LONG FINANCE

Chain Reaction:

How Blockchain Technology Might Transform Wholesale Insurance

July 2016

A Long Finance report prepared by Z/Yen Group

Principal authors: Michael Mainelli and Bernard Manson

Sponsored by

pwc

Foreword

Long Finance aims to 'improve society's understanding and use of finance over the long-term'. Long Finance has researched mutual distributed ledger (MDL, aka blockchain) technology for some time. *Chain Of A Lifetime*, published in 2014, explored the potential for blockchain technology to transform personal insurance. This study of blockchains for wholesale insurance is a natural successor to that work and reflects developments in everyone's understanding of the technology.

Our sponsor, PwC, is active as advisor, technology implementer, and project manager both in the global insurance market and in the use of blockchain and other technologies. PwC believes that there is now a huge potential for blockchain to be a transformational technology within aspects of wholesale insurance, and accordingly it has worked alongside Z/Yen during the course of this study. Z/Yen deployed its first mutual distributed ledger in 1995 and has several blockchain insurance clients.

Long Finance is grateful to PwC for their support which has allowed us to undertake this important and timely research.

Professor Michael Mainelli
Executive Chairman, Z/Yen Group Limited

Contents

Introduction

Mutual distributed ledger technologies – commonly known as blockchain – have the potential to transform the global insurance industry. Still, while there is no doubt that blockchain now looms large on the radar screens of financial services businesses, it's also the case that many businesses are only just starting to get to grips with what is possible. In one recent PwC study[1], 56% of firms said they recognised the importance of blockchain, but 57% conceded they did not yet know how to respond.

Insurers, in particular, are less likely to be familiar with blockchain technologies and applications, the PwC study shows. That's in line with the more general perception that insurance often lags behind other sectors of financial services in modernising its business processes and technology. This reflects the need to work with large clients, provide bespoke cover, and manage specialist risks; these require data-heavy interactions between multiple participants including brokers, insurers, and reinsurers.

BLOCKCHAIN TODAY

It's important to recognise that blockchain technologies are already being applied in insurance. For example, in June Allianz unveiled a prototype for using blockchain in the settlement of catastrophe swaps and bonds. XLRAS, meanwhile, is an application from Blem Information Management that helps firms manage their recoveries under 'excess of loss' reinsurance. This has recently been enhanced with functionality utilising a blockchain to provide immutable transaction evidence[2].

Elsewhere, shared workspace provider Vrumi has announced a partnership with blockchain start-up SafeShare to offer Lloyds of London-underwritten insurance products for the hosts that provide office accommodation in its Airbnb-style business[3]. We've also seen Everledger develop blockchain solutions that help the diamond industry – and its insurers – tackle fraud and theft[4]. Moreover, while practical applications of blockchain may not yet be widespread, there is growing awareness of the capabilities of the technology and how these might be of benefit to the insurance industry.

1 PwC Global FinTech Report (http://www.pwc.com/gx/en/advisory-services/FinTech/PwC%20FinTech%20Global%20Report.pdf)

2 MetroGnomo, www.metrognomo.com, built by Z/Yen and operated with the States of Alderney.

3 Blockchain Insurance Start-Up SafeShare Launches First Blockchain Insurance Solution with Vrumi [http://www.the-blockchain.com/2016/03/17/blockchain-insurance-start-up-safeshare-launches-first-blockchain-insurance-solution-with-vrumi/]

4 Everledger Brings Blockchain Tech to Fight Against Diamond Theft, Coindesk [http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft/]

THE POWER OF THE POSSIBLE

The potential for blockchain to deliver substantial value to financial services is enormous. For example, a recent report[5] from Goldman Sachs estimates that in banking, consistent use of blockchain in KYC/AML checks alone could save $2.5bn of the estimated $10bn global processing costs in the sector.

Not only does blockchain offer the promise of cost reduction and efficiency, but it could also enable revenue growth, as insurers attract new business through higher-quality service. Relationships with stakeholders, ranging from customers to regulators, will improve as errors are reduced and accuracy improved. It may even be possible to reduce capital requirements as insurers on opposite sides of a transaction proceed to agreement more quickly.

Above all, blockchain technologies can help the wholesale insurance sector fulfil its role in underpinning the global economy more effectively. Just as blockchain is being pursued as a force for positive change in other areas of society – from identification for refugees to better public service delivery – it can also help wholesale insurance to discharge its responsibilities for the common good.

Jonathan Howe
PwC UK Insurance Leader

5 Goldman Sachs report 'Profiles in Innovation blockchain' dated 24 May 2016, available at http://www.the-blockchain.com/docs/Goldman-Sachs-report-blockchain-Putting-Theory-into-Practice.pdf

Executive Summary

OBJECTIVES & SCOPE

The goal of this study was to review the wholesale insurance market in order to understand major business processes, to identify where there are perceived problems or inefficiencies, and to analyse where the new technology of blockchain can provide part of a solution.

This study aims to contribute to building a consensus across the industry by involving a wide range of market participants though interviews and a project workshop. This included direct industry entities such as brokers, underwriters, insurers, reinsurers, and specialists such as mutual insurers, and supporting organisations such as trade bodies, regulators, standard setters, and wholesale markets such as Lloyd's.

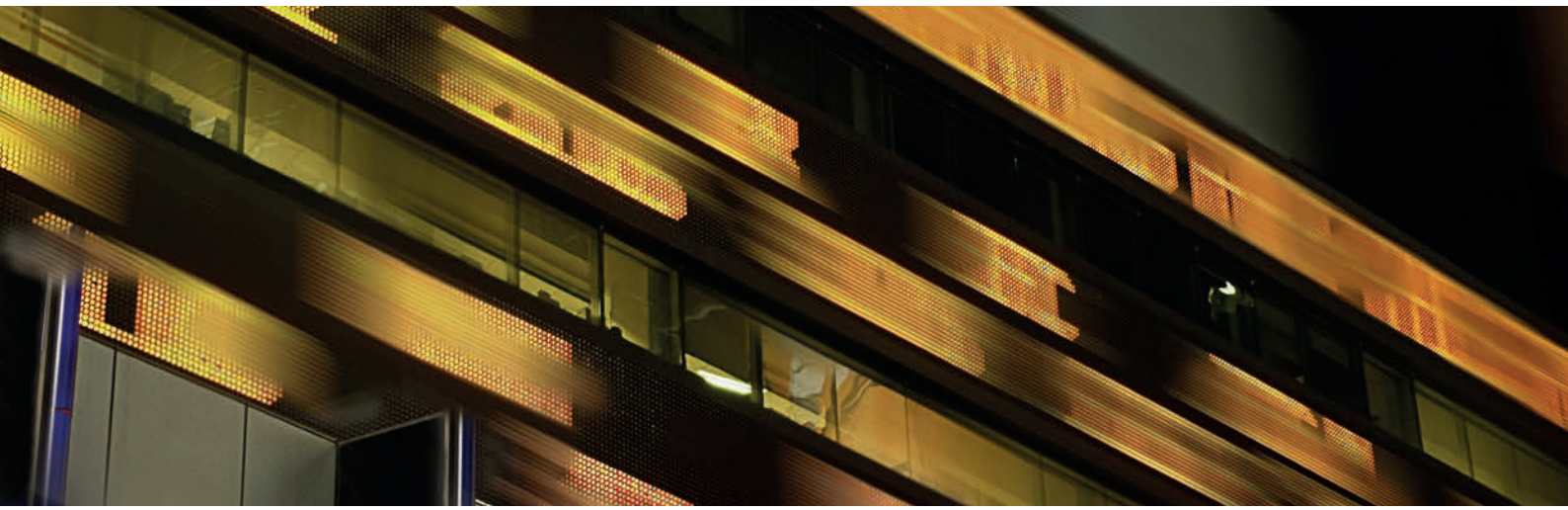
The purpose of the study is to identify practical uses for blockchain technology in wholesale insurance. Practical means having high value to individual firms and relatively low barriers to implementation, without requiring widespread industry consensus or regulatory change.

BLOCKCHAIN DEFINED

A mutual distributed ledger – more simply referred to as a blockchain is a computer data structure with the following capabilities:

- Mutual – blockchains are shared across organisations, owned equally by all and dominated by no-one;
- Distributed – blockchains are inherently multi-locational data structures and any user can keep his or her own copy, thus providing resilience and robustness;
- Ledger – blockchains are immutable, once a transaction is written it cannot be erased and, along with multiple copies, this means that the ledger's integrity can easily be proven.

Another way to think of blockchains is as permanent timestamping engines for computer records. Timestamps can be used to prove that data elements were entered at or before a certain time and have not been altered.



An accompanying output of the study is a technical Proof-of-concept (PoC) developed by PwC's Blockchain Development Lab to illustrate how blockchain technology can be applied to solve business problems in wholesale insurance. The PoC is explained in more detail in Appendix C of this document and may be made available to participants in the survey for the purposes of demonstrating the technology within their firms.

SUMMARY FINDINGS

Blockchain technology is high on the agenda of global insurers and reinsurers, with many of them investing in trials; in our research, smaller organisations also expressed a great deal of awareness and interest.

Most of the interviewees were aware of the key capabilities of blockchain technology: tamper-proof record keeping, the replacement of a central authority with decentralised processes, and the potential for 'smart contracts' – essentially computer code which executes in response to an appropriate trigger.

None of the use cases identified in this report explicitly use smart contracts, although the next stage of analysing more detailed functionality may well include smart contracts to execute processing.

Most of the discussions with respondents focused on the major business processes between participants in the wholesale insurance market:

- placement of insurance (client to broker to underwriter/insurer);
- reinsurance (underwriter/insurer to reinsurer);
- claims management;
- accounting & settlement;
- KYC/AML (viz., a variety of checking processes including Know-Your-Customer, Anti-Money-Laundering, sanctions screening, and determination of ultimate beneficial ownership).

In each of the first three of these areas, our respondents consistently identified problems such as inefficiency, cost, delays, the need to rekey data in unstructured and poorly standardised documentation, difficulties with access to information in ancillary documentation impacting pricing and risk management, and the possibility of error. In accounting and settlement, the key challenges concern agreeing amounts payable, particularly where netting is required. And with KYC and AML, the insurance industry is frustrated by the way in which different market participants have to routinely duplicate processes, leading to cost and delay.

At the technical level, there was significant discussion around the relative advantages of 'unpermissioned' and 'permissioned' blockchains. In an unpermissioned blockchain, such as those used in cryptocurrencies, anyone can access and update the blockchain. As the name implies, everyone has permission. New transactions are added to the ledger and inconsistencies resolved by methods akin to majority voting (albeit implemented by a statistical process), with users having votes pro rata to the resources they commit to the process. In contrast, in 'permissioned' blockchains, a governance structure defines which users can view or update the blockchain and how inconsistencies will be resolved.

The conclusion was that 'permissioned' blockchains were the more appropriate tool for the industry. These mapped better into the control structure required by companies, and would not require, in principle, changes in regulation. Critically, a governance structure allows the blockchain to 'evolve' more easily. With some central governance, the structure of the blockchain can change in response to new business requirements. Further, permissioned blockchains permit greater transaction throughput and significantly lower transaction costs.

Moreover, a permissioned blockchain could be set up to cope with data protection legislation. Records can be encrypted and applications built that meet, for example, the EU's General Data Protection Regulation objectives such as the 'right to be forgotten', user control, and data portability.

Because wholesale insurance is built on a network of risk transfer, many bilateral transactions are effectively part of a global process involving potentially all participants in the market. This means that any proposed process change has to be analysed in the context of its impact on the market as a whole.

A useful way to look at this is to segment changes into three types:

- market level;
- process level;
- point solution.

In practice, some business process changes affect the entire wholesale market – or at least the whole of the semi-autonomous markets that make up the global industry. Others are process level changes, implemented by a group of organisations that change a particular process between themselves. Some changes may be point solutions, implemented by a single organisation.

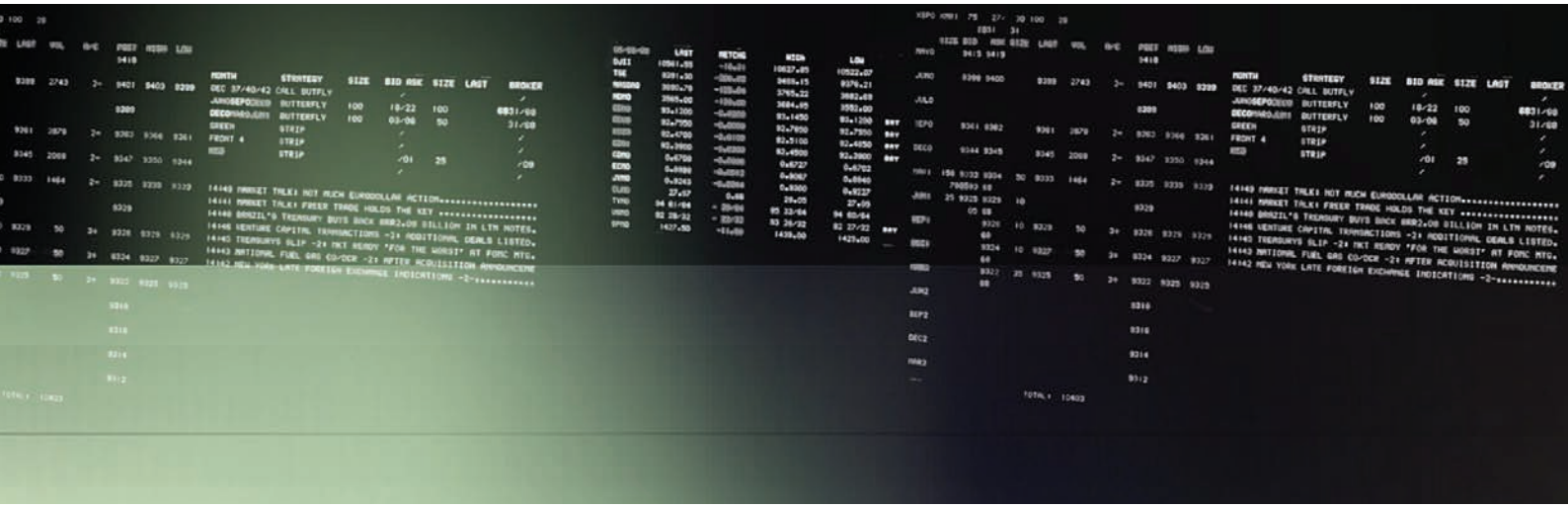
Blockchain technologies will initially deliver change at the process level. The fact that no central authority exists through which changes must be initiated makes it possible for distinct groups of market participants to work together on new initiatives. Through collaboration, trial and experiment, these groups will be able to explore what works (and what doesn't). And over time, the most successful process-level changes will be adopted at a market level.

Because of the structural difficulties of initiating change top-down at market level, the report methodology excluded potential applications which required this sort of immediate 'big bang' change. However, most respondents agreed with the logic that successful process-level change could be a viable medium-term route to stimulating market-level change in both process and standards.

The discussions with respondents around the business processes identified a long list of potential applications for blockchain in wholesale insurance. This list of applications was sifted through two filters, 'barriers to implementation' and 'benefit to business' to create a short list of low Barrier/high Benefit use cases. Although only three applications considered made this short list of potential use cases, the use of a deliberately conservative methodology for estimation suggests that other applications in the long list may have a positive business case when examined in greater detail.

