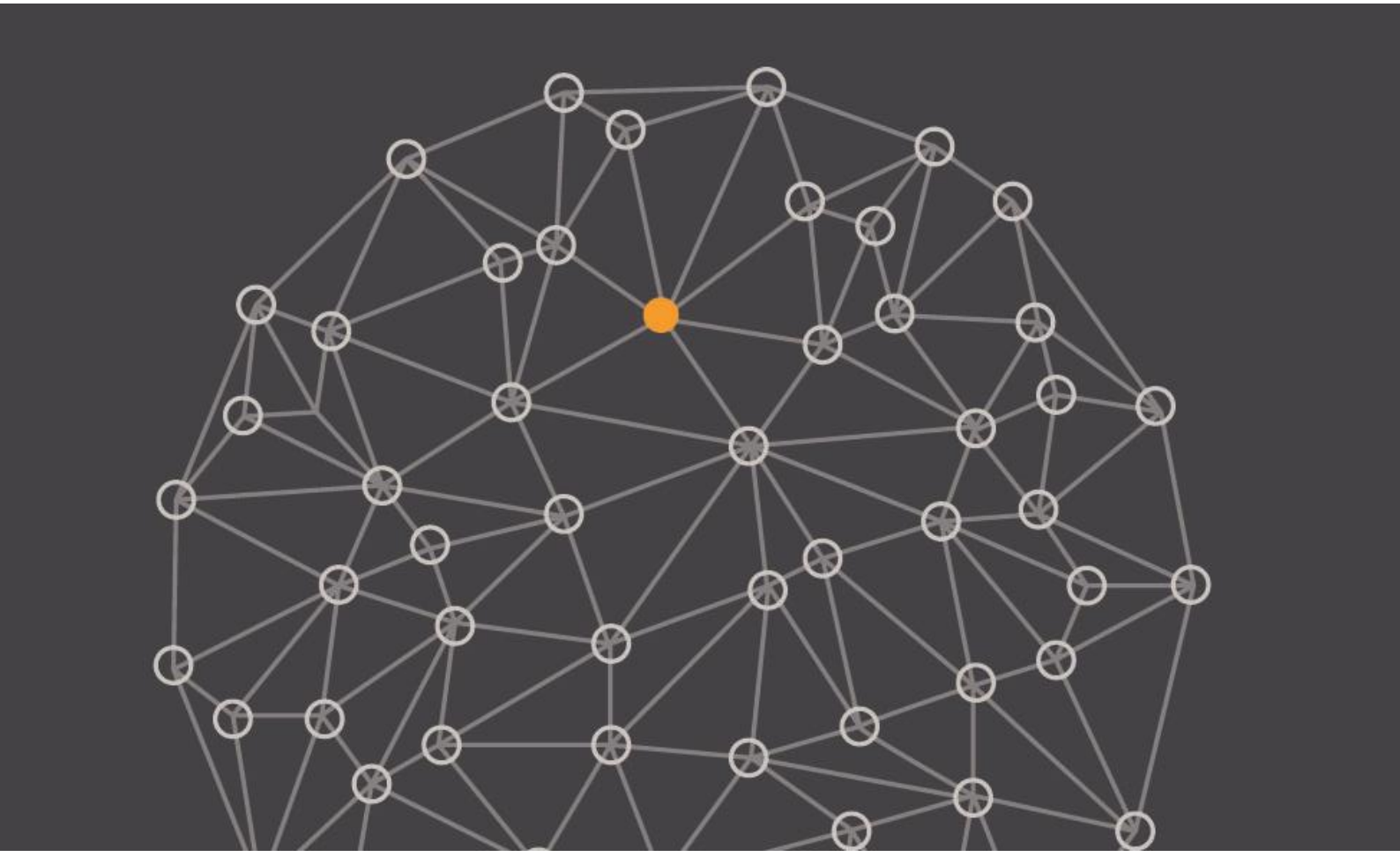
MILLIMAN RESEARCH REPORT

Blockchain and insurance

April 2019

José Silveiro, IA
Rubén Nova, IA



Milliman

Introduction

Blockchain is one of the emerging technologies frequently mentioned as advancements people in every industry ought to familiarise themselves with, and yet, the perception still exists that blockchain is more about theory than reality. On the other hand, there are already numerous initiatives underway in a variety of sectors to explore the possibilities that blockchain offers, and some of those possibilities are already being taken advantage of. Insurance is one of those sectors.

Blockchain is the technology upon which a validated and shared record of transactions and/or events is based and which, together with existing widely accepted technologies for data capture and analysis, offers itself as a decisive platform for generating value in the insurance sector.

In this report, we seek to explain blockchain technology, together with some of its current uses. We also present an example of an insurance product that could benefit from this technology, with the aim of providing some context for the aspects to consider when launching a prototype.

