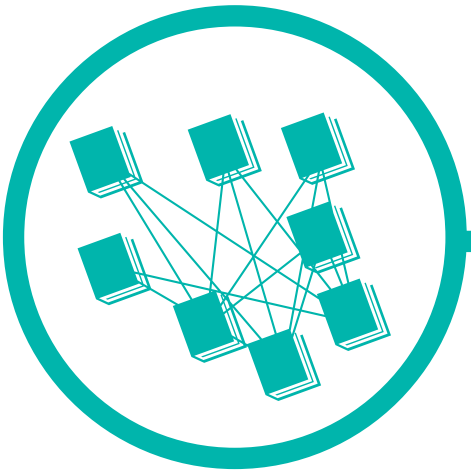
LegalWeek THE BRITISH LEGAL AWARDS 2016 WINNER

WINNER LEGAL BUSINESS AWARDS 2016 LAW FIRM OF THE YEAR

Pinsent Masons

appliedblockchain



Smart insurance contracts

A discussion paper by Pinsent Masons and Applied Blockchain on applications of blockchain, distributed ledger technology and smart contracts for the insurance sector

Tim Roughton
Partner TMT
Pinsent Masons LLP
T: +44 (0)20 7418 8200
M: +44 (0)7468 710904
E: tim.roughton@pinsentmasons.com

Peter Bidewell
Chief Marketing Officer
Applied Blockchain
M: +44 (0)7495 179727
E: peter@appliedblockchain.com

Pinsent Masons

At Pinsent Masons, we understand that Fintech has been hyped beyond all measure. But we also know that Fintech is transforming financial services forever and changing the way in which we think and talk about money payments and finance.

Whether a global bank, a leading insurer, wealth provider, emerging Fintech company or technology provider, we can help you navigate the ever changing legal and regulatory frameworks and the technology and data risks that may otherwise stand in your way.

We help you so that you can focus on innovating.

Applied Blockchain

Applied Blockchain is a blockchain applications development company, focusing on distributed ledger technology and smart contracts. Based in the Level39 Fintech Accelerator in Canary Wharf, London, Applied Blockchain has an expert team of in-house blockchain developers that have been building solutions for two years. The company is self-funded and has built private blockchain applications that are now live in production environments, being used by real customers.

The company founders each come with 20+ years' experience of enterprise IT architecture, big data, AI, integration and solution delivery in telecoms and banking. Using this experience, Applied Blockchain builds solutions that incorporate components such as privacy, security and integration, independently audited by third parties, and ready for use by enterprise clients that operate in regulated markets.

Blockchain up until now

For some time it had been a common misunderstanding that Bitcoin and blockchain were one and the same thing – a new technology used as a digital form of currency. However, in the last couple of years we have seen the emergence of next generation blockchain platforms, such as Ethereum and Hyperledger, which have moved far beyond the purely transactional ledgers of platforms like Bitcoin.

Unlike Bitcoin, however, these next generation platforms have a Turing complete programming language, which means that applications or programs can be built straight on to the blockchain. The result is a global computer, with a globally distributed database of information, where each member of the network has a perfect copy of all of the same information that is stored in a way that can never be retrospectively changed or tampered with – an immutable ledger.

Ethereum as an example

Ethereum is an open source platform that, like Bitcoin, is distributed in such a way that anyone can gain access and begin making transactions. Despite the $1 billion of value stored within the network, offering a large incentive for the world's most sophisticated hackers to attack the system, the platform's core protocol has never been compromised. This is due to the consensus mechanism that is native to almost every blockchain, which requires an attacker to gain control over half of the members of the network simultaneously in order to perform a successful hack. Ethereum, for example, has around 6,000 members, or nodes, that are randomly distributed all across the world, resulting in a very secure network indeed.

Smart contracts can offer real benefits to the insurance industry: they can simplify and automate processes, increase standardisation, offer electronic execution, provide immediate integration of contracts into data pools and self-execute.

Better than a centralised database?

