on the computer?

Mr Cheung: In terms of the infrastructure of Blockchain, we can classify the layers into three layers. There is an architecture layer at the bottom, a networking layer in the middle and an application layer at the top where it is tailored toward specific use cases. To write all of these layers, you need to have programming knowledge such as JavaScript.

But it is more important first of all to put together your key stakeholders, depending on the use case, such as your customers, your management and your suppliers, because they need to provide you with the data to put into the Blockchain.

The Blockchain is just an infrastructure to share data and exchange values. It is useless if there is not enough data and there is not enough scale. So you need support from the legal system.

Mr Montagni: Is there much that is available "off the shelf"?

Mr Cheung: There are some things available off the shelf. There are providers with cloud-based solutions – a layer that already allows you to write smart contracts and to deploy tools on this Blockchain network, so your customers can start sharing data with each other.

Mr Popovic: At the moment, I think the challenge is this. There are ways you can purchase a website at the moment, you just decide what you want to see and magically it is up on the Internet and it works on everyone's computer. The challenge is that because Blockchain is completely unregulated at the moment, there is not a standard set of rules or ways of implementing Blockchain, as there is with the Internet.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

The problem with using one of these off the shelf solutions is that if company X goes with one off the shelf solution and company Y goes with some other off the shelf solution, and then they want to work together, it may not be possible because of the lack of standardisation.

So, to answer your question, there is a hard way, which is coding it yourself with whoever you are working with on the Blockchain. Alternatively, there is a slightly easier way which is to buy an off the shelf solution. But that way is perhaps a little bit more difficult to scale, particularly for new participants, and to integrate with other ideas. There is plenty online in terms of the real technical details of how to do it and what you need.

Mr Lim: I guess it is worth bearing in mind that Blockchain is simply a network. All you need is a client to connect to it. To write applications for it, all you need is Notepad. If you want to use your favourite Integrated Development Environment, you are more than welcome. All you need is Notepad to write some code.

Miss S. Nanda, F.I.A.: I have a question in two parts. The first is on the triangle limitation, where only two of the three factors have been optimised. A bit more explanation around that would be helpful. One of the factors was scalability. Could you expand on what kind of scale we are talking about – at what point it becomes unsustainable? Let us say that we are doing a Blockchain on transactions. Are we talking about transactions of tens of thousands or millions? At what point does it require an undue amount of computational infrastructure?

The second question I have is the link to the DeFi network. Say that there are challenges in digital identity and certain elements in the network. Is it possible to apply Blockchain in only one part of the value chain? Let us say only to claim settlement in barometric insurance type use cases, or does it always have to be end-to-end, all the way from involvement to the claim? How does it work in practice?

Mr Cheung: I will start with the last question. My view is that the most successful use cases are those that are solving very specific problems in the business. For example, if it is claims management, then it should concern claims and not underwriting. Possibly in the future, there may be a solution where the whole value chain, from policy inception to claims all the way through to reinsurance, is linked together on a Blockchain. That will take time. I am not sure whether we will see this in the next 5 to 10 years. In real life, parts of this value chain have been done on Blockchain, for example, the brokering of reinsurance.

I think that the idea is that developers and companies want to experiment with Blockchain on ring-fenced areas within their business rather than undertake a full-scale adoption at this stage because it is simply not feasible. There is not enough understanding of Blockchain capability and certainly it is difficult to manage or cost if you go with a full-scale solution.

Mr Popovic: From my perspective, the most compelling use case for Blockchain is where you can efficiently address the complexity of data sharing. In terms of scale, there is an efficiency curve and there is obviously an optimal point. If you go past that point, it starts becoming inefficient again. To tell you where the point is, I think, probably impossible without some assumptions and factors. If your use case can address the complexity of data sharing without all the inefficiencies of a centralised standard database, then Blockchain is potentially a good answer to your problem. If it results in so much computation and calculation that it swings you back into inefficiency, then it has probably gone too far.