We begin by providing a brief introduction into blockchain, its uses and its properties.

What is blockchain?

Formally, 'blockchain' can be defined as a network that manages a data registry in a decentralised way, which requires stored data to be cryptographically protected, and is open to a predefined public. The blockchain enables parties who do not fully trust each other to maintain a single 'truth by consensus' without the need for a central (or intermediary) entity.

Any authorised person (i.e., member of the 'predefined public') may record a transaction in the network. Once verified, a new 'block' is formed, which is linked to previous 'blocks' in the 'chain', giving rise to the term 'blockchain'. The blockchain allows for the creation of a shared chronological record which may be consulted by any participant of the network, but never modified or erased (this is referred to as the property of immutability). This is a key benefit for processes that rely on traceability or auditability.

Blockchain was first used when Satoshi Nakamoto launched the bitcoin cryptocurrency in January 2009. Since then, the terms bitcoin and blockchain have often been confused. Bitcoin is a network that enables a system of digital payments without the intervention of a banking institution and which uses blockchain technology to make that possible. Blockchain may be used without need for the existence of cryptocurrencies.

As participants within a blockchain network, people and organisations are able to control a shared network of historical transactions and benefit from the aggregated information that it can offer about them or about the products that are of interest to involved parties.

USES AND CONSORTIUMS

One of the most well-known cases is the use of blockchain by Walmart to provide assurances to consumers and the health authorities about the traceability of its grocery products. By reviewing the shared record that is logged through each stage of the food distribution process, from harvest to sale, customers are able to trace the life of the product that they are buying, to ensure its provenance, to verify whether the cold chain has been respected and to know the time that has elapsed since it was harvested.

The company implemented a pilot during 2019 whose application would have lessened the financial implications of an incident that took place in 2018 involving an outbreak of the E. coli bacteria. The bacteria was associated with a batch of romaine lettuce, grown in the region of Yuma, and it caused 210 infections, 96 hospitalisations and five deaths in the state of Arizona (USA). Because the health authorities were unable to specify the source of the contaminated batch of lettuce, millions of bags of the product had to be removed from markets, regardless of their origins. Blockchain would have allowed for the identification and withdrawal of specific products within a matter of hours, not days. Following the successful trial by Walmart, 10 of the largest food companies in the world have joined the so-called Food Trust network, including Unilever and Nestlé.

In May 2018, a consortium in the automobile industry, the Mobility Open Blockchain Initiative (MOBI), founded by well-known automobile manufacturers such as Ford, BMW, Renault and General Motors, announced the launch of several blockchain uses. MOBI's first development involves equipping a vehicle with a digital identity so that it can be located at any time, which prevents manipulations of the odometer. Clearly, this use has benefits for various participants of the automobile industry.

- **Customers**: Potential reductions in fraudulent sales of secondhand vehicles, improved vehicle maintenance.
- **Manufacturers and garages**: More accurate vehicle history for their repairs and guarantees.
- **Insurance companies**: More accurate and reliable data for the calculation of their premiums.

The global interest in blockchain has led to the creation of consortiums in which participating companies are backing research, development and investment in the technology, to the benefit of all consortium members. Below, we cite three of the most well-known:

- The **Blockchain Insurance Industry Initiative (B3i)** was created in 2016, and involves the collaboration of global insurance companies, with the aim of increasing the efficiency of the exchange of data between insurers and reinsurers through the use of a blockchain. The founding members were Aegon, Allianz, Munich Re, Swiss Re and Zurich. In 2017, B3i launched a prototype of a smart system for the management of catastrophic reinsurance contracts.
- **Hyperledger** was launched in 2016 as a global collaboration organised by the Linux Foundation, including leading companies in the finance, banking, healthcare, supply chain, manufacturing and technology sectors. Nowadays, Hyperledger comprises more than 200 companies from all over the world, including IBM, R3, the University of Cambridge, the Bank of England and the financial group BBVA.
- **Enterprise Ethereum Alliance** is a nonprofit organisation that brings companies together to investigate and implement solutions based on smart contracts through Ethereum's public blockchain, founded in March 2017. Its members include companies in the Fortune 500, startups, academics and insurers. Some of its members are J.P. Morgan, Banco Santander and Thomson Reuters.