An important difference between a traditionally centralised database and what we might call a 'distributed blockchain database' is that there are many copies of the same information, stored by many different members of the network, but all using exactly the same data format and structure. The benefit of this is two-fold.

1. **Reconciliation:** as all members have their own perfect copy of the same data that is stored in the same data structure, there is no need to reconcile data, nor is there the need for arduous integration work to connect the different systems together – everyone is singing from the same hymn sheet. This greatly reduces the cost to run the system and facilitates connectivity by default.

Why does all this sound familiar?

A comparison that is often drawn is that blockchain is very similar to the internet, in that there is a global network connecting people or businesses together. Users can interact with the web applications on the internet via user-friendly screens, store their data in a database on a centralised server and interact with others on the same network. Distributed blockchain applications have the same familiar user interface screens, which can be accessed by typing an IP address into a web browser and operated by the user in the same way they are used to with normal websites today.

The key difference is that each user has their own copy of the application and database, where any updates to the system are then transmitted and logged by all other members on their copy of the database. The innovation is in keeping all copies of the ledger exactly the same, in real time, for every member of the network.

2. **Optimised for multi-party interaction:** for a global computer to operate, the code underpinning applications needs to operate and execute in exactly the same way and all at the same time for everyone on the network. As all the members of a blockchain network have a perfect copy of the same code and data, distributed applications operate and behave in exactly the same way for all members across the entire global network. This permits completely different types of applications that were not possible until now, as disparate parties can work directly with one another in a peer-to-peer manner to take actions logically, automatically and in real time, just like one large computer processor.

Smart Contracts in focus

More recent platforms include smart contracts. The term 'smart contract' has no settled definition – it can mean one thing to a blockchain technologist and quite another to a lawyer. Some of the definitions used include *"autonomous machines"*, *"contracts between parties stored on a blockchain"* or *"any computation that takes place on a blockchain"*.

The person widely credited for inventing the idea of a smart contract is Nick Sambo. He defined the term as *"a set of promises specified in digital form, including protocols within which the parties perform on these promises"* [1]. This definition pre-dates the invention of the blockchain. He gave the example of a drinks vending machine – when the money is paid and a drink selected, an irrevocable set of actions is put in place to execute the purchase and delivery of a drink. Effectively, the contractual terms of the purchase of drink are embedded in the hardware and software that runs the machine.

This contract may be 'smart' because it automates performance of promises made. The vending machine automatically makes good its promise to give you a drink once you have inserted your coins. However, note that even in this smart contract context, the vending machine owner or operator and the customer have both agreed to transact by way of this automated process.

While a smart contract may be viewed as a container of code and data in one sense, there is a wide range of possibilities as to what that code and data might do. At one end of the spectrum, the code could constitute a record of contractual interactions and replace the need for a natural language contract. At the other end of the spectrum, the code could simply execute agreed business logic (eg. a payment) based on contractual parameters that are agreed or expressed outside of the

'Permissionless' and 'permissioned' distributed ledgers

A permissionless ledger is one which allows, on a public network, any person to access it, submit messages to it and be involved in the authentication and validation of transactions made on it. Bitcoin is an example of a permissionless ledger. A permissioned ledger, on the other hand, is a ledger where its participants are subject to entry criteria. Entry may be controlled by, for example, compliance with 'know your client' (KYC) requirements or by the approval of an administrator of the ledger. A permissioned ledger may be accessible over a public or private network.

Typically, permissionless distributed ledgers are controlled by no-one and its participants are pseudonymous. These features raise a number of legal questions and challenges. If no-one has control of the ledger, who is accountable for its operation? How does a participant seek redress? Who or what should be regulated and by whom? What is the applicable jurisdiction? Who is the data controller on a distributed ledger and who is liable for data breaches?

Many of these legal challenges can be overcome or reduced by the use of a permissioned system. A permissioned system will, to some extent, be controlled by a central authority. This makes questions of responsibility and accountability more straightforward. As entry is controlled, jurisdiction can be controlled. Regulation of known participants is more straightforward and participants are more likely to be able to seek redress against other participants if entry is conditional upon signing up to clear contractual rights and obligations.