Mr Cheung: In terms of number of transactions per second or throughput, Blockchain is fairly unlikely to match the performance of a centralised database. You are not going to be able to process hundreds of thousands of transactions per second in the near future.

However, for insurance use cases this is not likely to be a problem. There will not be hundreds of thousands of claims coming through the door on your life policies.

Therefore, in my view, Blockchain as a technology is better suited to insurance than banking because you do need high throughput in banking, whereas you do not need this in insurance. Secondly, as we touched on earlier, I think that there is a bigger problem around trust in the insurance industry. There is always a lack of trust between customers and insurance companies and

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

between insurers and reinsurers. Even though the insurance industry is heavily regulated and overall companies are comfortable transacting with each other, there are always areas where there could be more trust in a system. This is where Blockchain comes in.

Miss Nanda: So were the use cases on the generally accepted accounting principles reinsurance, for example, made possible because there is some trusted body or oracle available in the form of external barometric data to establish trust?

Mr Cheung: My understanding is that the reason for doing that use case was connected to saving costs by reducing duplication of data. Costs would be saved around reconciling claims and sharing data between parties. I have not seen the cost versus benefit analysis, but that is the claim.

In other use cases, the motivation is more around trust. For example, I have seen use cases where the policyholders do not necessarily trust the insurers to execute their claim payments. Hence, a smart contract will provide a fairer way to do that.

Everything depends on the use case problems you are trying to solve using Blockchain. It all comes back to the point that it is not about using technology, it is about solving real-life problems and delivering real benefits.

Just to elaborate further, the insurance use case mentioned above has recently been decommissioned not because the technology does not work but because there is no business argument to support it further. My understanding is that there is not enough support from the counterparties or business partners.

So that is another real-life story where a use case has turned out to be unsuccessful, not because of technology, but because of politics or business constraints.

Mr Lim: I would just like to make a point about throughput. Consensus takes a much longer time to achieve in a permissionless Blockchain. This means you cannot have a high number of transactions per second. In a permissioned Blockchain, the number of transactions can be very much higher.

Ms R. Poliszak: I am a student actuary and I am quite excited by this area. What is the best way for people like me to become involved with Blockchain or other technologies similar to this?

Mr Cheung: I would talk to people within your organisation currently working on Blockchain and see if you can get involved. If not, there are many interest groups out there, who are very keen to share knowledge. For example, there is a club in Bristol where they meet every month to share ideas. In addition, you can search around smart contract developments. I think you will come across applications that allow you to write very simple smart contracts online for education purposes just to gain understanding. As I said earlier, to scale this in the industry, it needs wider support within your organisation and across the value chain, which is really hard to obtain.

Mr Popovic: I would like to draw an analogy with the situation a few years ago when the maturity of data science was equivalent to Blockchain now. What separated those who got relevant jobs from those who did not was really an ability to evidence being able to use the technology. Unfortunately, if you are not doing it in your day job, the only way to really evidence that is by completing other courses or doing relevant things online or joining appropriate societies. It is also a good idea to look for opportunities in your area of work and in your company.

As an example, in our company, like many others, there are various education days. These are days where there is general development and learning for the team. I am sure they would be keen for a presentation on Blockchain among all the other insurance matters, mortality table presentations, and so on. Volunteering to present something is a really good way to obtain exposure.

Mr Lim: Initially, I would recommend reading our paper. Reach out to the practitioners in the industry. They are the people doing the work on Blockchain at the moment. It is a matter of finding them on LinkedIn and reaching out to them. I have personally done that within my organisation.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

Even if your company is not exploring Blockchain, there is nothing stopping you from doing it. All you need to do is look at a few open source projects, explore coding up your own smart contract and publish it on the network.

Mr Popovic: The final thing I would add is that universities are a good place to look. We have had a number of discussions in the working party with a few universities which are researching all sorts of things in Blockchain. For our particular purpose in this paper, the match was not right, but I think that universities are quite keen to have people from industry involved in some of this. We are at the coalface.