PROPERTIES

Blockchains have each of the following key properties, which distinguish this emerging technology from other networks and ledger technologies:

- **Distributed:** The blockchain-supported ledger is managed by a limited group of users using consensus algorithms. Each operation recorded in the network is replicated by all of the participants in the chain, ensuring the security and robustness of the network against malicious attacks. Blockchains can also be combined with each other, thereby strengthening their distributed nature.
- **Permissioned**: When a blockchain is created, a protocol is defined in which the rules that govern the platform are established, including the definition of a common standard to delimit communication between the participants of the network.
- **Public or private:** A public blockchain is defined by a protocol that is open to any users who want to access, consult and validate the transactions. A private (or 'permissioned') blockchain requires a higher degree of familiarity between the parties, given that only authorised participants may access the recorded data. Depending on the terms of their protocol, they may be allowed to record transactions in the chain and/or verify changes that happen in the network. Hybrid blockchains also exist, known as semi-permissioned blockchains, which are a combination of the public and permissioned blockchains.
- **Universal**: The network allows operations to be undertaken between participants regardless of where they are located, due to the elimination of intermediaries and central entities, and thanks to the decentralisation of processes. The technology facilitates business-to-business (B2B) and peer-to-peer (P2P) operations, making it possible for the nonbanking population (38% of the world's population, according to data from the International Monetary Fund) to access the system. Moreover, it allows for the elimination of some friction associated with cross-border payments, reducing the inefficiencies, costs and risks of intermediaries. When undertaking an operation within a blockchain platform, the marginal costs and time associated with that operation are reduced.

- **Granting authority to the customer (self-sovereign identity):** The network provides each user with a protected digital identity using cryptographic systems that allow the user to dispense with the use of other forms of identification such as passports and driver's licences. Information about each user is distributed in different nodes of the network and third parties may be authorised to use specific data for specific transactions. This is known as a self-sovereign identity. It means that users control and administer distinct identities as well as control who has access to certain personal information. For example, if a person wants to access an event which requires a minimum age of 18 years old, rather than showing an identity card, which includes other information besides date of birth, such as street address, the digital identity can provide a verified date of birth without the need to reveal any other personal data.

Self-sovereign identity can concentrate a series of digital attributes, such as age, credit or accident history, licences and academic qualifications, into a single repository, allowing for the creation of a digital fingerprint that, together with a private key, allows users to ensure the authorised transfer and use of their data, documents and other files.

Smart contracts

One of the key developments built on top of blockchains are smart contracts, which involve the execution of one or more of the provisions of a contract in an automated way, on the basis of a validated transaction or event.

It is important to specify that, although insurance contracts (and any other stored information) remain as digital documents within a blockchain, the conditions that are stipulated in those contracts and which may give rise to processes outside of the blockchain (such as the management of claims, the renewal of policies and the applications of discounts on premiums) are programmable codes within the network itself. Therefore, we can define smart contracts as programmable code that, with blockchain, allows conditions to be established so that certain processes are executed automatically.

It is worth bearing in mind that, in many cases, blockchains do not have (or record) the necessary data for smart contracts to be executed. In these cases, an external verification source (referred to as an 'oracle') is needed to provide the trigger. For example, for flight insurance built on a blockchain, in the event of a delay or cancellation of a covered flight, then the state air agency would serve as the oracle, verify any delay or cancellation and trigger the payment of the amount stipulated in the insurance contract. In this way, neither the insurer nor the customer would need to verify that the incident occurred.

The advantages of smart contracts are magnified when they are combined with other technologies, such as the Internet of things (IoT). Imagine a leasing contract in which the smart contract detects an unpaid installment—a message could be sent to the screen of the car and/or other actions could be activated without the need for any human intervention.

Insurance products

In this section, we present an example of blockchain use in a theoretical insurance product. We assume that, as part of its digital transformation process, an insurance company is looking to explore the capabilities of blockchain based on a pilot project, and is assessing the contribution of the technology towards:

- **Optimising the premiums offered to customers**, incorporating the best information for the valuation of the expected cost of the insured risks.
- **Promoting a more personalised relationship with the insured party**, assessing the potential of the technology to improve knowledge about the customer and to share that knowledge with other suppliers (health and well-being services, sports or other service suppliers, technology providers).
- **Cost reductions** through improvements in the efficiency of certain processes and in the identification (or prevention) of fraud.

The company recognises that the adoption of blockchain does not represent a benefit or solution per se, and currently the sector is addressing the aforementioned aspects with other successful approaches. Further, the company recognises that blockchain technology does have associated infrastructure costs. The result of the pilot should provide insight into the advantages of starting a project early based on this technology as well as the current limitations of it and other possible risks.

The insurance product that is proposed consists of taking advantage of blockchain technology, combined with the IoT, by offering customers an insurance product for running and walking. The company intends to offer new coverage and services that allow customers to enjoy those activities in a safer way, introduced through a more personalised and efficient process thanks to the automation enabled by the blockchain.

COVERAGE OFFERED

The prototype offers a new coverage to complement the insurer's existing life, health and accident policies. It is an optional coverage, offered free of charge to insured parties who currently are covered by life assurance and either health or accident policies with the company.