[1] Smart Contracts, Building Blocks for Digital Markets, 1996

code. There is a range of intermediate possibilities, including a hybrid model, where digitised performance is encoded in computer code with wider contractual terms written in natural language.

Benefits of smart contracts

One of the key benefits of smart contracts is that data can be encrypted and stored within this container, locked with a private key to which only the user has access. Public keys are then shared to other members on the network to interact and make transactions. For a simple comparison, a public key is similar to an email address, while a private key is similar to the password to a user's email account. Smart contracts are also a way to translate business process logic into computational logic; a way of codifying process workflow to automatically self-execute when certain conditions are met.

As all members of the network have exactly the same copy of the application and the data stored within secure containers, smart contracts can be designed in a way to use logic to automate process workflow between different members of the same network that may not trust one another, want to share all their data, nor want to trust a centralised authority.

The secret to this is itemised data privacy. Unlike the pseudo-anonymous nature of the underlying platform, where everyone can see all of the transactions that take place, but have no visibility on the identities of the parties behind the transactions, businesses want the opposite – to know the identities of the members transacting, but not share the specific transaction values.

This enterprise necessity is not native to blockchain platforms, but has been solved by a select few blockchain development providers. With itemised data privacy, members can dynamically permission access to specific components of encrypted data to different parties at the right time during a certain logical process. This means that only the specific pieces of data that are needed to take the next step are accessed, by the right parties, and only for the window of time that they are needed to make the decision.

Blockchain is a new way of connecting different parties on a single network, where all members have their own copy of the entire history of all transactions and events that have been logged in a way that can be retrospectively verified, but not altered. Leveraging smart contracts and data privacy, members can create logical workflows to run distributed applications, while keeping their private information securely encrypted, resulting in a very secure system with no single point of failure that could be subject to a cyber security breach.

This is a stark contrast to the frequently reported traditional database breaches, such as that reportedly experienced by Yahoo in 2016 where it was said that data had been stolen from an estimated 500 million users.

See BBC News coverage: http://www.bbc.co.uk/news/world-us-canada-37447016

Applying blockchain to insurance

We are now seeing consortia, such as B3i, forming in the insurance sector to explore opportunities for the application of blockchain, distributed ledger technology and smart contracts. There are a number of features of the insurance sector that align to the features of blockchain:

Insurance sector features:

- insurance is heavily reliant on documentation, data analysis and databases – inefficient solutions are currently being used for recording and evidencing the relationship between parties in insurance contexts;
- insurance involves many parties or actors including consumers, brokers, aggregators, platforms and insurers – distributed networks make sense in this context where all parties can interact on a single blockchain using standardised data sets and protocols;
- insurance is a heavily intermediated industry; intermediaries add cost and complexity – the removal of a 'central authority' record-keeper has the potential to cause distribution disruption by reducing cost (eg. fees) and complexity (eg. multiple reconciliations);
- Internet of Things (IoT) data and telematics data lend themselves to storage/tracking and encryption on a blockchain;
- customer onboarding issues remain a concern for insurers – authentication/verification through the blockchain can provide a way forward; and
- reducing fraud and other financial crime is a key concern for insurers and their regulators – blockchain promises immutable records and tracking.

An insurance use case in seven steps

To better visualise the added value of blockchain technology in insurance, it is useful to apply the concepts to a real-world worked example. In this example, we will explain the user journey for a blockchain marketplace application that connects customers and insurers for home flood insurance, identifying the specific value add of blockchain at each stage.

Step 1

A customer types in the website address into her browser, exactly as she would with any non-blockchain web application, and signs up to the platform by entering her email address, password and details of her property.

Step 2

Upon sign-up, the customer is issued a public and private key, where the latter can be stored securely on her device or in her browser.

What is a private key?