Ms L. B. Morgan, F.I.A.: I currently work for the International Labour Organisation. We speak a lot about the value chains in different industries. Firstly, I was wondering if in your research you have come across any use cases where you consider the value chains of other industries where Blockchain has been used to bundle insurance into the value chain. Think of, say, the agricultural value chain. Maybe you want to insure some of the produce in that chain. So you would link that in to the already existing Blockchain.

Secondly, looking at the public sector, have you come across any examples of the use of Blockchain in social security? I have heard that Dubai and Bahrain are using it with their health insurance.

Mr Popovic: I have one example on your first point. I have come across an organisation which focused on the under-insured sector in central Africa. By way of background, there is a prevalence of mobile banking in a number of potential Blockchain use cases. They thought that as there are banking payments and other payments on the Blockchain, why do we not try to do insurance premiums and claims as well? There was both a good and bad outcome from this initiative. The good outcome is that it worked in that there is actually a live product.

The negative outcome is the lack of scalability that they are finding. I guess most of the people in the room have modelled actuarial products at some stage in their career. Often if you want to do a version 2 of a particular product, you copy and paste the relevant tables and change a few parameters. In simple terms, that approach does not work with Blockchain because of the way that it captures the time element. For every time step, the hash from T-1 is captured at time T. You cannot just copy and paste the elements of this approach and start a new product from scratch.

We made the approach work very nicely for one product. But it was hard work and took a long time. We realised that the way we had done it we were going to have to do all the work again for a different life insurance product.

This emphasises that you need to think through quite carefully how these things can work. That is the one example I have.

Mr Cheung: On the second question around public sector services, my understanding is that Estonia is the first country to introduce digital IDs. The idea is to better provide public services like health care. Another example is around the sharing of medical records in China. I do not think that the provider is the government, but most things in China are state-owned anyway. The idea is that it removes the friction around the sharing of data and of course reduces errors in sharing medical data, which is critical.

Time will tell whether these examples can be scaled. I am aware many other countries are exploring the idea of distributing digital IDs to their citizens to provide better services. In the UK, a think tank has written a paper to urge the government to consider Blockchain as a solution for public service.

Mr Lim: I am not sure if this is considered public sector, but a lot of central banks around the world are considering issuing digital currencies. Their whole aim is to move towards a cashless society and Blockchain has been chosen as a solution.

Mr Cheung: I was not going to raise this is an example because it might be politically sensitive, but I think it is worth exploring further. We are never going to see digital currencies such as Ethereum as the currencies in which we trade. CFOs do not want their balance sheet to be volatile on a day-to-day basis. That is not a realistic prospect.

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press

What is realistic is that central banks may issue currencies in digital form. Transactions and trades these days are all done electronically. If they issued digital currencies, then not only it is a better way to combat counterfeit coins but also to be able to track what is going on. I think that countries are exploring this option.

As an example, China passed a law around standardisation of cryptography. Many industry observers view this as a step toward state-sanctioned digital currencies. We do not know whether this will happen but I think it is definitely worth watching in the next 24 months.

The Chair: I will take this opportunity to summarise briefly the discussion tonight. This is a very timely paper. I particularly appreciated that certain concepts were explained without jargon.

The paper comes across as practical, particularly with connections to the ERM checklist as well as the examples of real-world applications of implementing Blockchain technology.

Finally, as with any good actuarial assessment, the sections discussing the risks and challenges involved when adopting Blockchain are very useful and should be kept in mind.

With that, it remains for me to say thank you very much to the audience tonight and for your contributions.

Finally, a big thank you to our three speakers tonight. Let us end the sessional event with a round of applause.

Cite this article: Understanding Blockchain for insurance use cases: a practical guide for the insurance industry. *British Actuarial Journal*. https://doi.org/10.1017/S1357321720000203

https://doi.org/10.1017/S1357321720000203 Published online by Cambridge University Press