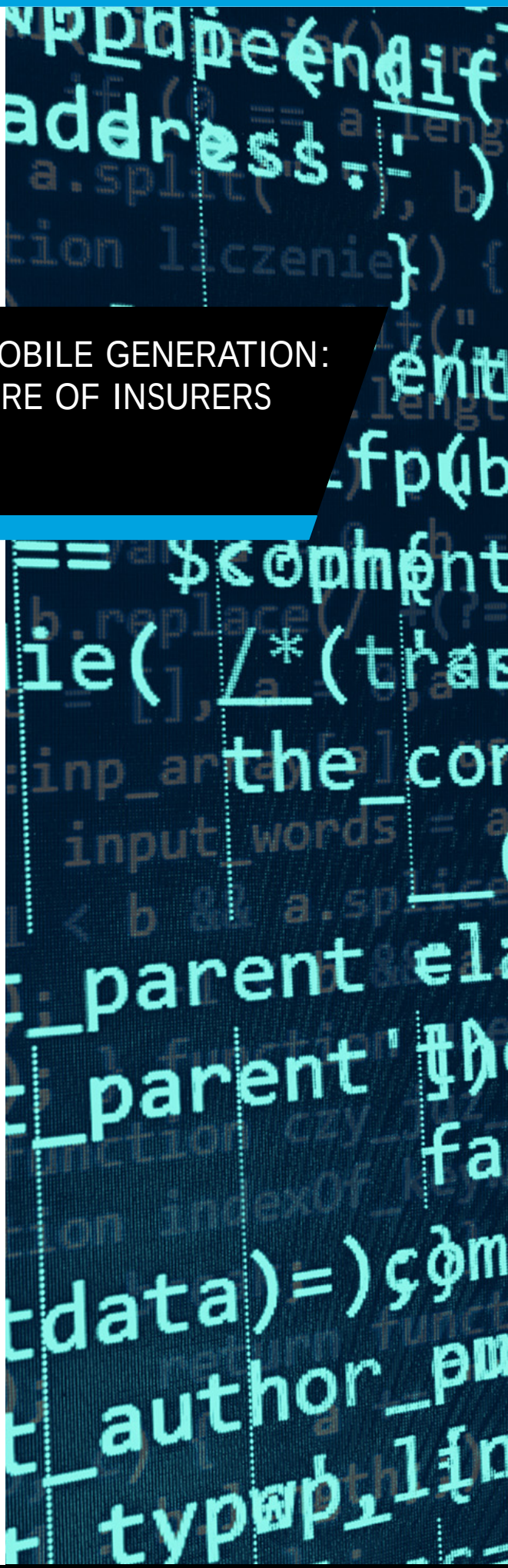
REINVENTING INSURANCE FOR THE MOBILE GENERATION: WILL BLOCKCHAIN SECURE THE FUTURE OF INSURERS OVER THE TECH GIANTS?

February 2018



Insurance is an old industry. Entrepreneurs are looking at how the latest technologies can create new business models to increase efficiency, reduce administration and make insurance products attractive to today's digital natives.

Blockchain technology offers the potential to break down many of the structural issues that have created frictions and a lack of trust in insurance markets.

In recent years, with a flood of investment in financial services and a leap in the ability of computing to process data and machine-read text, insurers have been widely reported to be in fear of their own "Uber moment" - with over 75% in the industry believing that a new market entrant disruptor will come in the next five years. With the global success of services such as Airbnb, as well as Uber themselves, it is possible to imagine a similar impact on the business of insurance.

In particular, social networks like Facebook or online providers such as Google have huge potential to leverage their warehouses of personal data to compete with incumbents. Given the extent to which Google track the online movement and behaviours of their users, what better way of pricing risk and evaluating trust than via this formidable data set?

Kennedys

Nevertheless, the traditional $4.5-trillion-dollar insurance industry has not been resting on its laurels. Insurance companies have been working to embrace startup culture and invest in new technologies including Blockchain - establishing substantial incubation and accelerator funds. These include Aviva's £100 million venture capital fund – 'Aviva Ventures', AXA's €100 million incubator – 'Kamet' and Allianz's €430 million fund and incubator – 'Allianz X'.

A number of new products have begun to emerge. Take US start-up Lemonade – a technology first and legacy-free insurance offering. Launched in September 2016 and powered by artificial intelligence (AI) and behavioral economics, Lemonade's peer to peer (P2P) offering is based on small groups of policyholders that pay premiums into a claims pool. If there is money left in the pool at the end of the policy period, members get a refund.