Private keys are unique to the individual user and are used to sign transactions or confirm important events. Private keys are only accessible by the individual and held in a secure place, such as the secure enclave on a mobile device. This greatly improves the security of transactions compared to a simple username and password of a non-blockchain platform.

Legal analysis of steps 1 and 2

- At this stage, there is very little difference between a consumer using the blockchain platform as opposed to any other aggregator/insurance quotation platform. Accordingly, the same legal considerations would apply, including data privacy, acceptable use and ensuring the blockchain platform operates in accordance with applicable consumer and e-commerce law (for example, ensuring adequate cookie consent notices where applicable).
- In particular, insurance-specific regulation shall apply. In the context of a blockchain platform directed at UK customers, the use of blockchain will not water-down the need for such insurance firms to comply with the Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) requirements. Whilst such rules and guidance are not currently tailored to the use of blockchain, insurers using the platform will still need to consider applying best practice and interpreting the FCA's High Level Principles to ensure good customer outcomes.
- At the point of signing up to the platform, the customer can be required to agree to terms and conditions applicable to the platform. The terms would govern the customer's use of the platform and, potentially, the terms and conditions of any products or services procured through the platform.

Step 3

The customer receives and installs a number tamper-proof flood detection devices to be installed in various locations in her home. These devices each have a hardware-secured private key of their own, a GPS locator, a built in camera, and an ability to detect and send water level information signed using their own private key.

More detail:

- This data is encrypted and stored securely within a smart contract on the blockchain, as part of the customer's account, using her device's private key.
- Unlike a traditional web application, where private customer information is stored centrally in one server by the platform owner, the blockchain shares a perfect, but encrypted, copy of the customer data across each node of the network, resulting in no single point of weakness vulnerable to an attack.
- As the customer and her devices hold their own private keys, the platform can even be set up so the platform owner cannot access her data, meaning far greater data privacy.

- A traditional database model requires the platform owner to be the custodian of the data. If an attacker breaks into the centralised database then they will have complete access to all of the data, as the data is not encrypted inside the database.
- A blockchain solution, by comparison, allows for the encryption of each individual item of data stored within the very secure distributed database, meaning that even if an attacker were to gain control of the system, the data within remains private.

Legal analysis of step 3

The data uploaded by the consumer will, to some extent, constitute personal data. Therefore, it is essential that controls are put in place and the blockchain is constructed in such a way as to protect that personal data as required by law.

The first question that will need to be assessed is who the data controller is and who would be liable to both the data subject and applicable regulator for data breaches. As the ledger in this instance would operate as a permissioned blockchain, it is likely that the consortium entity would be the data controller in the first instance. The governance of that entity would then need to assign responsibility and liability accordingly (for example across the consortium members). However, once a contract for insurance is entered into between the consumer and the insurer the insurer may then be considered a data' controller and the consortium entity a data processor.

European data protection laws place restrictions on the processing of personal data outside of Europe without adequate protections being put in place.

The distributed nature of the blockchain raises questions as to where and how data can be accessed and used. This risk can be managed, to some extent, through access controls on the permissioned ledger and governance of the consortium (for example by requiring that those consortium members abide by certain rules as to the location of the processing of personal data).

Data protection laws also prohibit data controllers from storing data for longer than is necessary and give data subjects the right to request deletion of their data. On the face of it, the immutable and everlasting nature of the blockchain ledger conflicts with these requirements – it is not technically possible to delete personal data from the ledger. It is arguable that the characteristics of the blockchain make the permanent storage of the personal data 'necessary' and thus permissible. This will probably be valid if the reason for the permanent storage is justified and communicated to the data subject. It may also be possible to destroy the encryption key to the data, effectively achieving deletion.

To avoid the strict requirements of data protection law, cloud service providers often use the argument that, if data is encrypted, it does not constitute personal data because, without a key, a living person cannot be identified from the encrypted data. A similar argument could be used in respect of encrypted data on a distributed ledger. If data only constituted personal data in the hands of the person holding or having control over the key, the scope of data processing caught by the law will be narrowed and therefore easier to control and regulate.