SHORT LIST OF POTENTIAL USE CASES
PLACEMENT AND CONTRACT LIFECYCLE – DOCUMENTATION

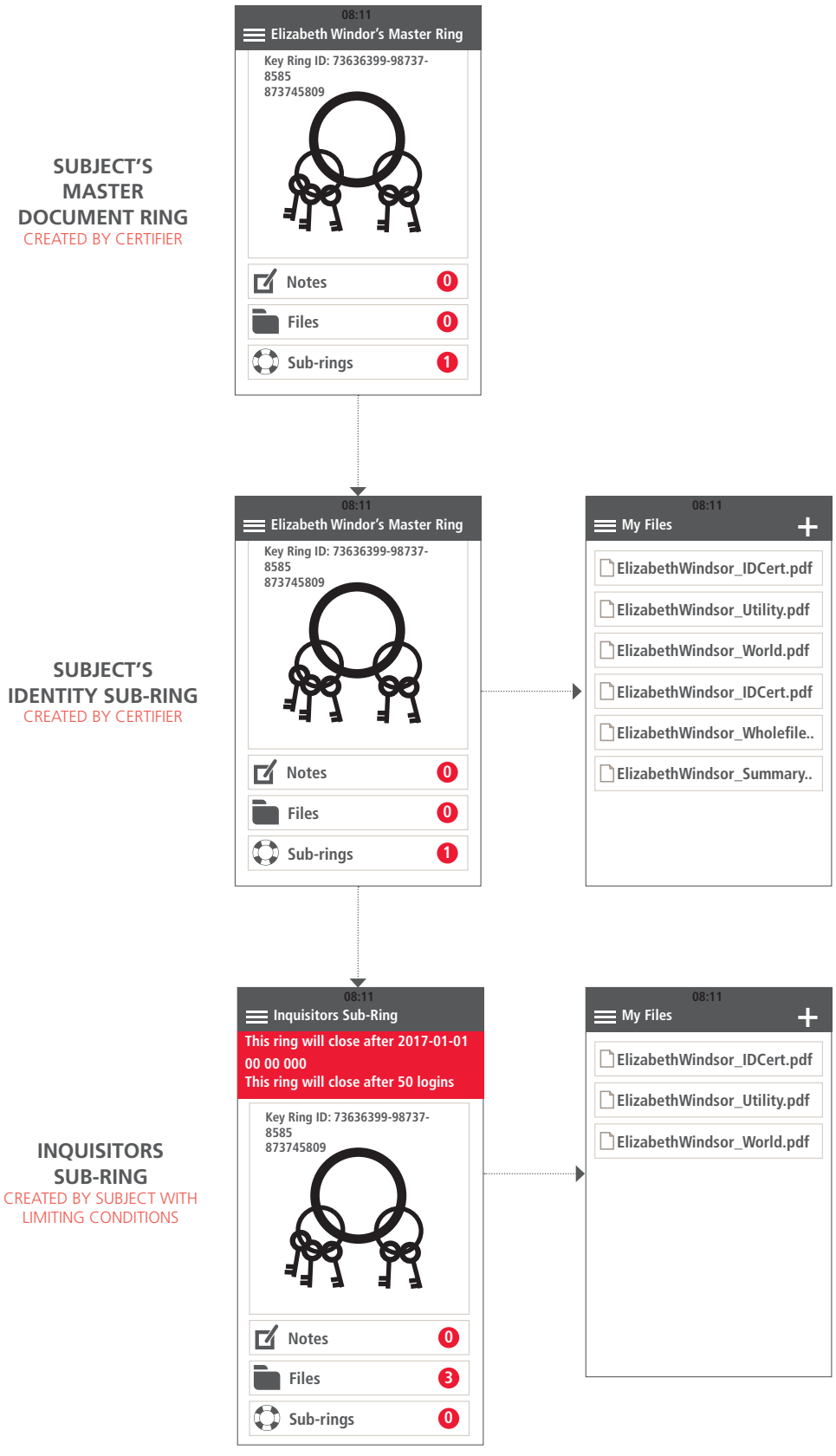
Issue	Wholesale insurance contracts generally reference an ancillary file of paper or electronic 'real life' documents which can be very large and which will be added to throughout the placement process and the contract life. As each participant has to check this file at each stage of interaction, which may for example be several times through an iterative underwriting process and at subsequent points in the deal lifecycle, there can be a heavy processing overhead in simply reconciling against the file presented on the previous occasion.
Proposal	Use a blockchain to store all ancillary contract documents, and share between the broker and underwriters (and as required other participants such as reinsurers and claims agents). This would ensure that every reference to contract documents is consistent and would remove the need for participants to check the same file on different occasions – at most they would have to check the documents updated since the previous occasion. The blockchain would also be viewable by regulators, tax authorities and other participants which would simplify reporting and checking processes. As it would not normally be the case that all participants could read all documents, the applications would need to encrypt certain documents and distribute keys in a controlled way. The actual documents could be included in encrypted form on the blockchain itself or else the blockchain could contain hashes only, with a few nodes holding the documents. This is a minimalist proposal, which would not in itself address the issue of rekeying made necessary by the prevalent use of paper or unstructured electronic documents in the industry. There is no simple fix to this, but the 'spring cleaning' effect of a group of first movers creating a new platform offers an opportunity to impose behaviours which accelerate the move to recognised standards and to the use of source electronic documents.
Benefits	■ Reduced processing cost and time ■ Instant availability of accurate current information ■ Legal certainty ■ Act as a catalyst to accelerate the use within the industry of structured and semi-structured electronic documents rather than scanned paper, thus reducing costs and leading to fewer errors



KYC/AML

Issue	Brokers, insurers and reinsurers have to perform KYC/AML (shorthand for a number of processes including not only Know Your Customer and Anti Money Laundering but also sanction screening and determination of ultimate beneficial ownership) on all of their counterparties, both legal entities and individuals, including third parties due payment under claims. If a client deals with a broker which deals with multiple underwriters, most of which deal through brokers with reinsurers, a single transaction can involve many tens of participants, each of which has to perform KYC/AML along the chain. This multiplicity of repeated checks adds to cost and delays.
Proposal	PwC's Know-Your-Customer Centre of Excellence has built, with Z/Yen, a prototype blockchain-based certified file transfer utility, IDchainZ. A similar utility in wholesale insurance could help to reduce KYC/AML costs significantly. The blockchain records customer personal documents and evidence of validation by the bureau. All documents on the blockchain would be encrypted with only the customer having the keys, thus resolving a set of regulatory issues around privacy and data protection. The customer could then present the blockchain entries together with an appropriate subset of keys to the next firm with which they seek to do business, and this firm would be able to rely on the validation done by the bureau without delay. The overall effect would be to reduce the total cost and time spent on KYC/AML within the industry.
Benefits	■ Reduced processing cost and time ■ Potentially make possible the insurance of time-critical transactions currently uninsured ■ Reduced reputational risk from delayed payment of claims while KYC/AML is carried out on a beneficiary

IDCHAINZ OVERVIEW – HOW SUBJECT OF KYC/AML CONTROLS ACCESS TO THEIR BLOCKCHAIN DATA



CLAIMS MANAGEMENT

Issue	When a claim is made on a policy, each underwriter involved will want to be kept informed of progress. For Lloyd's, only the lead underwriter and immediately following underwriter will be involved in processing the claim, but outside Lloyd's many or all underwriters may wish to be involved. Usually one claims broker coordinates the claims process, but there may be multiple underwriters pursing their own process (which may involve external lawyers) and generating additional costs for themselves and the client.
Proposal	There is scope for creating a blockchain incorporating all documents created in the claims process and making this available to all underwriters and in addition to the client broker and claims broker. This could enable more underwriters to accept the claims process without actively participating, as they would be able to monitor and review as they required. It could also reduce the cost of administration for the claims broker as it would reduce errors and duplication of communication. Depending on the design of the process, the 'Claims' blockchain could be standalone or could simply be an extension of the 'Contract Lifecycle' blockchain described above. In either case there would need to be additional functionality to map and control the claims process.
Benefits	■ Reduced cost ■ Reduced delay ■ Legal certainty ■ Reduced reputational risk from mishandling claims

Each of these use cases can be implemented by firms working together and generating business benefits from improved efficiency of interactions between them. More detailed analysis will be required to establish the costs and benefits of implementing a solution in each area, and the critical mass of participants necessary to make the implementation cost effective.

Undoubtedly there are many other use cases which will be implemented in the future, perhaps including more radical process architectures than this short study could encompass. Nevertheless, we believe that the concrete examples here can serve as a starting point for active analysis and implementation of the technology within the industry.

The proposed next step is to work with an industry consortium group to build a business case for a cross-firm development of one or more solutions, with a view to moving to a joint implementation.

> "CLAIMS MANAGEMENT IS THE FUNDAMENTAL DELIVERABLE IN INSURANCE."
>
> **CEO, INSURANCE ANALYSIS FIRM**

01 Background To The Study

This study was commissioned by PwC in May 2016 to be a rapidly completed analysis of how blockchain technology might impact wholesale insurance. It was conducted over June and July 2016 by a team from Z/Yen working with PwC. The study looked to identify areas where a problem or opportunity existed for which blockchain could be part of the solution. This report highlights those potential solutions which appear to have a stronger business case for development and implementation.

METHODOLOGY

The core of the work was interviewing some 50 market participants and other stakeholders. The focus of the interviews was to identify business processes perceived as needing improvement and to discuss where blockchain technology might be part of a solution. Proposals were presented to an overlapping set of stakeholders for discussion and challenge, and also at a group workshop. There was then a final round of review and challenge with PwC's insurance specialists.

Proposals were filtered to obtain a long list, after eliminating cases where:

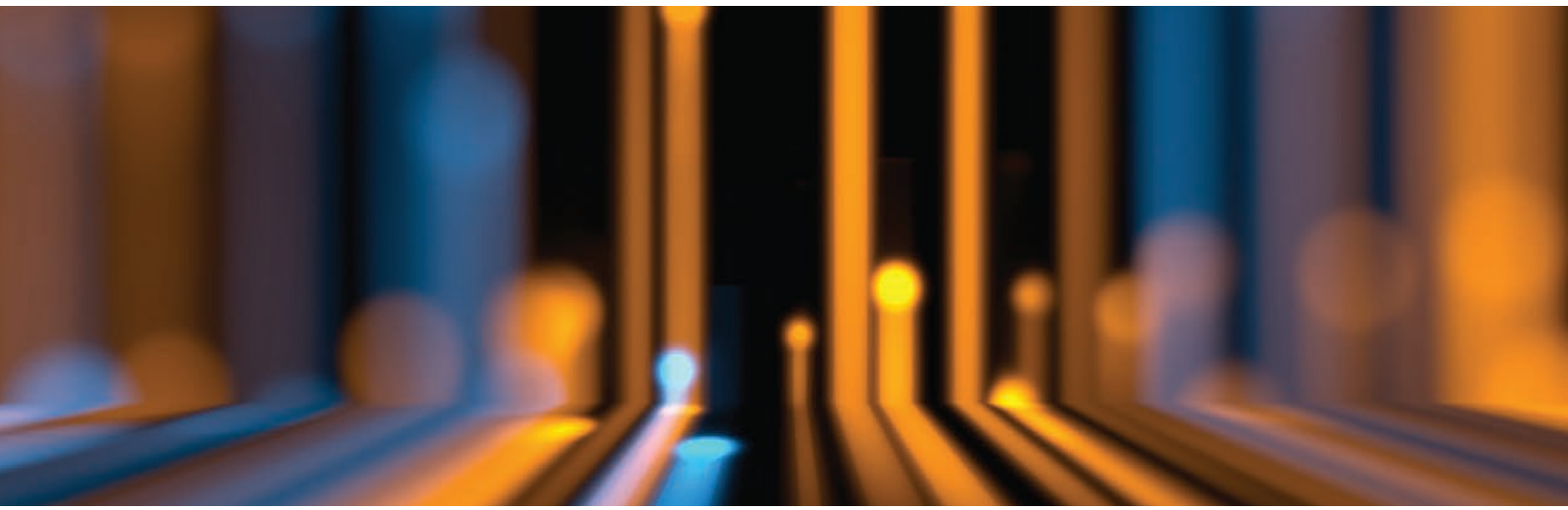
- alternative technology seemed to offer a better capability;
- implementation seemed to demand an immediate market-level solution.

As noted in the summary, exclusion of market-level changes at this stage was in part due to optimism that process-level change could in time catalyse change across a market.

The long list was categorised in a two-by-two matrix with a horizontal axis of 'Barrier to implementation' and a vertical axis of 'Benefit to business'. The definition of low and high barriers and benefits relies upon the view of industry specialists. The priority was to have confidence that the resulting short list was genuinely low Barrier/high Benefit, and therefore the process erred towards excluding doubtful cases from the short list. It seems likely that some of these excluded cases may provide viable use cases for blockchain in the future – as will, undoubtedly, many cases not identified in this report.

As the aim of the study was to be rapid and relevant, rather than outdated and spuriously accurate, subjective estimates were used to assess:

- the size and cost of processes for firms;
- the potential process cost percentages that could be saved;
- benefits other than cost savings – for example increased income or reduced delays;
- complexity of the new process and technology;
- any need to develop distribution and use outside a closed user group within the industry.



The high-level process undertaken does not guarantee accuracy, but we believe that it provides a good starting point for review by wholesale insurers themselves.

Some of the potential risks of blockchain are considered within this report, but clearly with any technology implementation there are hard-to-find risks and unintended effects. Any business case will need to look at risks in context.

PARTICIPANTS AND ROLES

The process chain in wholesale insurance is from the client through to the underwriter, mediated by one or more brokers, with the underwriters themselves managing some part of their risks through contracts with reinsurers. The major participants in the market are:

- clients
- brokers
- underwriters
- global insurers
- reinsurers
- capital providers

We interviewed participants from all of the above categories. As the aim was to understand issues around business processes, the roles covered included Chief Operating Officer, Chief Underwriting Officer, Chief Financial Officer, Chief Data Officer, Head of Digital Innovation and Head of Reinsurance Contracts. To complement these direct industry participants, we also interviewed a wider group of stakeholders including regulators, service providers, advisors, and trade bodies.

TECHNOLOGY & CENTRAL THIRD PARTIES

Wholesale insurance is a critical enabler of business and trade globally. By allowing companies and governments and their agencies to manage their risks, it increases the amount of business activity which can take place. Less insurance, smaller economies.

Wholesale insurance differs from capital market finance in some important ways. First, insurance is a 'promise to pay in future', not an asset transfer today. Second, while capital markets trade on information asymmetry, insurance is theoretically a market of perfect information and symmetry – you have to reveal everything of possible relevance to your insurer, but each of you has different exposure positions and interpretations of risk. Third, wholesale insurance is 'bespoke'. You can't trade your insurance cover with someone else. These three points lead to a complex set of interactions among numerous parties.