One year on and Lemonade has announced a new product, 'Zero Everything', offering members a 'zero deductible' upgrade for two claims each year. Trov (in partnership with AXA Insurance) is another example of reinventing insurance for the mobile generation – offering an on demand insurance platform for electrical items.

> "Lemonade co-founder Shai Wininger has summarised his offering as "*challenging the way insurance companies work, with a peer-to-peer business model fuelled by self-servicing technology. We've seen this kind of combination breathe new life into other industries, and we're determined to do the same for insurance*". "

THE RISING 'THREAT' OF PRIVACY REGULATION

Most initiatives seek to exploit the potential of data science and technology in a manner well practiced by the likes of Facebook and Google. This presents an interesting dynamic considering the current spotlight on data privacy and its regulation.

In Europe, this attention has shaped a new data protection framework in the form of the General Data Protection Regulation (GDPR), which will be directly applicable in all Member States and will take effect on 25 May 2018. The GDPR will impact almost every organisation that is based in the EU, as well as every organisation that does business in the EU – even if based abroad. The law applies to personal data that are processed in the context of automated systems, or relevant filing systems. While many of the underlying principles of the GDPR are already recognised, the GDPR places significant emphasis on increasing harmonisation across the EU in order to facilitate the free flow of personal data.

In practice, achieving greater legal certainty will mean increased compliance requirements for business. This includes a series of new rights afforded to data subjects – which may limit the ability of organisations to lawfully process data of data subjects.

Conversely, the United States is notable for not having adopted a comprehensive information privacy laws. However, calls for tighter regulation have reached fever pitch recently following a series of adverse incidents.

Arguably the US story began in 2013 when Edward Snowden leaked classified information from the National Security Agency before fleeing from America, seeking asylum in Russia. Snowden's disclosures exposed a number of US government-led surveillance techniques and brought data privacy in the US under the spotlight. Subsequently in October 2015 – and as a direct result of Snowden's revelations - the European Court of Justice declared the EU-US "safe harbour" scheme regulating firms' retention of Europeans' data in the US to be invalid. In one forceful swipe, all companies relying on safe harbour were forced to find an alternative mechanism for their data transfers to the US.

More recently, the Brexit and Trump campaigns saw concern arise around application of data analytics to swing voters via social media platforms (including Facebook, Google and Twitter). That has included the suggestion that Trump's campaign colluded with Russian hackers. In particular, focus has turned to marketing company Cambridge Analytica, which "uses data to change audience behaviour" in both commercial and political spheres.

> “By using cutting-edge technology to build psychometric profiles of voters to find and target their emotional triggers the suggestion is that it has been possible to influence electoral outcomes.”

Such power is likely to lead to close scrutiny over the behaviour of the tech giants in recent political campaigns. Meanwhile, the idea that a Facebook or a Google could take the leveraging of personal data to new heights and launch their own insurance company has been brought into sharp focus. Amazon have in recent weeks launched their first foray into the insurance world. However, their data warehouses are built purely upon purchasing preferences, less so on personal behaviours. Indeed, the business models on which Facebook and Google are built may find themselves under direct threat and facing their own “Uber moment”.

BLOCKCHAIN TECHNOLOGY

Investors have been quick to see the potential benefits. Total venture capital investment in Bitcoin and blockchain start-ups exceeded $1.1 billion in early 2016. The Blockchain offers the potential to conduct online transactions without the need to give up control over our personal data. Take a current social network like Facebook by way of example. Whilst it offers the benefit of sharing photos and memories with loved ones across the globe, the cost is control over personal data. Blockchain, however, is a ‘cake and eat’ it technology – users can continue to share media whilst retaining control over their personal data.

So what is blockchain, what does it do and how does it work?

Blockchain is append-only distributed ledger technology, which allows information to be collected and stored immutably in a decentralised manner on a network of computers worldwide. The changing state of the network is supported by a common agreement based on game theory and cryptography (pure mathematics) to ensure the validity of all entries

The first real application of the blockchain technology is Bitcoin - the global cryptocurrency where blockchain solves the double spend problem.

In traditional currency a bank is required to ensure money cannot be spent more than once. With Bitcoin, blockchain does away with the need for any central coordination at all.

The blockchain is the technological base for other virtual currencies including Ethereum and Litecoin.