Although the challenges presented by data protection obligations are complex and need to be carefully considered, there is no underlining reason they cannot be overcome.

These complex structures are common in the insurance market due to the number of intermediaries involved in the purchase and maintenance of insurance cover.

Processes and contractual arrangements exist between the players in the insurance market today and could also be so established within a permissioned distributed ledger – the considerations and application are just more complex. To achieve this, it will be essential to have a clear understanding of the architecture of the blockchain and the legal framework in place to manage the risks and responsibilities of the parties accordingly. This will need to be clearly and comprehensively provided to consumers so they can make an informed decision about the permissions they grant and the subsequent rights they have.

Step 4

The customer decides that she wants to receive an offer from an insurance company, and so requests a quote by permitting the insurers on the platform to access her flood detection devices and any personal information that may influence the quote they receive.

More detail:

- Rather than only basic information being provided, or too much information that is not relevant to receiving a quote, the customer can dynamically provide permissioned access to only the specific items of data that are relevant, and only for the period of time required by the insurer to return a quote. This can be as simple as a slider option to enable or disable access to certain categories of data.
- Additional integrations to third-party data sources may also be in place for KYC or further risk profiling. The platform operator/ consortium, could agree or stipulate the KYC requirements, which can then be relied on by the insurer participants.
- A smart contract between the insurer and the customer enables all of the relevant customer data to be provided and matched against the pre-defined risk criteria of the insurer, resulting in a perfectly tailored quote being automatically issued to the customer by the insurer.
- Information provided from a traditional database can still be itemised in this way, but often this involves some kind of conversion or reformatting for it to be entered into the insurer's system to provide a quote. A blockchain solution solves this by having all parties working from the same data structure.

Legal analysis of step 4

- In this example, such a platform would be set up as a permissioned ledger and a consortium of insurer members is likely to be established. An insurer or other participant could only become and remain a member to the extent that it accepts and adheres to a set of rules and corporate governance in order to participate.
- A group of competing insurers agreeing to do something together could, on the face of it, raise competition law concerns. Accordingly, it will need to be demonstrated that the justifications for operating the consortium (and

using the blockchain) outweighs any potential negative impact of the consortium: being able to show the potential benefit the blockchain will produce to consumers would be an argument to support this position. Other factors would also need to be considered in the operation of the blockchain to avoid competition law concerns. The construct of the blockchain will need to allow each insurer to continue to act independently. The pricing and product information of each insurer must only be visible to that insurer and kept confidential. What further data that can be extracted from the blockchain, and the value in the analysis of such data, will need to be considered. For example, statistics regarding the number of policies, claims, new products, changing products could (depending on how such is made available) be endless and the analysis of this would need to be managed to ensure no sharing of commercially sensitive information between insurers.

- The implications of 'big data' are becoming increasingly of interest to competition law authorities. Given the power, information and opportunity such data (and more specifically big-data) creates, it must be considered whether the blockchain would create a product with a large degree of market power (eg. by becoming an 'essential facility') in the market. It may be that competing platforms would need to be provided with some access or right to the information available on the blockchain to ensure that competition law concerns do not arise.
- The consumer benefit and demand for the blockchain is likely to justify many competition concerns. Nevertheless, it will be imperative to establish a suitable structure to govern the relationship between the insurers in the consortium and design the architecture of the blockchain itself to mitigate such risks.
- Adding to the complexity of the above is the increasing global harmonisation of the insurance market. To derive the benefits of this operating model, insurers are likely to want to allow consumers operating in multiple jurisdictions to use a single blockchain. Accordingly, the legal and regulatory considerations must be considered in each jurisdiction within which the products may be purchased. While the increasing harmonisation of global insurance regulation will assist this, it will still no doubt require the navigation of complex legal and technical hurdles.