Historically, wholesale insurance has been a slow adopter of new technology compared with other sectors of financial services. Clients,

brokers, underwriters, claims assessors, valuation experts, legal firms, actuaries and accountants all have a part in writing a policy, not to mention handling subsequent claims. An often-heard remark, reiterated by many respondents in the research for this report, is that wholesale insurance processing is inefficient. A challenge for the industry is that its participants simultaneously compete and cooperate, with complex information flows between participants being a key part of many business processes. Therefore, implementing effective change often requires resolving complexity and getting agreement across a variety of market participants to target dates. Historically, this has typically required a long period of negotiation and compromise, followed by an implementation timetable to suit the slower participants.

As well as technology, financiers often use central third parties to simplify processes. People use central third parties in many roles in finance, for settlement, as custodians, as payment providers, as poolers of risk. Central third parties perform three roles, to:

- Validate – confirming the existence of an item to be traded and membership of the trading community;
- Safeguard – preventing duplicate transactions, i.e. someone selling the same thing twice or 'double-spending';
- Preserve – holding the history of transactions to help analysis and oversight, and to be available in the event of disputes.

Many wholesale insurers are concerned about a central third party who might hold their information to ransom. They want to avoid natural monopolies, particularly as access to agreed information is crucial over multi-year contracts. Also, a central organisation that must be used for messaging might impose excessive monopoly rents. Many historic market reforms have left monopolies in place or created new ones. Because blockchains provide pervasive, persistent, and permanent records without central ownership, they lower the barrier to re-engineering central third-party functions.

Blockchains securely store transaction records in multiple locations with no central ownership. They allow groups of people to validate, record and track transactions across a network of decentralised computer systems with varying degrees of control of the ledger. In such a system, everyone shares the ledger. The ledger itself is a distributed data structure held in part or in its entirety by each participating computer system. Trust in safeguarding and preservation moves from a central party to the technology.

Blockchain technology offers new capabilities for firms to interact with each other. In any transaction where multiple participants exchange data, a shared common view of data eliminates the need to duplicate data entry and to reconcile between multiple individual data silos. A blockchain provides a 'logically central but physically decentral' database, eliminating much inter-firm messaging. This allows more efficient workflow for all parties, without the need for a central authority and without a 'single point of failure' risk.

Emerging techniques, such as 'smart contracts' (executable code stored in the blockchain, also known as 'sprites') and decentralised autonomous organisations (complex sets of code that emulate a business organisation), might in future also permit blockchains to act as automated agents. An example of a smart contract might be a deposit product which triggers repayment with interest on a particular date, or a weather insurance contract which makes a payment when a particular weather station records readings above a trigger rate. In either case there would have to be an interaction with a clearance agent to make the physical payment.

Blockchain offers the potential for making process-level improvements among a 'coalition of the willing' as opposed to having to implement simultaneous market-level change across an entire industry segment or geography. It is therefore a particularly exciting technology to investigate within the insurance industry.

IMPLEMENTING TECHNOLOGY

Blockchain is a technology – just like the jet engine or a hammer and nail. To use blockchain, it effectively requires identifying where it will solve a problem and repay its cost of implementation and running, taking into account any side effects its use generates. Given the industry structure described above, the assumption of this report is that it will not be possible to introduce blockchain where this requires an immediate market-level initiative across the industry. The focus is on identifying use cases which provide incremental benefits to individual firms when implemented as a process-level change across a relatively small number of market participants, in the belief that successful process-level change will in time stimulate market-level change.

There are already scattered examples of the use of blockchain in wholesale insurance. For example, XLRAS is an application from Blem Information Management Ltd which is used by several reinsurers and insurers to manage their recoveries under 'excess of loss' reinsurance. This has recently been enhanced with functionality utilising a blockchain to provide immutable transaction evidence[6].

In a commercial environment, technology will be introduced only when it satisfies a business need. This means that it has to help solve an important problem better than alternative technology, and must generate a benefit greater than the cost of implementation. In addition, it must not generate side effects, such as new risks, that outweigh the benefits created.

This research worked backwards from business issues to technological solutions. We asked senior managers in operations, risk, and business roles to identify business processes needing improvement, and discussed with them where blockchain technology might form part of a solution. From this initial list of potential use cases we filtered out those where an alternative technology seemed to be at least as good, and those where implementation seemed to demand too large a coalition of firms. The remaining cases became our long list. We filtered this list in turn by making a best-efforts estimate of a business case, and the most positive outcomes gave us the short list of use cases presented in the executive summary above.

Our focus was on identifying use cases that are good enough to motivate firms to work together in more depth with the intention of implementing if they are investable. We do not assert that we have identified the three best use cases for the industry, but we are confident that we have identified three cases meriting serious investigation by brokers, insurers and reinsurers.

6 MetroGnomo, www.metrogxznomo.com, built by Z/Yen and operated with the States of Alderney.

02 Blockchain Technology

"A BLOCKCHAIN IS A SUPER AUDIT TRAIL"

RISK DIRECTOR, INSURER

"THERE IS NO SUCH THING AS A GENERIC BLOCKCHAIN."

IT INNOVATIONS MANAGER, REINSURER

CHAINS OF BLOCKS

A mutual distributed ledger – more simply referred to as a blockchain – is a computer data structure with the following capabilities:

- Mutual – blockchains are shared across organisations, owned equally by all and dominated by no-one;
- Distributed – blockchains are inherently multi-locational data structures and any user can keep his or her own copy, thus providing resilience and robustness;
- Ledger – blockchains are immutable, once a transaction is written it cannot be erased and, along with multiple copies, this means that the ledger's integrity can easily be proven.

Another way to think of blockchains is as permanent timestamping engines for computer records. Timestamps can be used to prove that data elements were entered at or before a certain time and have not been altered.

In a blockchain the data structure links a unique, computer generated signature, 'hash', of the previous record into a new record. Thus, the mechanism for adding new records must ensure:

- updated blocks are broadcast quickly to all users of the blockchain;
- individual users being unable to access the system does not stop the process of adding new records;
- where there is a conflict such that there are two incompatible versions of the blockchain broadcast at about the same time (a 'fork'), there is a process to ensure that the situation is resolved quickly and the integrity of the blockchain is maintained.

'PERMISSIONED' VERSUS 'UNPERMISSIONED'

Oxford Dictionaries define a cryptocurrency as "a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank". Cryptocurrencies – Bitcoin in particular – stimulated the current interest in blockchains, which are a core component of the digital technology making cryptocurrencies work.

A blockchain which can be read or updated by literally anyone, such as a cryptocurrency, is termed 'unpermissioned'. In contrast, a 'permissioned' blockchain can be updated or validated only by authorised users within set governance rules. Owing to the detailed properties explored below, the assumption in this report is that any blockchain used in wholesale insurance will be permissioned.

Permissioned blockchains need some form of governance that guarantees admission and expulsion from the community of authorised users and defines how updates to the

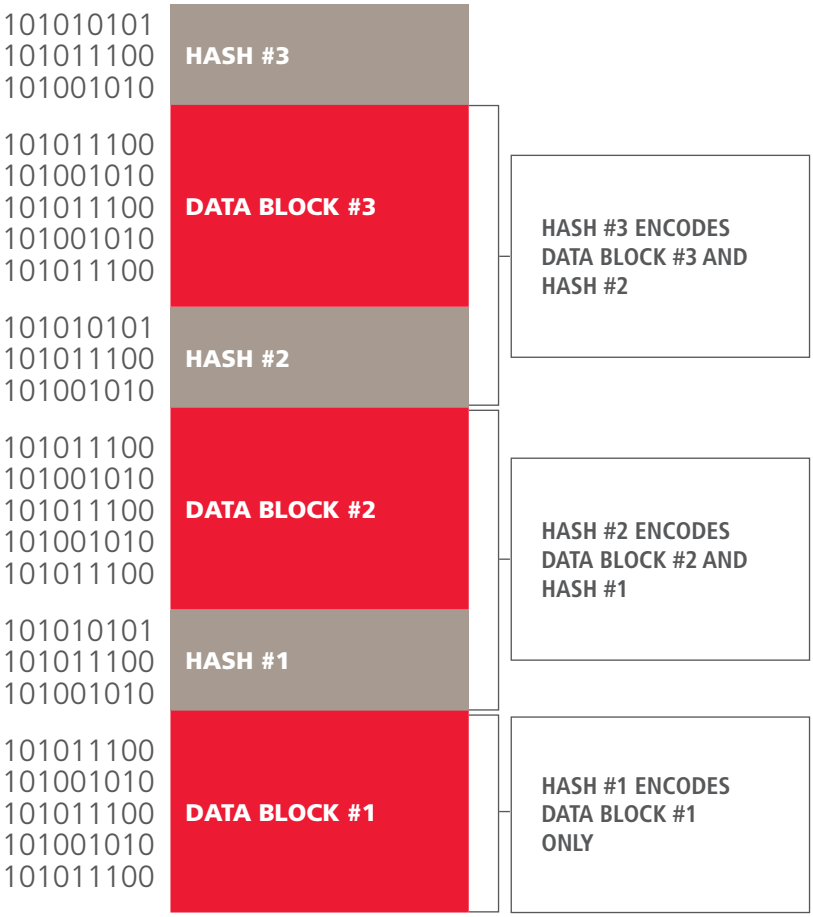
blockchain are made and validated. Permissioned blockchains have a significant advantage in cost and speed. They can also provide an ability to 'evolve', for example providing efficient and timely changes in the structure of the blockchain itself or in supporting processes, as new business or regulatory requirements emerge. Finally, a permissioned blockchain provides a structure for meeting legal and regulatory requirements to 'contract with someone'. In a regulated environment, there may need to be a 'user of last resort' which maintains a current copy of the blockchain and contracts to rebroadcast it if required.

A blockchain can also be 'public' or 'private'. A 'public' blockchain is available for everyone to read. Within the 'public' structure, users can encrypt information placed on the blockchain, so that although everyone can see the encrypted version only those who receive the key can actually read the information. A 'private' blockchain is visible only to authorised users.

Blockchain is generally thought of as useful in applications where multiple participants need to agree a regularly changing dataset. However, it can also be useful within one organisation to provide a tamperproof audit trail for external review or to simplify processes between multiple internal areas.

Appendix B gives further technical description for those interested, including more information on cryptocurrencies.

SCHEMATIC OF BLOCKCHAIN



03 Wholesale Insurance Markets

Insurance is a key enabler of business and trade globally. For example, the OECD explicitly recognises: 'the essential social and economic role [insurance] plays by covering personal and business risks'[7].

'Wholesale' as it is used in relation to the insurance market is generally restricted to transactions which are individually large or complex or are for large organisations. The statistics given below are reported with reference to this definition. Separately, insurers underwrite or reinsure portfolios of individual policies such as motor, health, or properties. Although this is generally described as retail business, it can lead to exposures with characteristics in common with wholesale and which raise similar processing issues.

The global wholesale insurance market is large; in 2013, it wrote £307 billion of Gross Written Premium (GWP), together with an additional £117 billion of GWP in reinsurance[8]. Unsurprisingly claims are also large. According to analysis by Aon Benfield[9] in 2015, in the previous 26 years there were 13 individual corporate liability settlements in excess of USD 10 billion, one every two years.

Within the global wholesale market, the London Market for specialty commercial business has a prominent position. This grouping of insurance businesses comprises about 300 broker and underwriter members of Lloyd's Market together with global insurers and reinsurers which commit capital to wholesale business in London. In 2013, about £60 billion of GWP was written in the London Market[10] . The commercial insurance market in the USA is about twice the size, but is dispersed across many centres; it is also largely domestic, while in the London Market two thirds of the premium is from overseas. The largest reinsurance centre is Germany, with £28 billion of GWP in 2013, about twice that of London[11].

The basic economic function of insurance is the transfer of risk. Clients pay insurers to assume certain types of risk. A simple example is property insurance. The client pays a premium for cover for a year and if the property burns down the insurer pays the loss that the client has incurred. The loss covered will be defined in the contract and could be, for example, the rebuilding cost to restore the property to its original state plus an amount to compensate the client for its cost of alternative premises during rebuilding. Another example is marine insurance, where the client again pays a premium and the insurer takes on the risk of repaying the costs if a ship sinks or a cargo is lost.

Without such a transfer of risk, any major fire, shipwreck, or other crystallisation of risk could bankrupt a company; if there was no insurance,

7 Source OECD website: http://www.oecd.org/daf/fin/insurance/globalinsurancemarkettrends.htm

8 Source 'London Matters: The Competitive Position of the London Insurance Market', Boston Consulting Group and the London Markets Group, November 2014.

9 Aon Benfield Insurance Risk Study 10th Edition 2015 'Global Insurance Market Opportunities' page 32

10 Source 'London Matters: The Competitive Position of the London Insurance Market', Boston Consulting Group and the London Markets Group, November 2014.

11 Source 'London Matters: The Competitive Position of the London Insurance Market', Boston Consulting Group and the London Markets Group, November 2014.

companies could not afford to carry risks which were large compared with their own capital. Insurers are able to support the risks they carry because they hold large capital and manage their risks on a portfolio basis, so that there is no single concentration of risk whose crystallisation could bankrupt them. As a result, insurers in aggregate need less capital to carry risk than would individual companies each carrying their own risk. An important tool for insurers to manage risk is reinsurance; this is effectively the same as insurance, but in this case the client is an insurance company which pays a premium to a specialist reinsurance company to assume the risk.

Because insurance and reinsurance functions in a global market, concentrations of risk can be spread over a large number of companies across different geographies. This means that the claims for even the largest insurance event such as a major earthquake can be paid for out of the capital of the chain of insurers and reinsurers involved.

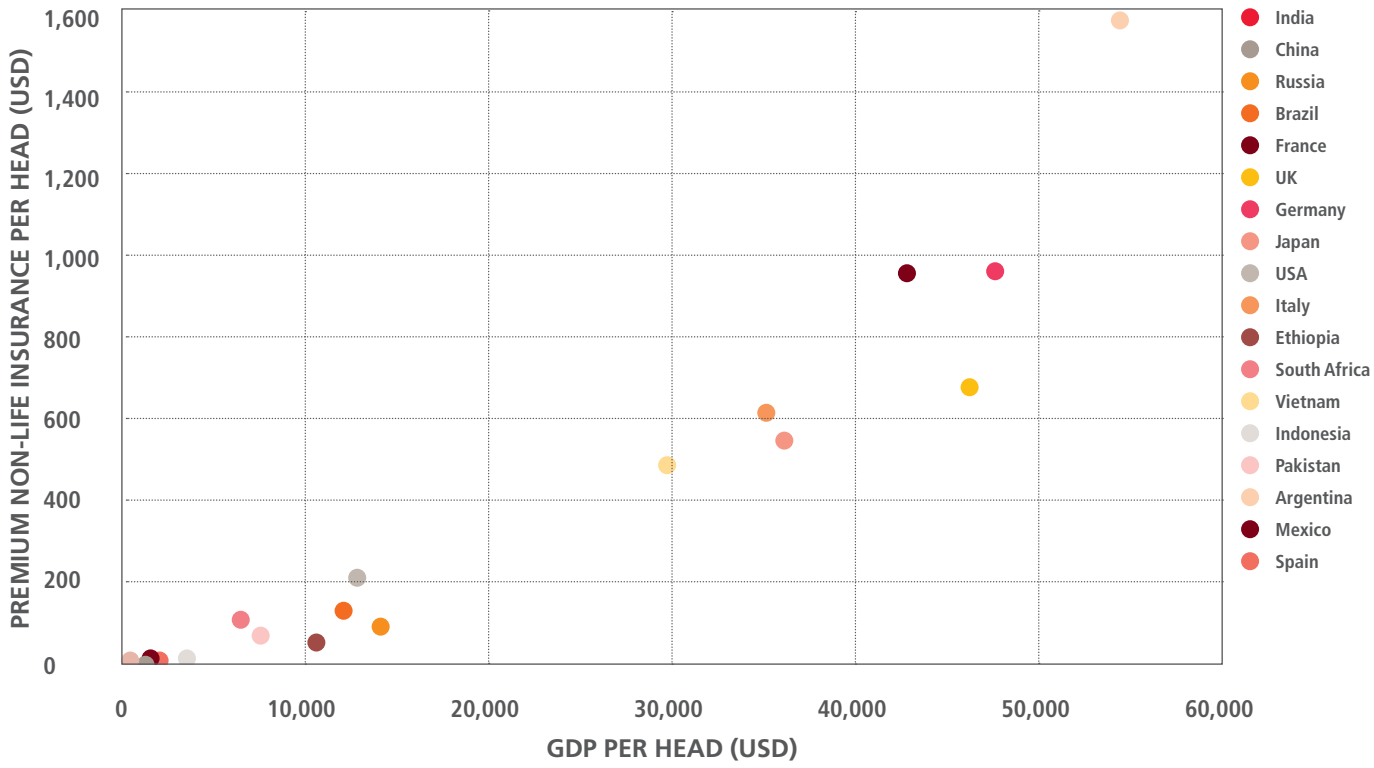
Insurance is most embedded in mature economies, meaning that the opportunities for growth exist disproportionately in the developing world. This is material for a report looking at ways of using new technology, given the difficulty of distributing insurance in countries with limited infrastructure.