The basic principles of blockchain technology include:

- **Redundancy**: A copy of the blockchain is stored on each computer (node) within the network and as a result there is no single point of failure. Communication occurs directly between peers instead of through a central node. Each node stores and propagates information to all other nodes in the network.
- **Peer to peer transaction**: each record (known as a block) is timestamped and linked to the previous block. Communication occurs directly between peers instead of through a central node. Each node stores and progresses information to all other nodes in the network.
- **Consensus**: each party on a blockchain has access to the entire database and its history. No single party can execute a transaction without agreement by all relevant parties that the transaction is valid. Each party can verify the records of its transaction partners, without an intermediary; helping to keep inaccurate or potentially fraudulent transactions out of the database.
- **Immutable**: once a transaction is entered in the database and the accounts are updated, the records cannot be altered retrospectively. Changing any one block breaks the entire chain, making it almost impossible for hackers to subsequently change blocks.

So how could Blockchain solve privacy issues?

With blockchain technology, individuals can choose who they share data with. Personal data itself often does not need to be stored on the blockchain – rather only its verification through an expert (e.g. a doctor). Moreover, ‘hashed’ copies (the process of applying a hash function to some data) of the file can also be stored to ensure verification can be achieved.

Currently, Facebook and Google rely on the acceptance of their users to relinquish their personal data in order to exploit its value. We may soon arrive at a place where new providers offer all the benefit of existing tech giants but without the data privacy downsides.

For insurance, this may mean that the threat of a tech giant exploding into the insurance world recedes and as it does, traditional insurances companies will be well placed to exploit the potential of blockchain technology themselves. But what shape and form might this take?

A QUESTION OF TRUST

One key issue blockchain can address with insurance contracts is the underlying principle of utmost good faith (*uberrimae fidei*). The principle means that every person who enters into a contract of insurance has a legal obligation to act with a standard of honesty greater than that usually required in most commercial contracts. It also means the insurer is required to trust they are being told the truth during disclosure by the policyholder. By contrast most other contracts are based on the principle of 'let the buyer beware' (*caveat emptor*), which means the buyer assumes the risk that a product may fail to meet expectations or have defects.

Applying blockchain technology to contracts of insurance and personal data can be stored once to the blockchain with consumers able to control who has access. The data itself remains stored on the user's personal device. Even then that data is often just verification data from a third party.

Arguably, insurances services and processes have evolved to respond to a perceived lack of trust and transparency. The Insurance Act 2015 intends, of course, to address this in principle and create a more even playing field to the laws governing disclosure in non-consumer contracts (amongst other measures).

As a consequence of that somewhat pessimistic picture, brokers emerged as important and necessary mediators - creating trust and bridging the gaps between insurers, reinsurers and customers.

However, if blockchain solves the problem of trust, the future role of the broker (or any other form of intermediary) may be brought into question (and in particular with the consumer insurance level).

> "Indeed, might we get to a point that removes the need for others involved in the service of insurance contracts – including lawyers, loss adjusters or claims handlers? In theory, all of these functions can, in principle at least, be managed by blockchain."

BLOCKCHAIN INSURANCE INDUSTRY INITIATIVE, B3I

The launch of B3i in 2016 shared with the world a singular vision: To build an efficient world-wide industry platform for market participants to more easily cede, handle and trade risks.

There is no broker representation in the emerging B3i consortium and AIG's blockchain-based policy for Standard Chartered was arranged without involving the bank's broker. While operations like Lemonade continue to depend on mainstream insurers to underwrite their products, P2P models imagine a world where risk sharing groups can come together and operate on the blockchain without even the need for insurers.

A SMART FUTURE

What if an insurance policy could be written as a code, offer full transparency and be executed in decentralised way without any human intermediary?

An additional feature of blockchain is the ability to execute Smart contracts – the next potential big win for insurance firms. The Smart contract is a computer program which is stored in a blockchain platform. It automates the obligations of the parties under an agreed contract – if a set of required conditions are met, then payments are made or property transferred, and the required transactions recorded on the blockchain.

In order to work effectively in an insurance context, the Smart contract depends on a reliable data feed which can be utilised to determine if a payment should be made and if so, how much. In other words, the claim is automatically calculated and paid out.

> “For example, aviation lost baggage claims could be based entirely on reliable data on flight information and the baggage tracing system.”