Step 5

The customer either manually selects their preferred quote or, if the platform has been designed to do so, the best quote is automatically selected for the customer, based upon their own preferences and pre-sets entered into their profile. The customer then confirms their acceptance of the offer.

More detail:

- The offer is confirmed by the customer signing the transaction with their blockchain private key. This can be done via biometric authentication (such as TouchID on the iPhone) if the private key is stored on the device, or by verification through the customer's browser.

- At this point, the customer enters into a legally binding smart contract with the insurer that will self-execute and automatically release payment if verified proof is given that the house has been flooded.
- A direct debit of the agreed monthly amount is initiated by the smart contract to be paid on the first day of each month.
- Compared to a traditional database, this entire process can take place in seconds, rather than several minutes of entering their payment information.
- If selection of the best quote is automated using smart contracts, then the entire process from providing permission for insurers to view customer data to signing the agreement with a private key and initiating the payment could take just a few seconds.

Legal analysis of step 5

The use of smart contracts in this context begs the question as to whether a smart contract can be legally binding and enforceable. To form a legal contract in the United Kingdom, certain basic requirements must be met: there must be an offer from one party that is accepted by the other; there must be consideration (the exchange of some form of value from both parties); there must be certainty of terms and there must be an intention to create a legally binding relationship.

- A key point to highlight here is that not all contracts need to be in writing to be legally binding. What is essential, however, is that the parties to the contract intend for their promises to be performed in the way in which the smart contract enables fulfilment of those promises to occur. There must also be certainty as to what those promises are.
- Smart contracts that exist purely in code and not in natural language are, therefore, theoretically possible. The legal requirements for a valid contract are, however, much more difficult to meet for smart contracts where natural language contractual terms may not be immediately obvious or available to a 'contracting party' or where the contract self-executes without the ability for a customer to accept (or refuse) the terms. How can a customer have accepted an offer on certain terms if those terms have not been communicated to her in a form she can understand? However, where natural language contractual terms are clear and accepted by a contracting party who consents to a business outcome being self-executed by the smart contract code in agreed circumstances – the legal challenges are far easier to overcome.
- In the example, the insurer is likely to have specified its contractual terms as part of defining the insurance product, or common product terms may be defined by the platform itself. To avoid any question that the customer has understood and accepted the contract on certain legal terms, the contract should be presented to the customer in natural language. It is most likely that this would be presented to the customer in the form of a separate document in very much the same way as such would be provided on an aggregator platform.

- In addition to considering standard common law principles governing the creation of a binding contract, industry-specific regulations need to be considered. Insurers will be aware of the requirements from their financial regulator to ensure that the appropriate information is provided to customers such as details of cover, evidence of cover, cancellation rights, Key Facts documents and statements of Demands and Needs, to name a few. Insurers will need to ensure that customers receive the information required by the Solvency II regime, relevant "Distance Marketing Information" under the FCA ICOBS Sourcebook and, from 23 February 2018, make the necessary disclosures under the Insurance Distribution Directive.

Step 6

Several months later, the customer's house is flooded. She returns to the platform to see the photos captured and water detection data recorded in the blockchain by the IoT device.

More detail:

- The data and images are stored on the blockchain directly by the device, signed by the devices' own hardware-secured private key. This time-stamped data, coupled with GPS location (including height), provides immutable proof of the water detection event occurring at a certain time and date.
- The report is only accessible by the specific insurer that requires proof for the claim – no other insurer, customer or even the platform owner can access it.

The traditional, non-blockchain model for claims is very slow, painful and resource intensive, normally requiring several phone calls with a customer support centre.

Step 7

Automated image analysis, automated analysis of the flood level detector devices, GPS location and public flood information confirming a flood occurred in the area and the policy parameters are then processed by the smart contract (and associated automated analysis components) to make an automated decision for an agreed payment to the customer.

More detail:

- The payment may be initiated automatically, without any human interaction, where the platform integrates directly with necessary third party data sources to verify the existence and severity of the flood to be valid and checks this against details of the legally binding smart contract.
- The traditional claims model is resource-intensive and takes several weeks of back and forth for the due diligence of the claim to be finalised before a payment is made to the claimant – this is not a good customer experience. In addition, the customer needs to trust that the insurer will make the payout when the event occurs.