To illustrate this opportunity: a simple comparison of different levels of insurance per head in economies at different stages of development suggests that there is a clear trend: as GDP per head increase, insurance premium per head increases faster.

Unfortunately, statistics on wholesale insurance per country is not readily available, so the scatter diagram below uses 'non-life earned premium' as a proxy[12].

This illustrates the massive potential for increased levels of insurance in the developing world as GDP per head increases. It also suggests that for countries with lower GDP and insurance premiums per head, technology such as blockchain could help us meet this unmet demand by addressing distribution challenges.

NON-LIFE INSURANCE PER HEAD VERSUS GDP PER HEAD REPRESENTATIVE COUNTRIES 2014



12 Source Verdict.financial.

BLOCKCHAIN AND INSURANCE: IDENTITY, TIME, SPACE, AND MUTUALITY

Chain Of A Lifetime concluded that four themes applied to blockchain applications in retail insurance; Identity, Space, Time, and Mutuality. These four themes also resonate in wholesale insurance.

Identity – Blockchain offers the possibility of a portable, secure, globally available store of personal or legal entity data. This could greatly simplify KYC/AML processes, reducing delays and costs. Improved certainty on identity could also reduce the risk of fraud.

Space – Blockchain allows resilient interaction between dispersed participants. In the context of wholesale insurance, this could widen the network of insurers involved in a transaction, allowing faster adjustment across markets. Combined with other emerging digital technologies it could also allow more precise, on-demand products, such as insuring a cargo container on a single leg of its journey.

Time – By providing an immutable permanent record, blockchain can enable new capacities within insurance. For example, an insured client could maintain a real-time blockchain register of warehouse movements to prove the amount insurable at all times, thus allowing a new type of insurance covering actual risk rather than a maximum risk. Separately, by providing a 'super audit trail' a blockchain can improve legal certainty where parties dispute the timing of events.

Mutuality – This is an area in which the power of blockchain manifests itself in several guises in wholesale insurance. Use of the technology enables entities to interact without a central processor, reducing the need for 'natural monopolies' which tend to extract excessive rents.

Much of the processing cost base of wholesale insurance arises from simply keeping track of ancillary contract documentation, and making sure that records are consistent between client, broker, underwriters, reinsurers, and claims managers. Blockchain provides a natural technology for controlling large complicated files which change over time, to create 'one version of the truth' timestamped and tamperproof and available to all, allowing processes which reduce errors, delays, costs, and legal uncertainty.

One model of wholesale insurance is the mutual insurance company, as discussed in the box below for mutuals in the shipping industry. Barriers to creating such arrangements for other sectors undoubtedly include factors beyond technology, but blockchain does offer the possibility of standardised processes to simplify the creation and running of new mutuals.

One important feature of the example of P&I clubs is that it shows the possibility of alternative structures arising in wholesale insurance once the environment becomes favourable.

P&I CLUBS

An existing model of mutual insurance in the wholesale market is Protection & Indemnity (P&I) insurance for ship owners and operators.

P&I clubs emerged in the mid-1800s to fill the gap of conventional insurance over covering third-party claims. These cover a wide range of liabilities including personal injury to crew, passengers and others on board, cargo loss and damage, oil pollution, wreck removal, and dock damage.

Clubs provide a wide range of services to their members on claims, legal issues and loss prevention, and often play a leading role in the management of casualties, as well as mutual reinsurance amongst themselves. Each year, all club members must pay a certain amount in based on activity. If the claims exceed the pooled money, the members must add supplementary money. Surplus money is returned to the members or applied toward a future year.

Despite their 19th century origin, P&I clubs are still very much in use today, accounting for 90% of the world's sailing tonnage.

04 Reactions

AWARENESS OF BLOCKCHAIN TECHNOLOGY AND ACTIVITY AMONG COMPANIES

Almost all respondents were aware that blockchain technology offered the potential of new capabilities for processing in wholesale insurance. A majority had been to a course or a talk on blockchain or had read articles on the subject, although only a few of those in non-technical roles felt they had a good grasp of the capabilities of the technology. The large insurers and reinsurers typically had active programmes to look at the potential of the technology, with a view to identifying use cases and producing proofs of concept.

Some initiatives are in the public domain. For example, Zhongan Insurance in China plans to release a platform based on blockchain technology which will enable peer-to-peer and mutual insurance entities. Zhongan states that its cloud-based IT architecture also incorporates blockchain as part of its core processing. The global insurer Allianz has announced a catastrophe bond/swap prototype which uses blockchain and smart contracts for settlement. Furthermore, a systems supplier, Blem Information Management, has added an application using blockchain technology for authoritative timestamping to a system currently in use by reinsurers.

IMPLEMENTATION JOURNEY

Many respondents emphasised the difficulty of showing a viable business case for a process change using new technology in an environment where operational benefits often came from improved interactions between firms rather than from improved internal processes. Each firm had its own process of investment appraisal and prioritisation to decide which operational changes were implemented. The decision process progressed from strategic priorities, to budgets and plans, and then to prioritisation of individual investments.

Firms seek solutions, not technology; the process is driven by finance and risk considerations. Most respondents confirmed that they included improving operational efficiency, measured as the ratio of expense to premium income, in their strategic priorities. There are many other factors, such as risks mitigated, effectiveness, and wider business objectives. Once budgets are set, investments are often categorised as:

- necessary, because of regulation or commitment to a membership organisation (such as Acord or the Lloyd's Market);
- investible, high net present value (NPV) due to cost savings or attracting significant additional business; or

- strategic, aligned with a move to a target systems architecture (including decommissioning legacy systems).

Since much of the processing in wholesale insurance involves information exchange with other firms, there is a network effect whereby the greater the number of firms adopting a change, the greater the cost saving for each firm. This gives an incentive to agree such changes with as many other firms as possible, but this is counterbalanced by the difficulty of agreeing detailed changes and coordinating implementation, which grows with the number of firms involved. As well as this structural difficulty, several respondents expressed the cynical view that some large participants had a vested interest in maintaining the status quo.

Respondents generally agreed that while change was difficult it was not impossible, and that if a process change agreed together by a small group of market participants could be shown to have a positive business case and a credible route to implementation then their firm would be interested in taking part.

POTENTIAL SCALE OF BENEFITS

Respondents pointed out that although their main interest in blockchain arose from the potential for improving process efficiency, benefits could come from increased income as well as from reduced costs. For example, reduction in delays in setting up insurance or paying claims could attract new business.

Process improvements also offered the possibility of reduction in errors and an improved relationship with regulators, tax authorities, and auditors who would have access to accurate and timely information. As an example of scale, in a recent report[13] Goldman Sachs estimated that in banking, consistent use of blockchain in KYC/AML could save $2.5 billion of the estimated $10 billion global processing costs. There was also an effect whereby insurers on both sides of a transaction might have to carry extra capital while a difference between them was resolved; reducing errors and delays could thus reduce total capital requirements.

One respondent suggested that a move to new technology such as blockchain offered an opportunity for 'spring cleaning' and could provide a stimulus to accelerate the move to greater use of structured electronic data in the industry.

> "SOMETIMES A MARKET HAS HIGH COSTS AND HIGH MARGINS AND BARRIERS TO ENTRY, AND THE INCUMBENTS CHOOSE TO KEEP IT THAT WAY."
>
> **FINTECH CEO**

13 Goldman Sachs report 'Profiles in Innovation blockchain' dated 24 May 2016, available at http://www.the-blockchain.com/docs/Goldman-Sachs-report-blockchain-Putting-Theory-into-Practice.pdf

Process improvements also offered the possibility of reduction in errors and an improved relationship with regulators, tax authorities, and auditors who would have access to accurate and timely information. There was also an effect whereby insurers on both sides of a transaction might have to carry extra capital while a difference between them was resolved; reducing errors and delays could thus reduce total capital requirements.

One respondent suggested that a move to new technology such as blockchain offered an opportunity for 'spring cleaning' and could provide a stimulus to accelerate the move to greater use of structured electronic data in the industry.

STANDARDS

While respondents generally agreed on the tactical approach recommended in this report of looking to implement changes among a small group of firms, several pointed out the potential danger of 'islands of standards' where several different blockchain applications existed in slightly different form amongst different groups of firms. A more optimistic view was that the emergence of local standards would force the industry to choose its preferred standard.

> "THE WAY TO DEVELOP GOOD STANDARDS IS TO GET INVOLVED AT THE PROCESS DESIGN STAGE."
>
> **PETER TERESI, ACORD**

A consortium of national regulators and interested parties, led by The States of Alderney and assisted by PwC, has started a feasibility study for inter-governmental standards for mutual distributed ledgers. The objectives are to explore and raise awareness of approaches for regulating blockchains in financial and other services, with a particular focus on voluntary standards, such as ISO accreditation and certification. The study will sketch out the wide range of possible technical, performance, inter-operability, and governance and management standards.

A frequent observation from respondents was that they have to expend extensive processing time rekeying documents. For example, in property insurance they may have to enter data from paper copies of property and lease schedules, and the schedules are likely to differ between clients. Even structured electronic documents may require rekeying, as different descriptor fields may be used to describe the same type of asset or different encoding methods may be used for data elements such as addresses or geolocation.

In principle, pressure to use electronic files rather than paper documents, the development of standards, and the use of technologies such XML to label data elements give a route for moving towards greater data consistency and hence less rekeying. In practice, insurance is a global industry with clients in every country, and with major data exchanges with other sectors such as shipping, property, and banking; moving towards standards is a slow process.

Respondents were interested in any impetus which blockchain applications could give towards the use of (semi) structured electronic documents rather than paper and towards the adoption of data standards.

REGULATORY & LEGAL

Insurance is a highly regulated sector, and any entity that is proposing to use blockchain would need to comply with its existing regulatory obligations or, alternatively, liaise with regulators and law-makers to amend the existing law to allow for such changes in the systems it uses[14].

In particular, the greatest difficulty with blockchain would be the use of an unpermissioned system, where anybody could access the system and there is no guarantee of knowing the contracting parties. Regulation currently operates by regulators imposing rules on entities; not on systems or networks. A change in approach, particularly to embrace an unpermissioned system, would require a wholesale rethink of how regulation applies (although there are precedents; for example, emails are transmitted through a system without specific legal entity obligations through the chain of transmission).

Assuming that this is not envisaged and that regulation will continue to apply to particular entities or individuals, then a permissioned system seems likely to be

14 The information in this section is largely based on discussions with Freshfields Bruckhaus Deringer, and it reflects thoughts on principles rather on specific facts. We are grateful in particular to George Swan, Adam Ryan and Claire Harrop for giving us their time and expertise to support our research. This material is for general information only and is not intended to provide legal advice.

more satisfactory from the perspective of those entities. A broker or insurer remains liable for its own contractual and regulatory responsibilities to its customers and a permissioned system could allow only certain entities meeting certain requirements (for example, authorisation as an insurance company under certain laws) to join the system, and each entity would know the identity of the counterparties in the system.

As discussed in further detail below, firms must satisfy themselves with the integrity of systems and processing, which could be problematic with unpermissioned blockchains. In addition, the discussion on data protection demonstrates why unpermissioned blockchains would be impractical in any application involving personal data.

For these reasons, this report assumes that any blockchain technology to be used in wholesale insurance will permissioned based.

The legal and regulatory position for permissioned blockchains breaks into two main categories:

- cybersecurity and outsourcing;
- data protection.

Similarly to other regulated sectors, insurers often rely on third parties and outsource various aspects of their operations. At an EU level, the Solvency II directive contains a number of provisions relating to outsourcing. The basic principle is that whenever an insurer enters into an outsourcing arrangement with a third party, the insurer remains responsible for compliance with its regulatory obligations. Therefore, insurers have to be satisfied that any provider of a system, or use of another system, will not breach the insurer's regulatory obligations.

Further, insurers are under increasing regulatory pressure to have effective risk management practices in place to address cybersecurity risks. Cybersecurity has become a key priority of the UK's Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA). By way of example, the PRA recently issued a questionnaire to insurers designed to understand firms' current policies and capabilities in the area of cybersecurity. This focused on three areas: cybersecurity and resilience capabilities, the extent to which firms underwrite cyber-insurance business, and (in conjunction with the FCA) what confidential customer information firms receive and how this is handled and stored.

In principle a permissioned blockchain system could provide improvements to existing systems, including reducing cyber risk and reducing reliance on a single provider of services, which should be viewed positively by regulators. Indeed, blockchain is regarded as having innate cybersecurity advantages. Insurers, however, would have to be satisfied that the blockchain application achieves at least the same integrity of processing as the technology it supersedes.

This may create a problem of timing, since regulators tend to want to review what exists, rather than give permission in advance, but insurers may not be willing to develop (or pay a third party to develop) systems based on blockchain without knowing that this will be acceptable. In practice, regulators may be persuaded to engage in an iterative way, before the point at which a proposed change becomes well defined, so that it should be possible to get reasonable assurance that a change to a blockchain application will be acceptable.

It should be noted that future outsourcing requirements and the focus on cybersecurity will remain, even after moving processes to a blockchain-based system.

Data protection creates issues even for permissioned blockchains. If a blockchain contains personal data (that is, any information relating to an identified or identifiable natural person) or sensitive personal data, this gives several legal requirements. In the EU, for example:

- the data must be obtained only for specific lawful purposes and used only for the purpose for which it was collected;

> "REGULATORS DO NOT WANT TO TRY AND REGULATE SPECIFIC TECHNOLOGY – THEY DO WANT TO REGULATE OUTCOMES."
>
> **PATRICK SPENS, PWC UK**

- the data must not be kept for longer than is necessary;
- there is a general prohibition on the transfer of personal data from the EU to a country outside the EEA unless that country ensures an adequate level of protection for the data. In practice, this means to a limited number of non-EEA countries that have been designated by the European Commission;
- the 'right to be forgotten' potentially allows an individual to demand the destruction of person data held about him or her.