The new coverage is for costs associated with injuries caused by the physical activities of running and walking. Therefore, it is aimed at a wide range of policyholders, aged between 18 and 75 years old, and offers:

- Support services for transporting the insured party to a health centre in the event of an emergency
- Climatological alert services for the planned journey and geolocation
- An automated call service to a contact person identified by the insured, indicating the place of injury and the health centre to which the insured person has been transferred
- A discount of 20% for approved physiotherapy services for the first five sessions, which would be added as an additional benefit for those insured parties who have contracted health insurance

The coverage would be subject to the same exclusions and underwriting rules as those relating to the life, health and accident policies. The assistance and automatic call coverage would be 100% reinsured. An annual use limit is established for the coverage, which may not exceed two uses in two consecutive years. The coverage is annual with the option for renewal upon expiry by both parties.

PRICING

As stated above, the coverage is offered free of charge to those insured persons who have contracted two or more of the aforementioned coverages with the company.

In addition, and by way of a payment to the insured party for the additional information that the company obtains about how that person's habits influence the use of the policies, each session of physical activity will be rewarded with 'tokens', which can be accumulated and are exchangeable for discounts in the network of service suppliers participating in the program.

In this way, a new open system is developed between the customers of the insurance company, the insurer itself and the other service suppliers, based on the tokens system, defined in the smart contracts and recorded in the blockchain.

Over the medium term, once the insurance company has been able to understand the impact of the healthy habits, more sophisticated pricing systems could be considered for life, health and accident insurance. Beyond an improvement in the segmentation of customers, it will also be necessary to understand the implications of working in collaborative ecosystems, to determine whether there is a real cost saving and/or improvement in the prevention of accidents, as well as any possible risks relating to the product not previously considered.

ACTIVATION OF THE COVERAGE

The initial activation of the coverage would be promoted through the insurance company's different channels and, in particular, would be considered as a loyalty tool for the agency channel. The activation would begin with the download of an app on the customer's smartphone and the subsequent configuration of a digital identity.

The table in Figure 1 shows the information that would be requested from the insured party. In addition to information collected during initial activation, during any 'logged' physical activity, information relating to the location and physical condition of the insured party would be recorded. Finally (and based on the preferences of the insured party) the information may be shared with third-party service providers for the purpose of benefiting from a discount scheme.

FIGURE1: INFORMATION ABOUT THE INSURED PARTY

INITIALLY	DURING THE ACTIVITY	RECORDED BY THIRD PARTIES
AGE	HEART RATE	MEDICAL EXAMINATIONS
HEIGHT	HEART RHYTHM	ENDURANCE TESTS
WEIGHT	LOCATION	PHYSIOTHERAPY TREATMENTS
IF HE / SHE PLAYS OTHER SPORTS	DATE AND TIME	MONITORING OF WEIGHT AND DIET BY NUTRITIONISTS

DEVICES NEEDED

The contextual activation of the coverage would be performed by the insured party at the beginning of the physical activity, for which an electronic device must be worn and the app open to access the account using biometric recognition technology or a personal code.

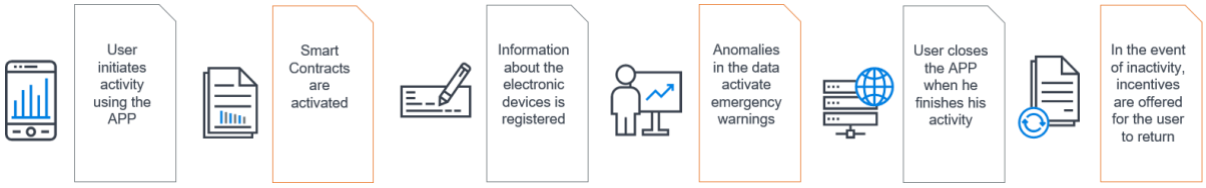
To record information during the activity, the agent would offer the insured party a 'smart bracelet', which would be connected to the internet and linked to the app on his smartphone (e.g., via near-field communication [NFC] or Bluetooth) for the use of GPS and other applications.

USE OF BLOCKCHAIN

The bracelet may incorporate the following sensors: an accelerometer, a heart rate monitor, a thermometer, a gyroscope, a geolocator and an altimeter, and therefore would allow the heart rate and duration of the session to be recorded along with the location and time of the activity. This device, together with the insured party's smartphone and the smart contracts defined by the blockchain, would enable the automation of the following processes:

- **Contractual**: Together with the notification of an injury suffered by the insured party, the smart contract would verify the conditions agreed in the insurance contract and automatically initiate the provision of the service. These notifications may be transmitted easily through the app or may be identified automatically thanks to the sensors on the bracelet.
- **Management of the service:** In the event that anomalies are detected in the data that is being recorded, several smart contracts would be activated to ensure the safety of the customer. The first would be an automated message to the insured party to check that person's status by means of a vibration lasting several seconds. In the event that said alert is not deactivated, another smart contract would generate a telephone call to the user to assess the situation. Finally, emergency services would be alerted and provided with the location of the insured party for appropriate treatment as quickly as possible.
- **Anti-fraud**: In the case of anomalies that could reflect fraudulent use of the service, additional security measures would be requested. For example, if the physical activity is performed by a person other than the insured party, given that the history of the activity is traceable, any cardiac behaviour or walking or running speed outside of the range observed for the individual could be detected, and so an additional biometric test would be requested, such as a photograph.
- **Customised service offering:** Based on certain agreed service rules, contracts may be activated to offer contextual services (nutritionist, personal training, medical tests for athletes, etc.). The contracts would remain suspended in the network and, in the event that prolonged inactivity of the user were detected, then incentives could be activated to encourage a return to activity, or the option could be given to connect the insured party with other users to join physical activity classes.

FIGURE 2: MONITORING USER HEALTH WITH BLOCKCHAIN



PILOT PLATFORM

The insurance company has realistically considered the technological developments that it can lead internally and those for which it has to rely on third parties to provide access to up-to-date and high-level solutions. In addition, it must offer guarantees regarding strict compliance with the data protection laws.

Therefore, it has been decided that the blockchain and IoT infrastructure should take advantage of the resources provided by a known consortium, agreeing to the following conditions:

- During the first two years, the information would be shared only between the insurance company, the reinsurer and the service providers authorised by the customer. From year 3 onwards, the customer would have the option of benefitting from any service offered in the blockchain network, including offers from other insurers, which would then have access to the history of the physical activity and services of the insured party.
- The intellectual capital developed belongs to the consortium and would be shared with all of those insurers with an interest within the consortium.
- The insurer is not obligated to share the knowledge acquired about customers or its methodologies for analysing the information.

MEASUREMENT OF SUCCESS

To measure the success of the project, the insurance company has defined combined metrics over a time horizon of between 12 and 18 months, taking into consideration:

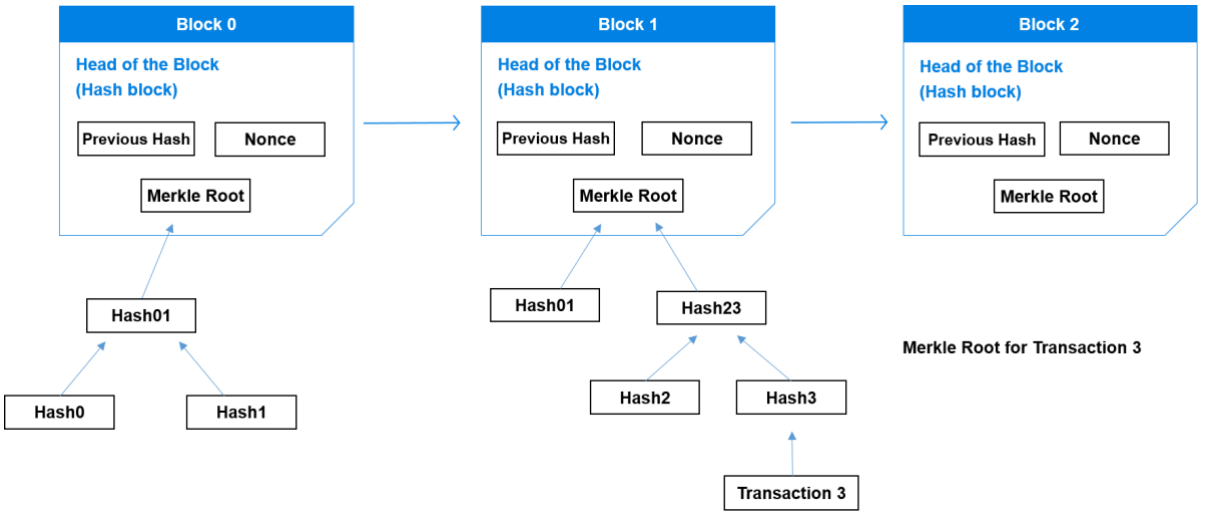
- **The new users and effective use of the application:** Statistical analysis shows the customers who have used the application, their recurrence, the influence on other services offered by the insurance company, etc.
- **Improvement in the retention of the policies that use the coverage:** Has use of the service had a positive impact on the number of non-renewing customers?
- **The commissions received by third parties:** This product allows commissions to be obtained from third parties in exchange for benefits provided to the company's customers for the services offered in the collaboration agreements.
- **The quality and predictive capacity of the new information (e.g., life habits):** This is for use in life, health and accident insurance as well as in the prevention and improvement of the experience of the insured party.