Indeed, AXA has launched a product called ‘Fizzy’ that does exactly that - insuring customers against flights that are delayed by two hours or more. Products like this make the claim process entirely transparent and substantially improve the perceived fairness of the product.

Looking ahead, marine insurers are set to begin using blockchain in contracts in 2018. AP Moller-Maersk, the Danish conglomerate that includes the world’s largest container shipping business, and the insurers MS Amlin and XL Catlin are among the companies involved in a new blockchain platform that will go live in 2018.

Other potential Smart contract examples include:

- Payouts to insured farmers when drought conditions are reported by verified climate/weather databases.
- Cars, electronic devices or home appliances having their own insurance policies that detect damage; triggering repair and payment.

AN ANSWER TO FRAUD?

The final big win for blockchain centres on fraud. In the UK, the ABI estimates that insurance fraud costs approximately £2.1 billion per annum. The figure for France is £3.9 billion per annum and in the USA, fraud is said to cost the industry over $80 billion a year across all insurance lines (5-10% of claims costs for US and Canadian insurers).

Most fraud exploits the lack of trust and transparency in the insurance process, exploiting the gaps between insurer databases. Blockchain offers the potential to record all policies and all claims, along with the ownership and authenticity of goods to be validated. Further, because Blockchain is a ‘cake and eat it’ technology, no one insurer is required to share their book of claims with any other insurer.

CHALLENGES AND RISKS

Like all new technologies, there are issues and risks. Bugs in the code that supports blockchain and Smart contracts can be extremely costly. In June 2016, one third of a venture-capital fund was lost to unscrupulous users who exploited a vulnerability. During a pilot of blockchain enabled ‘Flight Delay’ insurance, decentralised insurance platform startup Etherisc allowed customers to buy insurance for past flights - thus guaranteeing a payout.

Other issues include:

- **Standardisation**: to realise sustainable benefits from a shared and distributed system, standards are absolutely critical. With Blockchain in its infancy, technical standards themselves are also in their infancy and will need to be developed to support future applications.
- **Processing power**: as characterised by diverse IoT ecosystems, which could mean different computer capabilities that interfere with speed and efficiency.
- **Scalability issues**: as presented by the consensus-based validation mechanisms and the continuous replications that underpin blockchain.
- **Storage**: even if there are newer implementations of blockchain that have fewer performance restrictions, high-speed/high-volume transactions, real-time data capture and storage of large volumes data are not the intended domains of blockchain. The ledger has to be stored on the nodes themselves and the ledger will increase in size significantly with time. That may well be beyond the capabilities of smart devices that have low storage capacity.
- **Security**: new technology means new potential security loop holes and by enabling multiple organization to put their trust in a single ledger albeit distributed there is a still arguable an industry wide single point of failure.

CONCLUSION

It should be remembered that blockchain is a network technology. Like all network technologies - the value of the network is determined by the number of people who use it. It is possible that existing database technology may be deemed

satisfactory. Indeed, in the UK, fraud databases have been operating for some time - despite the benefits of blockchain. Therefore, it will take a concerted effort and substantial coordination between competing databases and insurers for existing practices to be displaced.

> “The increased focus on privacy laws could prove to be a real opportunity for insurers to consolidate their markets at precisely the time that the tech giants are under threat of their own “Uber moment”.”

Blockchain could become the system of choice as insurers (and others in financial services), seek greater trust, security – as well as efficiency – in multiple transactions taking place simultaneously around the world. Realising that potential will, however, require a bringing together of those with complementary capability and a shared vision.

Overall, we are likely to see the myriad of business opportunities increase and the evolution unfold at a quickened pace. Blockchain is no longer about experimentation.

> “By laying down the foundations today to explore the challenges that blockchain presents, the future of insurers will be secured.”

Indeed, we expect the majority of insurance firms to implement blockchain into their business models by 2020.

FURTHER INFORMATION

To find out more about our services and expertise, and key contacts, go to: **kennedyslaw.com**

KEY CONTACTS

Karim Derrick
Head of Research and Development
t +44 20 7667 9776
karim.derrick@kennedyslaw.com

Martin Stockdale
Partner
t +44 161 829 7456
martin.stockdale@kennedyslaw.com

Richard West
Partner
t +44 1245 299 877
richard.west@kennedyslaw.com

Deborah Newberry
Head of Corporate and Public Affairs
t +44 20 7667 9508
deborah.newberry@kennedyslaw.com