In analysing the impact of these requirements on the use of blockchain, it should be noted that insurance companies must already comply with them. Absent of a change in law, any adaptation of existing processes to use blockchain would also need to comply with such requirements. For example, contracts between companies should ensure that all data protection requirements are complied with by the company receiving personal data.

A central issue is, of course, that the blockchain is immutable, so that personal data once entered will be included for ever. One potential mechanism to resolve this is to encrypt each document separately[15]. Instead of deleting the record of the sensitive personal data, the firm would delete the key to that data. This may be satisfactory from a practical perspective, but the approach has not been tested in court as meeting statutory requirements and would likely need to be discussed with appropriate regulators. Using encryption also creates the need to distribute the keys in a controlled way; this will have to be resolved in any viable application.

A technical issue to be considered is the capacity of future cryptography. Certain ciphers used today, particularly the most common types of public/private key ciphers such as RSA, are vulnerable to decryption if a quantum computer of adequate power is developed[16]. There are ciphers which are believed to be not vulnerable to quantum computers[17] although key sizes may need to be increased. Given the need to prove that data records are unreadable when the key is destroyed, there is a need to ensure that cryptography methods used are believed unbreakable on any reasonable timescale.

Drilling down into the detail of personal information shows that there are more subtle cases to consider. For example, if an electronic document in a blockchain contains structured lists of personal data, there may have to be a key at the level of the record for each individual. If a scanned paper document contains details of multiple individuals, the problems of control are analogous to those of the paper-based processes which exist today. Similar issues exist with unstructured electronic documents such as emails.

15 The UK Information Commissioner's Office recognises encryption as "a valuable tool for safeguarding data" (amongst a range of technical and organisational measures).

16 See for example http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment for a non-technical explanation.

17 See for example http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf for the USA Government recommendations.

POTENTIAL USE CASES

The thrust of the interviews was to identify potential use cases. This subsection looks at process issues mentioned by respondents which did not meet the criteria for the long list, that is, either we could not identify a blockchain application as part of a best technical solution for the perceived process issue, or there was a relevant blockchain application, but it did not seem feasible to implement it except by doing so simultaneously across a sector or geography.

The process issue raised most often related to accounting and settlement in the London Market, currently mediated by central processing. Although this was seen as expensive and inefficient, no respondent was able to give a clear vision of an alternative solution using blockchain which could be implemented at process level by a small subset of firms.

One respondent suggested the creation of a national fraud register, where all financial transactions were recorded, providing a database for checking by banks and insurers to help prevent future fraud. A good example of the importance of this would be the £24 billion paid out by UK banks in payment protection insurance (PPI) claims since 2009 (approximately £1,000 per UK household), excluding fines and administration costs[18]. The application would be based on a blockchain with all banks and insurers as users and updaters. The national fraud register might be structured in a way that permits financial firms to avoid organised fraud schemes, while protecting consumers' rights and consumers' abilities to redress incorrect information. This idea is currently being explored in Australia.

A few respondents talked about the potential role for blockchain in supply chain management and provenance. When goods were lost or damaged along a supply chain, there were often arguments as to where exactly this happened and therefore which insurance policy covered the loss. If there could be more certainty as to which individual items arrived safely at each point of the chain, then there would be more legal certainty around insurance and less time, effort, and cost spent identifying which insurer carried the risk. Chain-of-custody, or provenance, problems exist in many industries, from low value (timber or fish) to high value (drugs or rare-earth elements).

Various respondents mentioned blockchain applications which were relevant to wholesale insurance but not a part of it. For example, there was interest in the Everledger[19] initiative to use a blockchain application to track individual diamonds, thus proving provenance and offering protection from fraud and from the sale of stolen stones. This – and its potential extension to other domains such as works of art – was seen as a positive development for insurers. There was also interest in announcements from Honduras and Denmark on putting their land registry on a blockchain, as a way of creating legal certainty and reducing scope for corruption. Honduras was seen as a test case for creating infrastructure in the developing world which could accelerate the use of insurance.

DISRUPTIVE VERSUS INCREMENTAL CHANGE

What is disruptive depends on the viewpoint of the observer. Uber is disruptive for licensed taxi drivers, but not yet for cyclists. Respondents did not see the proposed use cases in this report as having the potential to disrupt the insurance ecosystem as a whole, but some saw potential for radical impact in particular areas. For example, a substantial increase in efficiency of transmitting ancillary contract information has the potential of increasing the power of the insurers and reinsurers over the brokers currently active in the reinsurance market, potentially leading to brokers being squeezed out.

Because the research focused on existing processes, it is not surprising that the use cases identified relate to incremental change.

> "FIRST YOU APPLY NEW TECHNOLOGY TO EXISTING PROCESSES. ONLY THEN DO YOU SEE HOW TO USE IT IN A DISRUPTIVE WAY."
>
> **HEAD OF IT, INSURER**

18 Since January 2011, a total of £24.2 billion has been paid out to customers who were mis-sold payment protection insurance (PPI)." – retrieved from FCA website (25 July 2016) - https://www.the-fca.org.uk/consumers/payment-protection-insurance/monthly-ppi-refunds-and-compensation

19 See http://www.everledger.io/

05 Long List Of Potential Use Cases

This list includes all areas where respondents thought blockchain technology might improve or transfer wholesale insurance processes, making them more efficient or effective. As described in the methodology, the filtering removed cases where an alternative technology seemed to offer a better solution or where implementation would require market-level agreement across an entire sector or geography.

The long list consists of:

- Placement and contract lifecycle – documentation;
- Establishing treaty between reinsurer and underwriter/insurer;
- Archiving of bindings;
- Claims management;
- Proof of insurance;
- Managing policies for multinational clients;
- KYC/AML;
- Inter-firm accounting reconciliation;
- Managing a global health policy;
- Tracking policies imposing operational limits on policyholder;
- P&I club bail bond cancellation;
- Excess of loss reinsurance;
- Managing a portfolio of retail insurance risks;
- Mobile phone and blockchain to create insurance infrastructure in developing markets.

Suggested cases filtered out before creating the long list were:

- Accounting and settlement in the London Market;
- National fraud register;
- Improved supply chain management information.

20 https://next.ft.com/content/8a8c4c5e-44e4-11e6-9b66-0712b3873ae1

1 PLACEMENT AND CONTRACT LIFECYCLE – DOCUMENTATION

Background	The current process for a broker to obtain a quote from an underwriter for a transaction of any complexity is to present a 'heads of terms' of the overall contract required, together with ancillary documents comprising both electronic files and physical paper documents. These ancillary documents will describe the insured risk; this often requires immense detail.
Issue	Insurance contracts relate to a file of electronic or paper 'real life' documents which can be very large and which will generally be added to throughout the placement process and the contract life. As each participant has to check this file at each stage of interaction, which may for example be several times during an iterative underwriting process and at subsequent points in the deal lifecycle, there can be a heavy processing overhead in simply reconciling to the file presented on the previous occasion. There is operational inefficiency in preparing any paper document and in the underwriter copying required sections. Moreover, even with electronic files it is difficult to create an adequate audit trail to show the exact documents and versions included. As there are multiple participants and iterations in the process, there is an additional risk that the file will change (or be changed accidentally) between requests to underwriters.
Risks	■ Errors from processing inefficiencies ■ Cost ■ Delay ■ Legal uncertainty
Use of blockchain	Use a blockchain to store all ancillary contract documents, and share between the broker and underwriters (and as required other participants such as reinsurers and claims agents). This would ensure that every reference to contract documents was consistent and would remove the need for participants to check the same file on different occasions – at most they would have to check the documents updated since the previous occasion. The blockchain would also be viewable by regulators and tax authorities which would simplify reporting and checking processes. As it would not normally be the case that all participants could read all documents, the applications would need to encrypt certain documents and distribute keys in a controlled way. The actual documents could be included in encrypted form on the blockchain itself or else the blockchain could contain hashes only, with a few nodes holding the documents. As noted in the Executive Summary, this is a minimalist proposal, which would not in itself address the issue of rekeying made necessary by the prevalent use of paper or unstructured electronic documents in the industry. There is no simple fix to this, but the 'spring cleaning' effect of a group of first movers creating a new platform offers an opportunity to impose behaviours which accelerate the move to recognised standards and to the use of source electronic documents.

ESTABLISHING TREATY BETWEEN REINSURER AND UNDERWRITER/INSURER

■ Fundamentally this is the same issue as above, to be resolved by the same proposed solution.

ARCHIVING OF BINDINGS

■ Fundamentally this is the same issue as above, to be resolved by the same proposed solution. Many of the existing placing systems, most recently Placing Platform Limited (PPL)[21] in the London Market, could archive their information after 'placing' or 'binding' using blockchains.

21 https://next.ft.com/content/8a8c4c5e-44e4-11e6-9b66-0712b3873ae1

2 CLAIMS MANAGEMENT

Background	When a claim is made on a policy, each underwriter/insurer/reinsurer (abbreviated below simply to underwriter) involved will want to be kept informed of progress and will potentially wish to instigate specific actions. For Lloyd's Market, generally only the lead underwriter and immediately following underwriter will be involved in processing and fighting the claim, but outside Lloyd's typically many or all underwriters will wish to be involved. Usually one claims broker coordinates the claims process.
Issue	There are multiple underwriters pursing their own process (which may involve external lawyers) and generating additional costs for themselves and the client broker.
Risks	■ Cost ■ Delay ■ Legal uncertainty ■ Reputational risk
Use of blockchain	There is scope for creating a blockchain incorporating all documents created in the claims process and available to all underwriters and in addition to the client broker and claims broker. This could enable more underwriters to accept the claims process without actively participating as they would be able to monitor and review as they required. It could also reduce the cost of administration for the claims broker as it would reduce duplication of process. Depending on the design of the process, the 'Claims' blockchain could be standalone or could simply be an extension of the 'Contract Lifecycle' blockchain described above. In either case there would need to be additional functionality to map the claims process.

3 PROOF OF INSURANCE

Background	As an example, before an aircraft takes off it has to provide a proof that it is insured. This can create complications particularly in developing markets, since the paperwork may be complicated and there is a risk of fraud. Similar requirements exist in other markets.
Issue	If the paperwork is difficult to sort out, the plane can be delayed, causing disruption and costs.
Risks	■ Cost ■ Delay
Use of blockchain	By linking the insurance of an aircraft to a blockchain distributed to a number of trusted insurers round the world, it should be possible to provide instant confirmation of insurance by each airport having a link to a specific insurer. This is in some ways similar to how credit cards achieve global coverage through a chain of providers.

4 MANAGING POLICIES FOR MULTINATIONAL CLIENTS

Background	A single policy for a large multinational company may be implemented as a set of local policies in each country in which the company has a presence. This requires a complex process to break out and track the overall policy against the subsidiary policies in each country. The same issue arises for claims under the policy.
Issue	It is generally complex to set up and manage the contracts for individual jurisdictions which have to be set up through subsidiaries or third parties. Payments of premium and ultimately for claims have to be passed up and down the chain as will contract amendments as insured assets move between jurisdictions, and aggregate global limits have to be applied locally. Risk management may be complicated by the disaggregation of the global contract. Local tax authorities may query payments both for the insurer and the client, and the insurer will have to support the client in reconciling payments, cover, and claims.
Risks	■ Cost of processing ■ Delay ■ Mistakes in risk management or claims leading to costs ■ Errors in tax reporting or inability to prove reporting to tax authorities ■ Reputational risk if the insurer causes problems for the client
Use of blockchain	By recording the overall contract and its split country by country in a blockchain, it should be possible to provide certainty internally, to the client and to external stakeholders such as tax authorities. This would allow development of more robust processes for risk management and claims handling.

5 KYC/AML

Background	Brokers, insurers, and reinsurers have to perform KYC/AML on all of their counterparties, both legal entities and individuals, including third parties due payment under claims. Other processes such as sanctions screening or the determination of ultimate beneficial ownership are either part of this process or sit alongside. Requirements also differ by regulator. If a client deals with a broker which deals with multiple underwriters, most of which deal through brokers with reinsurers, a single transaction can involve many tens of participants, each of which has to perform KYC/AML along the chain. This multiplicity of repeated checks adds to cost and delays. KYC/AML generally has to be repeated for the same individuals or firms in different transactions, and by different brokers, underwriters, insurers, and reinsurers in the same transaction chain.
Issue	The need for each institution to carry out KYC/AML from scratch creates cost and delay.
Risks	■ Cost ■ Delay ■ Loss of business which cannot be placed within the timescale required by the KYC/AML process ■ Reputational risk if payment of claims is delayed while KYC/AML is carried out on a beneficiary
Use of blockchain	Building on an existing model developed by Z/Yen for PwC, use an outsourced bureau to perform a major part of the validation of customer identity. Use blockchain within this to record all the customer's personal documents and evidence of validation by the bureau. All documents on the blockchain would be encrypted with only the customer having the keys, thus resolving a set of regulatory issues around privacy and data protection. The customer could then present the blockchain with an appropriate subset of keys to the next institution with which they want to do business, and this institution would be able to rely on the validation done by the bureau without delay. The overall effect would be to reduce the total cost and time spent on KYC/AML within the industry.

6 INTER-FIRM ACCOUNTING RECONCILIATION

Background	Outside the London Market, brokers, insurers, and reinsurers typically exchange payments statements each quarter.
Issue	These are not standardised and typically contain rounding differences as well as some errors, creating a processing overhead to achieve agreement.
Risks	■ Cost of processing
Use of blockchain	Potentially gross payments could be reflected in a blockchain creating a trusted record for reconciling against.

7 MANAGING A GLOBAL HEALTH POLICY

Background	An example is insurance of warehouse contents up to a value of €5m, with an 'after the fact' increased premium paid for periods where the value is above this.
Issue	The insurer needs to deliver a quick response and to handle sensitive data in many different countries on the one policy.
Risks	■ Breach of data protection laws ■ Conduct risk if data security breached ■ Reputational risk if data security breached
Use of blockchain	Putting individual data on a blockchain in encrypted form with keys available only to the individual and in escrow would lend itself to a structure where information is widely distributed but safely held.

8 TRACKING POLICIES IMPOSING OPERATIONAL LIMITS ON POLICYHOLDER

Background	An example is insurance of warehouse contents up to a value of €5m, with an 'after the fact' increased premium paid for periods where the value is above this.
Issue	Operationally it is hard to prove the value held day by day, even when every stock movement in or out has a € value recorded.
Risks	■ Premium paid will not reflect the full risk, creating a loss for the insurer over time
Use of blockchain	By writing all stock movements to a blockchain there would be a 'super audit trail' which would allow reconstruction of the history of value held each day. This could also be used to support a new type of product insuring actual value rather than a maximum. Another example might be 'geostamping' the geolocation of insured assets, registering their location, e.g. a ship or vehicle with certain navigational restrictions.