Legal analysis of steps 6 and 7

The automatic payment initiation is an example of a self-executing smart contract. There is no legal barrier to such automatic execution provided that all contracting parties have agreed to the triggers and to be bound by them. This proviso highlights the need to have clear contract terms communicated via natural language. In reality, it may not be in one or more of the parties' interests to have completely automatic self-execution. The insurer, for example, may want to carry out a claims assessment before initiating payment.

- A key point to note here is that there is no use of cryptocurrency at any point during this process. All payments are made using traditional means such as Direct Debit or Faster Payments. This is important from a regulatory standpoint, as blockchain is therefore being used as a distributed database that improves workflow efficiency, not a new payment methodology.
- What happens if there is a dispute between the insurer and the customer? If the smart contract has not been communicated in clear language, a dispute may well arise as to the nature of the contractual terms themselves. In these circumstances, to make matters more complicated, the forum and process for resolving disputes will not be clear – leading to complications around jurisdiction and enforceability. To avoid these difficult questions, a clear dispute resolution procedure can be included in the natural language contract communicated and agreed between all relevant parties. In the context of insurance to UK consumers, it is likely that complaints regarding such insurance contracts will fall within the jurisdiction of the Financial Ombudsman Service. Insurers must inform customers of their right to refer complaints to the Financial Ombudsman Service and the parties cannot agree to 'contract out' of this complaints service. Accordingly, the smart contract must make provision for this.

Final thoughts

There are a number of features of the blockchain platform which align with general shifts in the consumer insurance sector. First, the consumer has more control over the scope of the insurance to be provided aligning with the shift in power from insurers to the consumer. Second, the insurer can also use the information provided to apply more sophisticated information analytics, resulting in more accurate risk profiling and accordingly more individual specific products and premiums. Consumers may also have the option to integrate third party data sources and devices into their profile to further enhance the information being provided and increase the level of automation in triggering a payment, thereby removing the need to trust the insurer to make the payout.

Blockchain-based insurance contracts could provide many practical benefits to the customer experience and whilst this is good for an insurer's own goodwill with its client base, it also has a reciprocal benefit of assisting insurers in meeting the FCA's objectives of requiring good customer outcomes and treating customers fairly. The FCA has recognised that blockchain and distributed ledger technology has the potential to offer genuinely innovative solutions to financial services.

There is no legal framework specially designed for blockchain, distributed ledgers and smart contracts. To date, legal analysis and commentary on these issues focusses on the theoretical risks and challenges of unregulated, permissionless ledgers and smart legal contracts in their purest form (ie. the smart contract being exclusively contained in code). The underlying blockchain and smart contract technology can, however, be adapted or designed so that the solution fits within the existing legal framework. So, for example:

The way forward:

- questions concerning the legality and enforceability of smart contracts can be answered by using smart contract code that executes the promises made in an otherwise 'typical' legal agreement expressed in written language – which is communicated to the relevant party. This is, effectively, no different to other online platforms that can execute agreed actions based on inputs;
- while permissionless distributed ledgers can raise risks and issues around regulation (who or what to regulate), jurisdiction, data protection (for example, who is the data controller if there is no central authority), these risks can be avoided or mitigated through the use of a permissioned system which is controlled with access controls (giving the ability to control entrants, jurisdiction and the legal basis of participation); and
- while, on the face of it, an immutable ledger that can be seen by any participant raises questions about data security, data protection and confidentiality, in reality, the distributed ledger can be configured with encryption and access controls which can make the ledger more secure and more compliant than traditional databases.

[2] Speech by Christopher Woolard, Director of Strategy and Competition at the FCA, delivered at the BBA FinTech Banking Conference, 22 September 2016 – https://www.fca.org.uk/news/speeches/our-role-promoting-innovation.

10185