In short, this pilot is about achieving a closer relationship with the customer and a greater degree of interaction in terms of both frequency and the different types of activities that are complementary to the pure insurance activity. The way of achieving this is not necessarily through the use of blockchain combined with other technologies, but the prototype would serve to assess the different alternatives.

How does blockchain work?

The graph in Figure 3 depicts how blockchain works schematically.

FIGURE 3: ELEMENTS THAT FORM BLOCKCHAINS



A 'block' refers to each unit that forms the chain, formed by the head of the block and the Merkle root.[1] Each block contains different elements:

- Each head of the block contains the *hash* of the head of the previous block, except for block zero, called the 'genesis' block, where the previous hash is just zeros.
- *Nonce*[2] works in combination with the hash as a control element to avoid the manipulation of the information in the blocks (it also incorporates a timestamp).
- Merkle tree hash root of all included transactions.

Each one of the previous blocks can store different operations. In the context of automobile insurance, Block 0 or the genesis block could be the signing of an insurance contract, Block 1 the declaration of a claim and Block 2 a renewal. Transaction 3 within Block 1 could be, for example, sending a photo of the damaged vehicle, to which police reports about the accident or a doctor's report could be attached. Each report forms a different transaction within the Merkle root, which contains a summary of all of the transactions undertaken that depend on the tree.

Each blockchain protocol defines the size of each block, which depends on various factors, such as the speed of the transaction, robustness and verification tests, and on which it is regulated by consensus between the participants. For example, the bitcoin protocol establishes that the size of the blocks must be 1 MB. The capacity of the blocks comes into conflict with the purported scalability of the blockchain, which implies that a system has to grow and adapt without compromising its performance. Continuing the example, a bitcoin transaction typically occupies 0.5 KB on average and, because the blocks must be 1,024 KB (1 MB), 2,048 transactions can be made in one block.

The *hash* function is also known as the summary or digest function. It is defined as an irreversible cryptographic procedure whereby a mathematical algorithm is applied to transform information into an alphanumeric sequence. Whenever the same function is applied to the same content, the same hash will be obtained. In this way, if someone tries to modify any of the content, then the hash will change completely, and so they are very useful in cryptographic applications.

If we use the function Secure Hash Algorithm (SHA)-256[3] to apply the hash function to an input that contains the message: 'Milliman', the resultant output would be:

f65e5463f55186c7c8a515f4e429a02192460ce62d229bf3a46ce581a8c2aeb4

By contrast, if the message were: 'Milliman has written this document,' the hash function would be represented in the following way:

3f1828b144913a7cd6bc5d22b662484b851ab1b77f981afe7450fd206a874cd1

The characteristics of hash functions include:

- No pattern can be deduced from which to trace the input to the output. In other words, it is (currently) impossible to deduce the output of the hash function just by knowing that the input message is 'Milliman' in the previous example.
- It is impossible to reverse. As in the previous point, it is difficult to determine the original message based on the output of the hash function (without having the keys needed to decipher it).
- Whenever the function is applied to the same input, the same hash will be obtained. In this way, whenever the message is 'Milliman,' the same hash will always be obtained, and so it is easy to check whether a transaction has been modified.

Hashes are always the same length regardless of the length of the input. In other words, the size of the message, document or file to which a hash function is applied does not matter. The output will always be the same length (equivalent to 32 bytes).

1 Merkle root : Structure of values in the shape of a tree where each hash is the result of applying a hash function onto a previous hash until it reaches the root hash. In this way, it provides a method of safely and efficiently verifying the contents of large data structures.

2 Nonce (for 'number used only once'): A number that changes sequentially to vary the original message and cause the hash that is obtained to be different for each attempt. The nonce is used to check that a block has been verified and to avoid any kind of manipulation.

3 Secure Hash Algorithm (SHA)-256: A cryptographic hash algorithm developed by the National Security Agency (NSA) of the US and the National Institute of Standards and Technology (NIST) with the purpose of generating unique hashes on the basis of a standard that could be used for encrypting communications. It is one of the most widely used due to the balance it achieves between security and computational cost.

To see the potential of the hash function, let's imagine that we want to protect information about all the books that exist in the library of a university in a single hash, which would occupy just 32 bytes. That is possible given that the block only saves the output produced by the summary function and that has a fixed length, regardless of the size of the files to which the function is applied. Therefore, if we access the hash of a block, we can access the URL address that is associated with that hash, which may be located on the cloud, accessing the address where the books are located. Moreover, if someone tries to modify the document or delete one of the books, the hash function would change completely, and the rest of the participants could reject the operation, and so it also serves as proof of verification.

Other relevant concepts for the operation of blockchain are the concepts of tokens, public and private keys and the validation of transactions.