9 P&I CLUB BAIL BOND CANCELLATION

Background	As an example, where a ship in port causes damage covered by insurance it may need to present a 'bail bond' to be allowed to leave. This 'bail bond' is a standby letter of credit guaranteeing payment of the insurance claim directly to the port. Resolution of complex claims may take five to ten years, and the bail bond cannot be cancelled until the claim is paid in full.
Issue	Bail bonds are paper and have to be physically cancelled. This can be a difficult process, especially in developing countries.
Risks	■ The bail bond remains open, and the insurer has to continue to pay the bank, maintain capital, and suffer loss
Use of blockchain	By recording the bail bond in a blockchain rather than in paper it can be linked directly to payment of the claim and cancelled automatically. This could be achieved, for example, by having extra terms in the insurance that allows the issuing bank to cancel the bail bond following (a) receipt of a 'confirmation of final settlement request' and (b) confirmation of receipt of payment by the port's bank. This needs a blockchain structure, because a paper bond would still require physical return to enable cancellation.

10 EXCESS OF LOSS REINSURANCE

Background	Reinsurance contracts ('treaties') can be equivalent to underwriting a percentage of the risk of a single client contract, but there is also a form of reinsurance at the portfolio level which pays out losses on specified risks over a trigger limit up to a higher limit. This is known as 'non-proportional' reinsurance or 'excess of loss' reinsurance.
Issue	An excess of loss treaty can be complex in its underlying documentation and processing, especially when there are claims. If the cedent (party insured) makes a claim it has to demonstrate its portfolio losses for the stated risk. Complexities include assigning time, jurisdiction, and exchange rate to losses, and the fact that at various stages the estimates of loss included in the calculation will be updated.
Risks	■ Process errors ■ Capital tied up while differences are resolved ■ Need for reinsurer to hold additional liquid assets to make payments, due to inability to forecast liabilities accurately ■ Reputational risk
Use of blockchain	By recording the evolution of internal losses on a blockchain for each treaty, the insurer and reinsurer can track and reconcile the emerging liability. Moreover, by standardising this reporting across treaties, the insurer should be able to improve its controls over how it tracks its own risks, enabling better risk management

11 MANAGING A PORTFOLIO OF RETAIL INSURANCE RISKS

Background	Wholesale insurance processes involve handling documents holding large quantities of retail client information which have been grouped into portfolios for group processes, such as reinsurance, run-off, or trading – such as portfolios of motor policies.
Issue	It is difficult to ensure protection of data by participants downstream in the broker/insurance/reinsurance/claims chain. Further, if the data is unstructured, it is difficult to aggregate the information effectively for risk management and pricing.
Risks	■ Breach of data protection laws ■ Conduct risk if data security breached ■ Reputational risk if data security breached ■ Processing cost ■ Poor pricing and risk management from failure to aggregate data effectively
Use of blockchain	Use of blockchain for document handling naturally lends itself to encryption of data and to permissioning of individual documents to individual users. It does not necessarily improve on conventional technologies as regards to more granular protection of individual data fields, but protection at document level may be sufficient for many applications. Blockchain also does not automatically impose standardisation of data to improve aggregation, but it could provide an impetus to encourage use of standards.

12 MOBILE PHONE AND BLOCKCHAIN TO CREATE INSURANCE INFRASTRUCTURE IN DEVELOPING MARKETS

Background	In some developing markets the use of insurance is limited by distribution costs, as well as by issues in legal and commercial infrastructure – for example the risk of corruption. This impacts insurance volumes – for example in property insurance.
Issue	Costs and risks of legal uncertainty can make it prohibitive to create a network to distribute insurance.
Risks	■ Lack of infrastructure creating risk of fraud or high legal costs for insurers ■ Underinsurance among potential customers leading to lower income for insurers ■ Slower economic development for the country
Use of blockchain	Use of mobile phone apps as a channel with standardised contract structures can make blockchain a natural tool for recording liabilities that cannot be disowned by either party and are not susceptible to interference by third parties. At least one large global insurer is developing a prototype application in a developing country.

06 Short List of Potential Use Cases

EVALUATION OF 'BARRIER' AND 'BENEFIT'

As described in the methodology, the process followed excluded from the long list potential use cases where an alternative technology gave a better business case than blockchain or where implementation required market-level cooperation across a sector or geography.

We show below the process of filtering the long list use cases based on an initial subjective evaluation of their 'Benefit to business' and 'Barrier to implementation'. The factors considered in the evaluation were:

Barrier:

- complexity of the expected functionality;
- need to develop distribution and use outside the industry.

Benefit:

- size of the process involved for the relevant firms;
- potential fraction of process costs which could be saved;
- other non-cost benefits, such as reduced delay, extra business, or reduced reputational risk.

In the tables below, each of these factors is estimated on a scale from 1 (low) to 4 (high) and combined to give an overall rating for Barrier and Benefit.

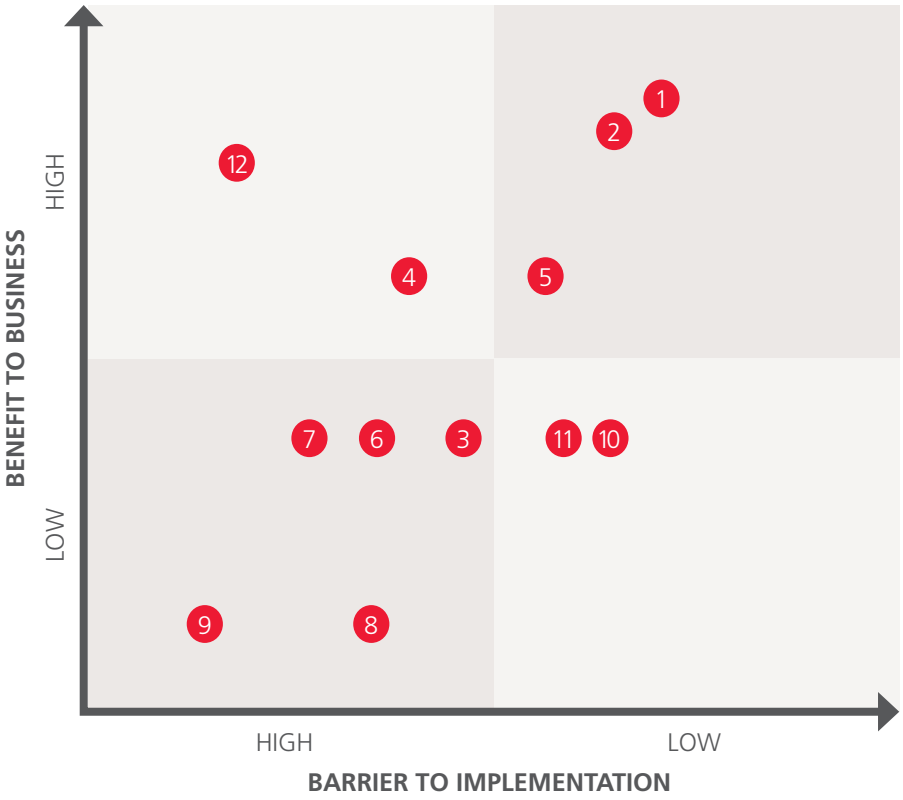
BARRIER

#	Use Case	Expected Functionality	Reach beyond industry	Barrier
1	Contract documentation	2	1	2
2	Claims management	2	1	2
3	Proof of insurance	1	3	3
4	Multinational entity policies	2	2	3
5	KYC/AML	2	2	2
6	Inter-firm accounting	3	3	3
7	Global health policy	3	2	3
8	Operational limits	3	2	3
9	Bail bond	1	4	4
10	Excess of loss reinsurance	3	1	3
11	Portfolio of retail risk	2	1	2
12	Mobile phone app	3	3	3

BENEFIT

#	Use Case	Size of process as fraction of business for firms involved	Potential saving (as fraction of cost of individual process)	Non cost benefit: e.g. speed, reputation, more business	Benefit
1	Contract lifecycle documentation	4	4	2	4
2	Claims management	4	2	4	4
3	Proof of insurance	1	3	4	2
4	Multinational entity policies	2	4	3	3
5	KYC/AML	3	2	4	3
6	Inter-firm accounting	2	2	1	2
7	Global health policy	1	2	3	2
8	Operational limits	1	2	2	1
9	Bail bond	1	2	2	1
10	Excess of loss reinsurance	2	2	2	2
11	Portfolio of retail risk	1	2	2	2
12	Mobile phone app	1	1	4	4

These estimates give the following grid, which has been used to select the short list of use cases.



The short list is the three use cases in the top right quadrant:

- Placement and contract lifecycle – documentation;
- Claims management;
- KYC/AML.

These seem worth serious investigation by an industry consortium.

07 Conclusions and Recommendations

CONCLUSIONS

Blockchain technology has unique characteristics that create new organisational and operational opportunities within wholesale insurance. Market participants are aware of the technology. Many have taken initial steps to learn more about blockchain, with several larger firms setting up their own projects to identify use cases and to develop proofs of concept. Allianz has recently publicised a catastrophe bond prototype and Blem Information Management has introduced a blockchain application within an existing industry product.

Furthermore, the London Market Target Operating Model (TOM) project is also looking at the use of blockchain for different applications, and plans to publish its initial programme shortly.

The aim of the report was to identify use cases for blockchain which seemed likely candidates for having a positive business case provided that a relatively small group of firms is willing to implement together. There are at least three plausible use cases:

- Placement and contract lifecycle – documentation;
- Claims management;
- KYC/AML.

It was not possible to identify and analyse every potential use case, and undoubtedly there are other examples of potential applications for blockchain likely to show positive business cases.

Although we have identified only a few immediate candidate use cases, we are confident that creative minds within the industry will identify many more over the years to come. Mutual distributed ledgers help communities share information across time and space, and provide protection from central monopolies. Blockchains ledgers provide persistent and permanent utilities that safeguard transactions and preserve transaction data and could displace much centralised messaging and shared data functions. Moreover, the technology is well suited to support process-level initiatives which could act as a catalyst for change across markets, thus bypassing the structural barriers to immediate top-down market-level change. These capabilities make blockchain well-suited to the needs of the wholesale insurance industry.

RECOMMENDATIONS

The recommended next step is to identify a group of firms willing to join a consortium to investigate the business case for at least one of the potential use cases. The consortium firms would also work together on areas of common interest by, for example:

- expanding frontiers – develop and publishing thoughts on common insurance applications of blockchain technology;
- changing systems – provide evidence-based examples on where blockchains work and don't work in wholesale insurance;
- delivering services – such as standards, common technology bases, and shared demonstrators;
- building communities – engaging wider stakeholders (regulators, trade bodies, customers, suppliers) through meetings, networking and events, including conferences and training using collaborative tools.

The expectation is that the first stage of this would be a relatively high-level (and hence swift and inexpensive) exercise, with the following activities:

- reviewing the initial subjective estimates of 'benefit to business' and 'barrier to implementation' used to establish the short list of use cases;
- defining the minimal functional requirements for the proposed new process and blockchain application;
- estimating the development cost of the application;
- validating that the risks and issues of the proposed change are understood and manageable;
- each participating company estimating its business benefits and cost of implementation;
- combining the above to form an aggregate business case and a business case for the individual companies.

This would be analogous to the process which an individual company would carry out to estimate the costs and benefits of a proposed process change, as part of its methodology of selecting the changes to implement. Assuming that the resultant business case was attractive, the consortium would look to obtain approval from its members to build and implement the application.

Long Finance is pleased to have had the opportunity to research and publish this report, and looks forward to its stimulating the use of blockchain in wholesale insurance.

Appendix A – Acknowledgements

We would like to thank all those who have contributed time and expertise to this research. Without implying any endorsement of our conclusions, we would particularly like to thank people working at the following organisations for their input. Please note that the views expressed are not of the companies they are employed by. Any misinterpretation or errors are the responsibility of Z/Yen.

Acord
Airmic
Arthur J Gallagher
Allianz
Aon
Assicurazioni Generali
Association of British Insurers
Aviva
Axa
Bank of England
Barclays Bank
Beazley
Bitcoin Foundation
Blem Information Management Ltd
Brit Insurance
Chain Finance
Consensys
Deutsche Bank
Ethereum Foundation
FCA
Freshfields Bruckhaus Deringer
Great Lakes (Reinsurance) UK
Hannover Re
Hiscox
IdenTrust
Informa
International Underwriting Association
Irish Funds Association
Jardine Lloyd Thompson Group
Liberty Mutual Insurance
Litmus Analysis
Lloyd's of London
London & International Insurance Brokers' Association
London Market Group
Markel International Insurance Company
Marsh
Microexchanges
Miller
Munich Re
Norton Rose Fulbright
Prudential UK
PwC
RFIB
SafeShare Insurance
Sumitomo Life
Suncorp Group
Swiss Re
Thomas Miller
UBS
Willis
Xchanging
XL Catlin
Zhongan Insurance

Appendix B – Technical Background On Blockchain

BLOCKCHAIN TECHNOLOGY

The key purpose of the technology is to produce a data file which is guaranteed tamper proof, and which can be shared between users. All users can read the file and check its consistency, and one or more users will be able to update the file. A configuration enabling updates by multiple users can remove the need for a central owner.

The basic tool is a 'hash' embedded in the data file to guarantee that the data has not been tampered with. The hash is produced by an arithmetic function taking as input every bit (0 or 1) of the data and changing its output unrecognisably if a single bit is changed or added.

Thus, for example, SHA-256, a commonly used hash function, gives the following output for data files 'abcdefghijklm'and 'abcdefghijklo' – two strings differing only in the last letter and there only by a single bit in the computer code:

ff10304f1af23606ede1e2d8abcdc94c229047a61458d809d8bbd53ede1f6598
and
880433bd8ba16631775ddfba51d505df76d8a3420db9e21d123c2fcbd46fe48f

(Each output is a number which would be about 77 digits in decimal and is represented here slightly more efficiently in base 16 – hexadecimal – where the numbers from 10 to 15 in decimal are represented as 'digits' a, b, c, d, e, f.)

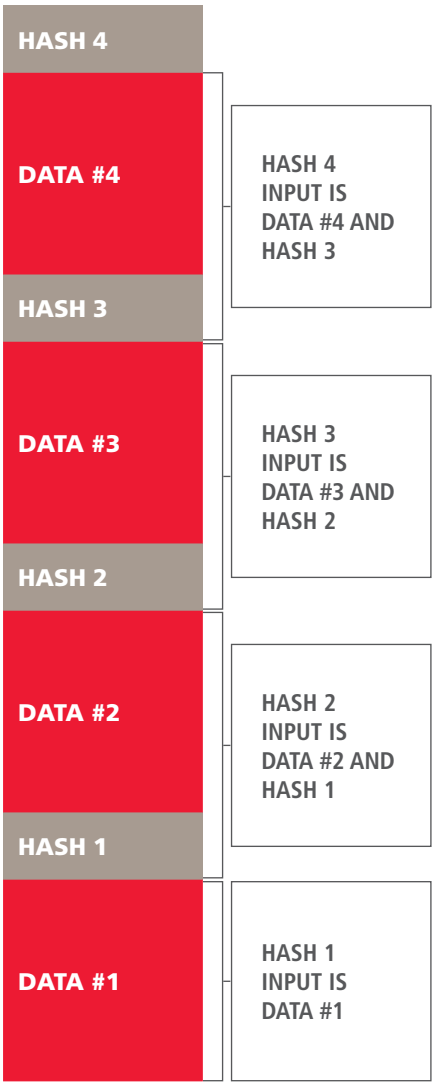
Given a SHA-256 code for a random file, your chance of finding a second file with the same code – assuming you have a computer per person on the planet each capable of processing a billion billion billion files per second, and the time available since the big bang – is infinitesimal: about one in a million billion billion billion.