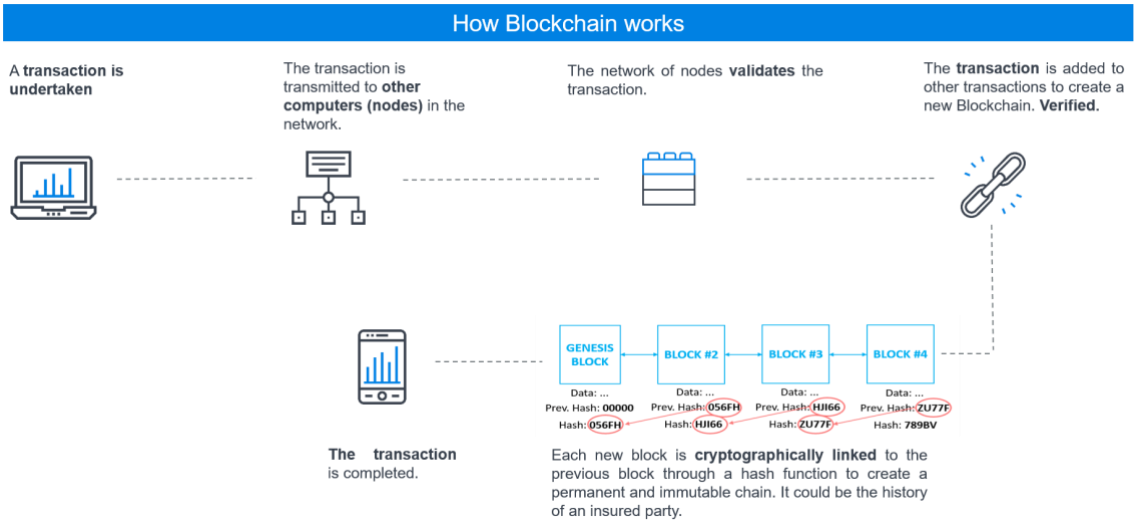
A token is a digital asset in which one or more rights may be incorporated. Any physical, digital or service asset may be uploaded to the chain under the concept of a token. Today, the cryptocurrencies in the bitcoin and Ethereum networks account for a large volume of the tokens that exist. Nevertheless, thanks to the digital fingerprint that the technology allows, any element may be susceptible to being tokenised and, therefore, exchanged in the market with immediate liquidity.

Tokens may or may not be fungible. Fungible tokens are those that are exchangeable for another token of the same value with no regard for their individuality-- for example, cryptocurrencies. Non-fungible tokens have unique characteristics, which means it is possible to distinguish them from other tokens of the same type. Examples include a house, an insurance contract and data about a particular person.

Public and private keys are two cryptographically asymmetric keys that are linked to each other by a mathematical function. The public key is calculated on the basis of the private key. If we know the private key, we can know the public key but not vice versa. If someone wants to send an encrypted message, only the public key is required, which will encrypt the message and which can only be deciphered using the private key. One example of a public key would be a bank account number. A bank account number may be provided to a third party to make a transfer or to record a direct debit, but that third party will never have access to the data or balance of the account nor will it be able to withdraw cash from that account. Only the person in possession of the private key can perform those operations.

Finally, on validation of transactions, when we say that the network of nodes validates a transaction, we refer to the fact that one of the authorised parties that make up the blockchain verifies that the transaction is correct (for example, an independent expert certifies a claim). Once verified, it is shared with the rest of the network automatically. It is not necessary for all of the parties involved and authorised to verify the transaction. In this way, if an independent expert validates a claim, the insurer or reinsurer does not need to verify it again, given that the information can be accessed automatically. If an independent expert certifies a false claim, and that is detected by the rest of the network, then new transactions may be created to correct the previous one, but the possible error or fraud attempt can never be erased.

FIGURE 4: EXAMPLE OF A TRANSACTION WITHIN A BLOCKCHAIN NETWORK



LIMITATIONS AND CONCESSIONS

To put into context the possible current limitations, it is necessary to differentiate between the limitations of the use of bitcoin or any other cryptocurrencies, and the limitations of blockchain technology itself.

In the case of the former, there are limitations that arise due to the bitcoin protocol, such as the execution time of transactions (around 10 minutes). That is the average time needed by network nodes (called 'miners' in the bitcoin parlance) to validate a block, which in this case is done through Proof of Work (PoW). On average, approximately three transactions are performed per second on the bitcoin network (note, only for comparative purposes, that this is significantly fewer than the 56,000 transactions per second that Visa supports on its network). Therefore, although each blockchain's protocol establishes the speed at which transactions on that particular ledger are managed, we are still a long way from implementing efficient blockchain solutions on anything close to a global scale.

Another limitation relates to the computational cost. For cryptocurrencies, the more PoW is used, the more the complexity of the mining required increases, which requires a corresponding increase in the consumption of power needed to keep the network secure.

In terms of the typical limitations of blockchain technology itself, the following stand out:

- **Scalability:** When using a blockchain, each new record must be validated, which means that the operational component is slower than in traditional databases. Each protocol must consider the trade-off between the processing speed of operations and other factors such as the security of the network, resistance to cyberattacks and computational costs. In general, blockchains that do not support cryptocurrencies tend to be scalable.
- **Data protection:** Under EU regulations**,** users have the right to authorise or withdraw permission from any interested entity to access their personal data. Thus, when a company needs to use personal data to undertake its work, it should request access to that data in advance. Such authorisation must be requested when the company requires data other than that previously authorised by the customer.
- **Vulnerability of the cloud:** Traditional cloud-based services require users to register with the service provider and, therefore, they allow that company to administer their identities and digital credentials, a fact that contrasts with the decentralisation nature of blockchain technology. Another limitation would arise in the event that the server that manages the cloud suffers a loss and the blockchain nodes cannot access the information. It is true that this limitation would not actually be caused by the operation of the blockchain technology but rather by the idiosyncrasy of the cloud itself. For these reasons, different business initiatives are emerging that propose a decentralised space on the cloud, allowing for the rental of unused spaces to different users and entities, and where files are divided into different locations in a protected way. Thus, only those who have the private key are able to access the complete information and delete it when requested.
- **Reliability of the data**: Because a record on the blockchain is immutable, it cannot be modified or deleted once integrated into the chain. However, that does not guarantee some incorrect data was not validated initially, and so the auditability can only be guaranteed from the moment it is incorporated. For example, the mileage of a secondhand vehicle could be entered for the first time in the chain after it has already been manipulated. The chain guarantees the consistency of the information from the moment it is incorporated, but the original information could still be erroneous. The protocol allows us to establish that the participant is responsible and/or the validation process for the original data recorded is correct.

In summary, it is important to consider all of the limitations inherent to an emerging technology. In the case of blockchain, many solutions are being investigated thanks to the work of different startups, technology companies and consortiums.

Conclusions

At the moment, insurance companies have a siloed view of their customers; and the same customer may be perceived as a different risk by different companies. The range of premiums offered for the same risk of insuring an automobile, which is diverse in many markets, serves by way of example.

Blockchain, with its properties of traceability and auditability, allows for greater transparency, both by improving knowledge about customers and their needs as well as how that influences the personalisation of their products and services.

The generation of value in the near future will depend to a large extent on the ability of companies to incorporate themselves into digital ecosystems, in which customers will lead the relationship and choose whether they want to present themselves directly or through other partners. Blockchain makes it easier for customers to have control over their data, to choose with whom they share that data and to benefit from a personalised treatment that allows access to information that has never before been so complete. Of course, the use of information must always follow the guidelines of the consumer protection and data privacy bodies.

The use of blockchain technology is maturing and once the research and pilot testing stages are over, the technology will likely transition to real solutions in different industries. In this report, we have mentioned just a few of the known success stories.

The insurance industry would benefit from further maturity of the blockchain technology, although any competitive advantages will not be obtained from the mere adoption of the technology. In our opinion, the priority for insurance companies should be to enhance and update their modelling and programming techniques to support innovation in many different areas.

In conclusion, we think that blockchain technology has the potential to support increased efficiency and business dimensions for insurance companies. Therefore, it is in the interest of those companies to be ready for its future adoption once the technology has fully matured. Moreover, the technology will increase the level of competition. It is the traditional capabilities of the industry that will convert the new risks and opportunities into tangible benefits for each business.

References

How blockchain could address five areas associated with GDPR compliance. IBM. (2018).

IBM and Walmart: Blockchain for Food Safety. Walmart & IBM. (2017).

Blockchain: Aplicación en el sector asegurador. Ruben Nova. (2018).

Why blockchain and IoT are best friends. IBM. (2018)

https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/

https://academy.bit2me.com/

Introducing MOBI: The Mobility Open Blockchain Initiative. IBM. (2018)

https://www.ibm.com/blogs/blockchain/2018/06/introducing-mobi-the-mobility-open-blockchain-initiative/

Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. Satoshi Nakamoto. (2009)

https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Insurance Interrupted: How Blockchain Innovation is Transforming the Insurance Industry. Forbes. (2019).

https://www.forbes.com/sites/andreatinianow/2019/01/09/insurance-interrupted-how-blockchain-innovation-is-transforming-the-insurance-industry/#20faf0683ec6

Monetary Statistics. Blockchain Luxembourg. (2017)

https://www.blockchain.com/es/stats

Milliman

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

José Silveiro
jose.silveiro@milliman.com

Rubén Nova
ruben.nova@milliman.com