In a blockchain, a hash is appended after each new block of data. This takes as input not only all of the new data but also the previous hash. This guarantees that any change of data anywhere in the entire file will create an inconsistency in the final hash.

The integrity of the process is underwritten by distributing copies of the blockchain file to all users each time there is an addition of a data block and hash. Everyone thus has an updated copy of the file and can check the consistency of the hashing. This also allows for different users (with appropriate permission) to update the file, subject to there being rules in place to deal with simultaneous updates.

A blockchain file therefore looks like:

BLOCKCHAIN STRUCTURE



By removing the hashes, you recover a normal data file which can contain any set of data you wish. This could include databases, word documents, PDFs, spreadsheets, and photographs or video or audio files. The blockchain can thus be used to replace any paper or electronic files and to transmit the whole with perfect integrity and version control (each new version will require a new hash).

An alternative structure is to include just the hashes in the distributed blockchain and to store the data elsewhere. This means that the blockchain itself is much shorter and there is potentially better data protection, while the core capability of providing proof that the data blocks were added at specific times is maintained. However, there now has to be a separate process for maintaining distributed copies of the data blocks, raising new issues of governance, process, and risk.

Given that blockchain guarantees accuracy of data, it can be used for Smart Contracts. These are contracts embedded as code in the blockchain and executed automatically when some trusted external data source hits a defined value. An example with relevance to insurance might be a weather insurance contract which pays out if the rainfall in a specific location in a specific month exceeds 7cm, as defined by a data output from the UK Met Office.

UPDATE PROCESS FOR NEW BLOCKS

The internal design of the blockchain is described above, but there also needs to be a process by which the blockchain is extended each time there is a new block of data to be added. This mechanism for update must ensure the following:

- whenever there is data to add, it is added to the blockchain as a new block maintaining the integrity of the blockchain structure;
- update is timely;
- updated blocks are broadcast quickly to all users of the blockchain;
- whe process is resilient against individual users being unable to access the system;
- where there is an update of the same blockchain by different nodes with different data, so that there are two incompatible versions of the blockchain broadcast at about the same time (a 'fork'), there is a process to ensure that the situation is resolved quickly and the integrity of the blockchain data is maintained.

There are different technical and governance models for achieving this for a permissioned blockchain. Choice of mechanism will depend on factors such as the application being supported and the number of active users. In a regulated environment, there may be a need for a 'user of last resort' which maintains a current copy of the blockchain and contracts to rebroadcast if required.

Part of the process of implementing any blockchain application will be to optimise the governance and technical framework for the update mechanism. There are many technical solutions for validating new transactions and adding a new block of data to the chain.

Perhaps most simply, high-volume ledger recording, such as data logging, may allow a stream of transactions to be added to a blockchain by any user. If there is little chance of fraud, then the mere act of adding the data, and timestamping if required, may be a sufficient level of validity.

The governance of a permissioned blockchain can establish a more sophisticated update process based on a voting system. At its simplest, a single central party could have the right to validate and update the blockchain – a single voter. Given the reason for choosing blockchain technology in the first place, it is more likely that governance would require some sort of involvement by all participants. This might require unanimity, or it might require a threshold number of participants. Many other models are possible.

The user adding a new block of data will generally include a block of cryptographic information to prove its own identity and to evidence the validation it has carried out.

Any 'democratisation of data' raises issues of governance, risk, and cost, but working solutions exist for these within existing applications.

CRYPTOCURRENCIES

This subsection is peripheral to the use of permissioned blockchains; it is included as background.

Another definition of cryptocurrency, this time from 'CryptoCoin News', is "a medium of exchange like normal currencies such as USD, but designed for the purpose of exchanging digital information through a process made possible by certain principles of cryptography."

Cryptocurrency applications such as Bitcoin are built on unpermissioned mutual distributed ledgers, but they add more. The distinguishing computer function of a cryptocurrency is how it validates new transactions and avoids people cheating by writing invalid transactions. The intense interest among technologists in Bitcoin derives from its innovative approach to achieving distributed consensus on new transactions: the 'mining' process.

Bitcoin's mining uses a 'proof-of-work' test to assign who can update the blockchain. On each iteration of the blockchain, this asks users to find – by running a hashing function on random numbers – a number which gives a SHA-256 hash within a target range. The more computing power a user puts in, the more likely it is to be first to the solution and hence to have the right to update the blockchain – and to receive a prize of newly minted Bitcoins which is the economic drive for participation in the process. Many other systems, such as the second most well-known cryptocurrency, Ethereum, use a similar approach.

Bitcoin's mining carries a heavy overhead in terms of cost and slowness. The process is energy-intensive meaning that the cost of writing a Bitcoin transaction is rather high (tens of cents or dollars) and is likely to remain high. The mining process is also slow, on the order of about ten minutes to process a new block of data. This is a dynamic environment and Bitcoin may get cheaper and faster, but at the moment it can process only about seven transactions per second at peak volume.

A suggested alternative approach is 'proof-of-stake' which requires users to prove ownership of a certain amount of currency or to use some of their 'stake' in the currency to indemnify transactions against fraud in order to take part in the next update of the blockchain. The most significant proof-of-stake environment is Ripple. The debate on whether 'proof-of-stake' is a viable approach is heated, and is outside the scope of this paper. To date, proof-of-stake approaches have been overshadowed by proof-of-work for unpermissioned blockchains.

Appendix C – Proof-of-concept

This Appendix was written by the Insurance Team members of the PwC Blockchain Development Lab in Belfast, who developed the Proof-of-concept (PoC) that accompanied this report.

BACKGROUND AND OBJECTIVE

When PwC and Z/Yen agreed to undertake this research, our objective was to both test the understanding and interest of the wholesale insurance market in this technology and to inform and illustrate how the technology could be applied to business problems.

Whilst the survey output will provide the industry with new and interesting insight into how the technology may be deployed, we also felt it important to go beyond the purely theoretical and demonstrate, with working code, some of the benefits that come from the deployment of mutually distributed ledgers. Indeed, we feel that a key success factor when working with such new technologies as blockchain is to move quickly from conceptual design to hands on experimentation. In this way firms can understand what is possible, discover limitations and learn from experience, how business problems can be resolved.

To that end the PwC Blockchain Development Lab in Belfast undertook to build a working PoC alongside the development of the industry report. The benefit to participants will be that they can see the technology in action, understand how it may be used to tackle business problems and also see the difference between this and more conventional centralised database solutions.

It is our intention to utilise the PoC in demonstrations (it was demonstrated already at the report pre-launch event on July 18th) and if there is interest then, with some restrictions, we may look to make it available to the participants in the survey to inform and educate stakeholders within their own firms.

The remainder of this section describes the approach to developing the PoC both to explain the purpose of it in more detail and to illustrate how an agile approach using this type of technology can rapidly (within 5 weeks) result in working code. The penultimate 2 parts of the section are intended for a more technical audience and provide more detail on the technology fabric selected and technology techniques adopted.

WHAT IS A POC?

According to the Oxford English Dictionary the definition of a PoC is:

Proof-of-concept n. evidence (usually deriving from an experiment or pilot project) demonstrating that a design concept, business idea, etc., is feasible;

The term itself is often misused. Some people view it as always being the first step on the road to a live production system. In some cases, that may well be true but the essence of many PoCs is that they are throwaway pieces of work. They are intended for scoping, experimentation, educating, learning and discovery.

In line with the definition given above our aim when we set out to produce this PoC was not to focus in too much detail on any existing insurance process but instead to provide evidence through an experiment to demonstrate how blockchain provides an especially elegant solution to some generic problems faced in the industry and how the technology has particular benefits over more traditional centralised database solutions. Given the short timeframe involved (5 weeks) we have focused on our core objective and the resulting PoC is by no means a 'complete' product.

A final objective of the PoC was to provide insight to survey participants in how we approached the development of the PoC. This illustrates how an agile development approach based on sharp focused sprints is well suited to this type of technology.

SCOPING THE POC

Mutually distributed ledgers have been around for a long time, so as part of the PoC we wanted to illustrate some of the characteristics that have driven the huge increase in interest. When Satoshi Nakamoto published the Bitcoin white paper back in 2008 (Bitcoin: A Peer-to-Peer Electronic Cash System) he brought together a number of existing technologies to solve a long standing problem. This major breakthrough was distributed trustless consensus and it has enabled systems to be built where there is no single trusted intermediary. Previously, mutually distributed ledgers required there to be a trusted intermediary to either update the ledger or to verify its integrity. These intermediaries add cost, time and complexity to business processes and thus the realisation that they can potentially be eliminated begins to justify the excitement.

A number of the perceived blockchain benefits that the PoC illustrates are:

- each party has their own copy of the shared data and every party is seeing a common shared 'single view of the truth'. This eliminates the need for a firm to reconcile their copy against a centralised view or another parties view;
- there is no single point of failure. If other parties in the blockchain network are down (maybe through a fault in their application or a networking issue) the other parties can access their records and transact;
- different parties can have different 'permissioned' roles. For example, we created a 'regulator' role for the POC that is able to see all transactions but not participate;

If the following conditions apply, then blockchain has strong potential to provide a solution:

1. **Multiple parties share data** – multiple participants need views of common information
2. **Multiple parties update data** – multiple participants take actions that need to be recorded and change the data
3. **Requirement for verification** – participants need to trust that the actions that are recorded are valid
4. **Intermediaries add cost and complexity** – removal of 'central authority' record keeper intermediaries have the potential to reduce cost (e.g. fees) and complexity (e.g. multiple reconciliations)
5. **Interactions are time sensitive** – reducing delay has business benefit (e.g. reduced settlement risk, enhanced liquidity)
6. **Transaction interaction** – transactions created by different participants depend on each other.

If you can't tick at least four out of six ask "why blockchain"?

- the technology provides an excellent, complete and tamper proof history complete with time-stamping. This can reduce disputes and eliminate fraud and enhance auditability of the transaction history.

To select the business process that we would base the PoC around we conducted meetings with PwC's insurance specialists, who have worked in many roles, from brokers to underwriters in many major insurance organisations. These people effectively played the role of the business stakeholders that are vital to the agile development approach that we followed. When preparing the stakeholder group for initial idea discovery workshops we provided them with guidance using PwC's six questions approach. For example, if the following conditions apply, then blockchain has a strong potential to provide a solution:

- Multiple parties share data
- Multiple parties update data
- Requirement for verification
- Intermediaries add cost and complexity
- Interactions are time sensitive
- Transaction interaction

APPROACH FOR THE POC

The development team was made up of the following roles: Product Owner, Delivery Lead, Solutions Architect, Software Engineers and Test Engineer. Each team member was involved at various times, in the full end-to-end development process, from ideation, to design, right through to execution. We strongly encourage close collaboration between all members of the development team at each stage of the process. In all seven people took some part in the PoC development.

At the outset we held ideation workshops to identify the priority business applications ('use cases') that we would focus on. Within the confines of this exercise these were conducted utilising the in-house insurance expertise of PwC. These sessions identified a wide range of potential use cases within the wholesale insurance market, from KYC, AML, claims management, and settlement to reinsurance. All of these have unsurprisingly also been identified by participants in this survey. Having discussed the use cases at length, we made the decision to base our PoC specifically on Policy Placement. Whilst we recognised that certain markets have or are developing automated solutions for this (PPL in London for example) the team felt that it is a natural starting point, and forms a substantial contribution to the pre-requisites of the other use cases identified. It was also felt that it was a sufficiently broad process to provide an opportunity for our PoC to highlight the unique blockchain capabilities defined above. Finally, it was felt that this process would be sufficiently familiar to all participants including international firms, to make the PoC meaningful.

Progressing from these introductory sessions, we moved to use case development, where we began to investigate at a lower level, concentrating on the current process and clearly identifying agreed problem areas. From this we commenced brainstorming on how blockchain could be implemented to help solve the current issues. Our approach to such an activity is primarily white-boarding and sketching. By removing the technology at this point, it allowed the entire team to focus and share an understanding of what we were trying to achieve, what we were going to build, who the end user would be and what the Minimal Viable Product (MVP) requirements were.

An identical approach was followed in the product definition stage. The initial whiteboard sessions concentrated on illustrating the breakdown of the use case into features, with this stage's objective being to list the potential features we could include within our PoC, and define what our MVP would be from this. Within product development, by definition the MVP is a product with just enough features to gather validated learning about the product and its continued development. To achieve this, we reviewed the full range of potential features we could cover and prioritised these, using a defined set of criteria:

- what benefit would this bring to the end user, and the wholesale Insurance market as a whole?
- how will this prove out specific blockchain capabilities we want to illustrate?
- what would the development effort be?
- can this be achieved within the short timeframe of five weeks?

At the end of this stage, we had a prioritised list of what we believe would satisfy the use case and demonstrate the key benefits of Blockchain functionality, and could be successfully developed by the deadline.

The Product Design stage requires buy-in from the entire development team, to ensure that the whole team are committed to delivering within the fixed timebox. Throughout this stage we identified who were the end users we would represent within the scope of the PoC, selecting the Broker, the Insurer, the Regulator and the Policy Holder. We considered what the PoC process flow would be, clearly recognising the functionality limitations dictated by time-scales, outlining assumptions and avoiding low level details and features. This resulted in a high level process overview. This is followed by the User Interface (UI) design of the application, which defines how an end user will interact with the product. This outlines the end user's navigation flow throughout the application which is vital as the product execution commenced.

To deliver the PoC, the team retained an agile approach, being flexible to adapt to changing needs and ensuring focus on the highest priority task. The PoC was delivered in an iterative fashion, working in weekly sprints for the 5-week duration of the project. The goal was to have a working prototype at the end of each week, allowing weekly demonstrations to our internal subject matter experts. Completing this on a regular basis provides an ongoing stream of feedback, ensuring we were not straying from the original goal, we had not made any erroneous assumptions, and reaffirming that at all times we were working on the correct features

In the time-frame allowed we were not able to gather significant feedback from participants in the interviews, which in a real development we would clearly have sought. Following input received at a workshop 3 weeks into the study, however, we were able to adjust the PoC to add some features that illustrated specific points that study participants had raised.

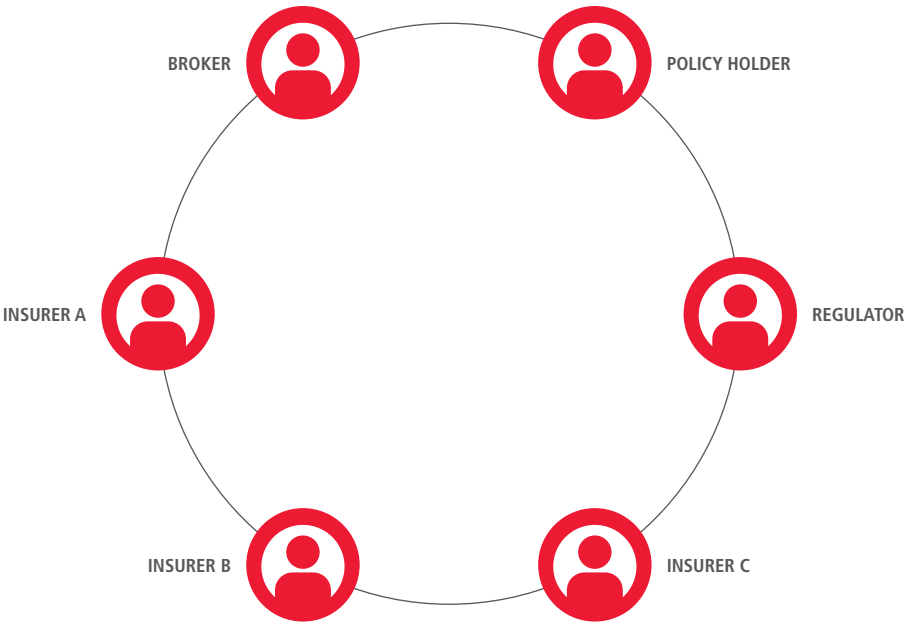
THE FUNCTIONAL SCOPE OF THE POC

The PoC itself represents a high level policy placement flow, allowing a Broker to create a digital policy which is shared on the blockchain. An Insurer can view policies on the blockchain, and make offers to back risk on a particular policy, with the Broker having the ability and control to accept or decline these offers. This communication and negotiation between parties takes place all within the blockchain. When a policy is fully backed, a formalised insurance Contract is created and again shared on the blockchain. This gives visibility to the Regulator and Policy Holder actors (used in the sense of 'participant in the process'). This is graphically detailed below.

When we demonstrated the application we were able to highlight the ways in which it illustrates a number of features for blockchain that provide elegant solutions for issues raised in the report:

- **Orchestration of multiple roles:** "… allows more efficient workflow for all parties, without the need for a central authority"
- **Distributed with no central authority:** "… a central third party … because, without choice, the natural monopoly rents might become excessive. Many historic market reforms failed to propose solutions that recognised this market structure."
- **No Single Point of Failure:** "… as there is no single central authority resulting in no risk of a single point of failure."
- **Timestamped:** "Timestamps can be used to prove that data elements were entered at or before a certain time and have not been altered. A blockchain is a super audit trail"
- **Traceability:** "Placement: It is difficult to create an adequate audit trail to show the exact documents and versions included"
- **Immutable Tamper Proof:** "Proof of insurance – as an example, before an aircraft takes off it has to provide a proof that it is insured … instant confirmation of insurance by each airport".

CHAIN REACTION



THE TECHNOLOGY FABRIC FOR THE POC

The blockchain technology landscape is evolving rapidly and there are multiple technology platforms that we could have chosen to use as the core. Given the short term and experimental nature of the PoC we used our knowledge, from our on-going research into blockchain technology, to quickly identify a candidate chain that would allow us to rapidly build the PoC..

We considered the potential benefits of smart contracts as the team have experience building with both Ethereum and Eris. For some more complex transactions the ability to capture conditions in code are very valuable. However, for this PoC we felt that the business logic required does not have to belong in the chain and that other features might be more important to this specific application.

When taking all the required features into consideration, we narrowed the choice to MultiChain, a platform that the team had limited experience of as it gave us the opportunity to try the technology out and learn more about it, adding to the experimentation and learning.

MultiChain builds on bitcoin technology offering a native asset support with atomic swaps and the ability to append custom data to transactions. The ability to create custom assets allowed the mapping of a policy to a custom asset within the chain. The policy details recorded as a JSON object (which is a standard for data interchange) within the metadata. Each insurer on the chain would then see this transaction, notifying them that a new policy is available to underwrite. The Insurers could then choose to underwrite the policy by creating a MultiChain offer with the percentage of risk that they want to underwrite, the premium amount and the terms attached to the offer.

IMPLEMENTING THE FUNCTIONALITY

One early challenge to face was how to share an insurer's offer with the broker, as offers are not published on chain. We wanted to ensure that we could do this on chain, so we adopted a MultiChain beta feature called data streams. Data streams allowed us to store arbitrary data permanently and immutably in the chain. We carried out a quick development spike to validate this approach before iterating on the create policy feature to add an address to receive offers for that policy. The insurer could then send the offer to this address notifying the broker that there is a new offer.

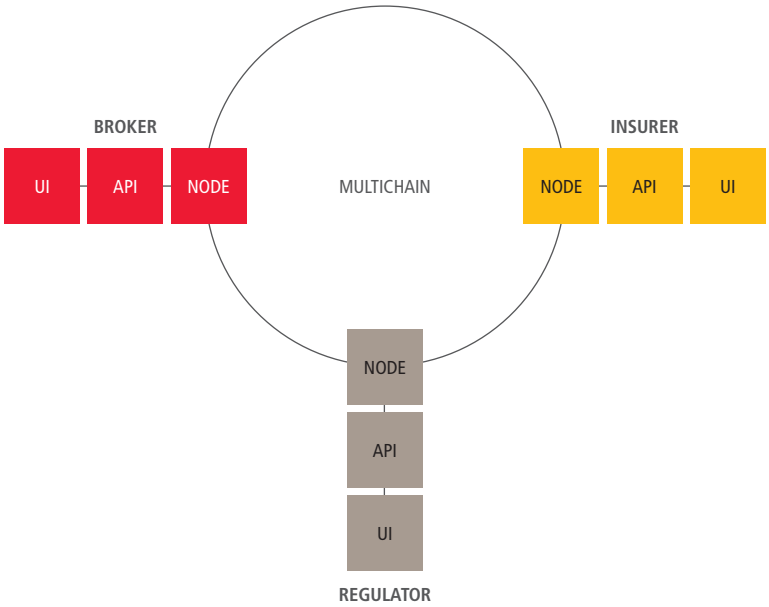
When a broker decides to accept the offer after reviewing the premium and any terms attached, they complete the transaction and broadcast it on the network. This sends the percentage of the risk to the insurer. Everyone on the chain can then see the details of the policy, and the terms that where attached to the offer.

We encapsulated this business logic in a RESTful API which also provided web sockets, abstracting away the fact that the storage mechanism was a blockchain. The API's allowed us to separate the logic and to concentrate on development of an effective user interface to help visualise the process.

We packaged each application and all their dependencies in Docker containers, published, tested and deployed on a swarm running in AWS cloud infrastructure. Our continuous deployment pipeline enabled us to rapidly add features to the product without comprising on quality.

See diagram below for the high level architecture:

CHAIN REACTION



Each actor in the system has their own application stack consisting of a node, the API and the UI. The system is highly resilient as there is no central party; each of the nodes are connected together to form a peer-to-peer network and nodes can connect and disconnect without impacting on other nodes.

CONCLUSION

As with any initial PoC, this exercise has been a learning and discovery phase, concentrating on a small piece of a much bigger jigsaw.

When we compare what the PoC illustrates to the key themes that have emerged from the study and that are documented in the body of the report we see many issues echoing in features that the PoC addresses.

- Ability to reduce manual paper flow and reduce rekeying and duplication of data
- Provision of a time stamped audit trail that could reduce disputes about when an insurer is 'on risk'
- Opportunity to reduce the effort associated with reporting to regulators and others
- No single point of failure/processing bottleneck in a process
- Ability of the policy holder to show a tamper proof immutable record of their being insured.

Many of the priority areas that warrant further consideration have been outlined in the main body of this report and all are worthy of consideration. Like any change that will lead to great improvement in such a complex area as wholesale insurance, there is a need to begin somewhere. In the words of Lao Tzu: "The journey of a thousand miles begins with a single step".

So, what's next?

Glossary

Actor	A participant in a process
API	Application program interface – definition of how different software components interact
Blockchain	The computer file underlying a mutual distributed ledger. It comprises a series of blocks of data added sequentially. Once a block is added it can never be deleted or changed. Each block includes a header section with index information and hash code(s) that ensure that data cannot be changed without making the entire file inconsistent.
Cedent	Party insured by a reinsurance contract or treaty (also 'cedant')
Cryptocurrency	A medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency (Andy Greenberg, Forbes.com, 20 April 2011. "Crypto Currency".)
Digital Currency	A currency where the units of value exist only on a computer file
EEA	European Economic Area: Treaty area comprising all countries of the EU plus Iceland, Lichtenstein, and Norway, giving these three named countries access to the EU 'Single Market'
Fork	A situation in which two rival versions of a blockchain exist simultaneously. A viable blockchain implementation must contain a mechanism to resolve forks in order to create a single agreed version.
General Data Protection Regulation	An EU Regulation (2016/679) strengthening and unifying protection of data on individuals in the EU
Geolocation	The physical location of an object such as a cargo container or an internet-connected computer
GWP	Gross Written Premium is the total insurance premium received by an insurer. This is in distinction to NWP defined below which offsets reinsurance premium paid by the insurer.
Hash	The digital signature for a file produced by a hash function
Hash function	A cryptographic function which provides a digital signature (a 'hash') for any computer file with the property that it is computationally impractical to find a second file with the same hash.
ISO	International Organisation for Standardisation – owns ISO standards
KYC/AML	Know-Your-Customer/Anti-Money-Laundering and related processes such as sanctions screening and identification of ultimate beneficial ownership which are ongoing requirements during the lifetime of a financial relationship.

MDL	Mutual Distributed Ledger – the output of the underlying blockchain technology. A tamper-proof updatable record which can be co-owned by multiple users with no central point of control
MVP	Minimum Viable Product – in a systems specification the functionality to meet minimum user needs
Node	The computer of a user of a blockchain, holding a copy of the chain and performing operations on it. These operations may be restricted to receiving updated versions and reading, but for at least some nodes must involve validating, updating, and broadcasting
NPV	Net Present Value used in evaluating the value of an investment as the current value of projected future cashflows
NWP	Net Written Premium – GWP less 'ceded written premium' – i.e. less premium paid to a reinsurer to take on some of the risk.
Permissioned blockchain	A blockchain which can be updated and validated only by users with explicit permission
PoC	Proof-of-concept – a pilot project demonstrating that a design concept is feasible
Point solution	A change implemented in a single organisation
PPL	Placing Platform Limited – electronic placing platform for the London Market to allow brokers and insurers to quote, negotiate, and bind business
Process-level change	A change implemented amongst a number of participating organisations rather than across a market
Private blockchain	A blockchain visible only to authorised users
Proof of work	A methodology for regulating update of an unpermissioned blockchain by giving preference to users devoting the most computing resources to the process. Bitcoin uses this methodology.
Proof of stake	A suggested methodology for regulating update of the unpermissioned blockchain underlying a cryptocurrency using a voting system with votes pro rata to holdings of the cryptocurrency.

Public blockchain	A blockchain broadcast freely to anyone
Quantum computer	A proposed computing machine which uses 'mixed' states of elementary particles to store data and thus has greater computing power than existing technology for certain – but not all – applications. The essential idea is that it can process a mix of 1s and 0s at the same time, rather than sequentially.
RSA	RSA Encryption – A public key/private key encryption methodology used extensively in electronic communication
SHA-256	A hash function defined by the USA National Institute of Standards and Technology (NIST) and in widespread use
Smart contract	A contract embedded in a blockchain which executes automatically when its trigger conditions are met
Sprite	A smart contract or a non-contractual computer program embedded in a blockchain which executes automatically in defined circumstances.
Treaty	An insurance contract between a reinsurer and an insurer (the cedent)
UI	User interface: 'everything designed into an information device with which a human being may interact' (Techtarget.com)
Unpermissioned blockchain	A blockchain which can be updated and validated by any user
XML	Extended Markup Language – a schema for defining data elements

Bibliography

'Blockchain' gets over 8 million Google results, 'Wholesale Insurance' over 69 million. This bibliography contains several relevant articles which the report authors have found particularly illuminating, and makes no pretence to be a systematic review. All of the items should be available through an internet search.

Acord & Equinix. "Challenge to Change Part 1 Embracing the Economy, People and the Future of Insurance", Industry report, Equinix, January 2014.

Acord & Equinix. "Challenge to Change Part 2 - The Impact of Technology2. Industry report, Equinix, January 2014.

Acord & Equinix. "Challenge to Change Part 3 - The Future of Insurance". Industry report, Equinix, January 2014.

Bruce, J.D. "The Mini-Blockchain Scheme." January 2014. (Suggests architectures which prevent the size of blockchains ballooning over time)

Buterin, Vitalik. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform". April 2014.

De Filippi, Primavera. "Legal Framework For Crypto-Ledger Transactions." 2014.

Gupta, Vinay. "Programmable Blockchains in Context" Medium.com, October 2015

IBM DeveloperWorks: "A Case For Permissioned Blockchains", April 2016.

Mainelli, Michael and von Gunten, Chiara "Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance" December 2014.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." White paper, 2009.

Swanson, Tim., "Consensus-As-A-Service: A Brief Report On The Emergence Of Permissioned, Distributed Ledger Systems". 6 April 2015.

Vasin, Pavel. "BlackCoin's Proof-of-Stake Protocol v2". White paper, 2014.

Walport, Mark, UK Government Chief Scientific Adviser "Distributed Ledger Technology: beyond block chain". 2016

World Economic Forum. "The Global Information Technology Report 2014: Chapter 1.5 Managing the Risks and Rewards of Big Data". Industry report, World Economic Forum, 2014, 61-66.

The Long Finance initiative grew out of the London Accord, a 2005 agreement among investment researchers to share environmental, social, and governance research with policy-makers and the public. In 2007 Long Finance was established more formally by Z/Yen Group and Gresham College with support from the City of London Corporation with the aim of exploring long-term thinking across a global network of people.

"When would we know our financial system is working?" is the question underlying Long Finance's goal to improve society's understanding and use of finance over the long term. In contrast to the short-termism that characterises today's economic views the Long Finance time-frame is roughly 100 years. Long Finance aims to:

- expand frontiers – developing methodologies to solve financial system problems;
- change systems – provide evidence-based examples of how financing methods work and don't work;
- deliver services – including conferences and training using collaborative tools;
- build communities – through meeting, networking and events.

Long Finance runs programmes exploring four major themes:

- **London Accord** – looking at environmental, social, and governance investment research issues;
- **Financial Centre Futures** – seeking to explore how finance might work in the future;
- **Meta-Commerce** – aiming to identify and structure the critical questions underlying the long-term viability of the financial system;
- **Eternal Coin** – encouraging a global discussion on the nature of money and the concept of value.

www.longfinance.net

Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
T: +44 (20) 7562-9562
E: hub@zyen.com
www.zyen.com

THE Z/YEN GROUP OF COMPANIES

Michael Mainelli
Executive Chairman
+44 (0) 20 7562 9562
michael_mainelli@zyen.com

Bernard Manson
+44 (0) 78 7911 8875
bernard_manson@zyen.com

PwC

Stephen O'Hearn
PwC Global Insurance Leader
+41 (0) 44 628 0188
stephen.ohearn@ch.pwc.com
Twitter: @stephen_ohearn

Jonathan Howe
PwC UK Insurance Leader
+44 (0) 20 7212 5507
jonathan.p.howe@uk.pwc.com
Twitter: @JonathanHowePwC

Steve Webb
PwC UK Financial Services Blockchain Leader
+44 (0) 20 7804 1597
steve.webb@uk.pwc.com