Blockchain,

a catalyst for new approaches in insurance

pwc

Thought up as the underlying architecture for the Bitcoin cryptocurrency in 2008, blockchain technology is currently a hot topic and the subject of numerous studies in sectors outside the payments industry to which it has often been confined in the past. Blockchain is considered by some to represent the next technological revolution after the Internet.

In fact, the idea of a decentralised, secure and transparent ledger distributed among users can be relevant to many different fields. The insurance industry, with its highly complex processes, could be a major beneficiary of the technology.

By removing intermediaries in a new type of arrangement, blockchain technology could completely upend the insurance value chain:

- Development/acceleration of new products/markets for which business models were difficult to define until now.

- New approaches to underwriting, contracts and claims management, particularly through a combination of smart contracts and the Internet of Things (IoT).

- Overhaul of the modus operandi of insurance agreements.

- New reinsurance approaches, particularly internal reinsurance via smart contracts.

- Transformation of asset management with automated settlement and delivery of intangibles.

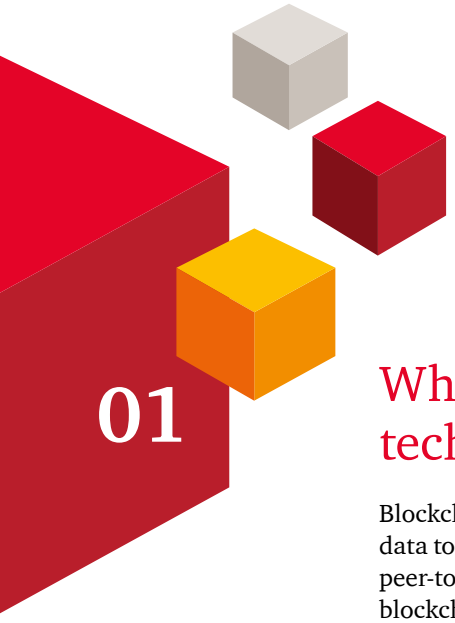
Use of blockchain should help to cut acquisition, management, documentation and compliance costs. It should help new players enter the market and new markets to emerge, particularly in developing countries. By simplifying use and increasing transparency, it will also help to improve customer satisfaction.

Although the upside is significant, several risks should also be anticipated.
These include competition with InsurTechs, a legal framework that will need to evolve, and the challenges of rolling out the technology on a large scale.

PwC's recent study on the topic ("Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance") shows that while 56% of insurance firms recognise the importance of blockchains, 57% still do not know how to respond and capitalise on this opportunity.

Pauline Adam-Kalfon
PwC France Insurance Director

Selsabila El Moutaouakil
PwC France Insurance Manager



How does the blockchain work?

01

What is blockchain technology?

Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer[1] (P2P) basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithms[2]. It is used in a decentralised manner and removes the need for intermediaries, or "trusted third parties".

Blockchain emerged from the marriage of two concepts:

1. **Asymmetrical cryptography**, which allows the use of a **paired public and private key system**.
2. **Distributed IT architecture** (especially P2P).

Asymmetrical cryptography enables users who do not know each other to exchange encrypted information. The system is based on a public key that can be made available to all, and allows encrypted data to be sent to a third party. The third party accesses the encrypted data via a paired private key. The public key is similar to a bank account number, which can be provided to anyone. The private key, which remains secret, acts as the password to the same bank account.

A distributed system is a series of independent computers (nodes) that connect to a network and can communicate with each other. It is similar to the Internet, which also has no central node. Downtime for one server does not affect the other users. The blockchain network is a P2P distributed system. Information is shared among the different users.

The blockchain is open-ended and operates in a decentralised, ongoing manner thanks to the activity of its users who can store information, and to consensus algorithms (notably "proof-of-work" and "proof-of-stake"[3]) which certify the information per block (unit). Users running these algorithms are known as miners. When a block has been validated, it is added to the blockchain and shared with the network. Blocks are connected to each other in such a way that if users wish to change one block, the entire blockchain must also be changed.

On the Bitcoin blockchain, network security is guaranteed by the availability of massive computer power.

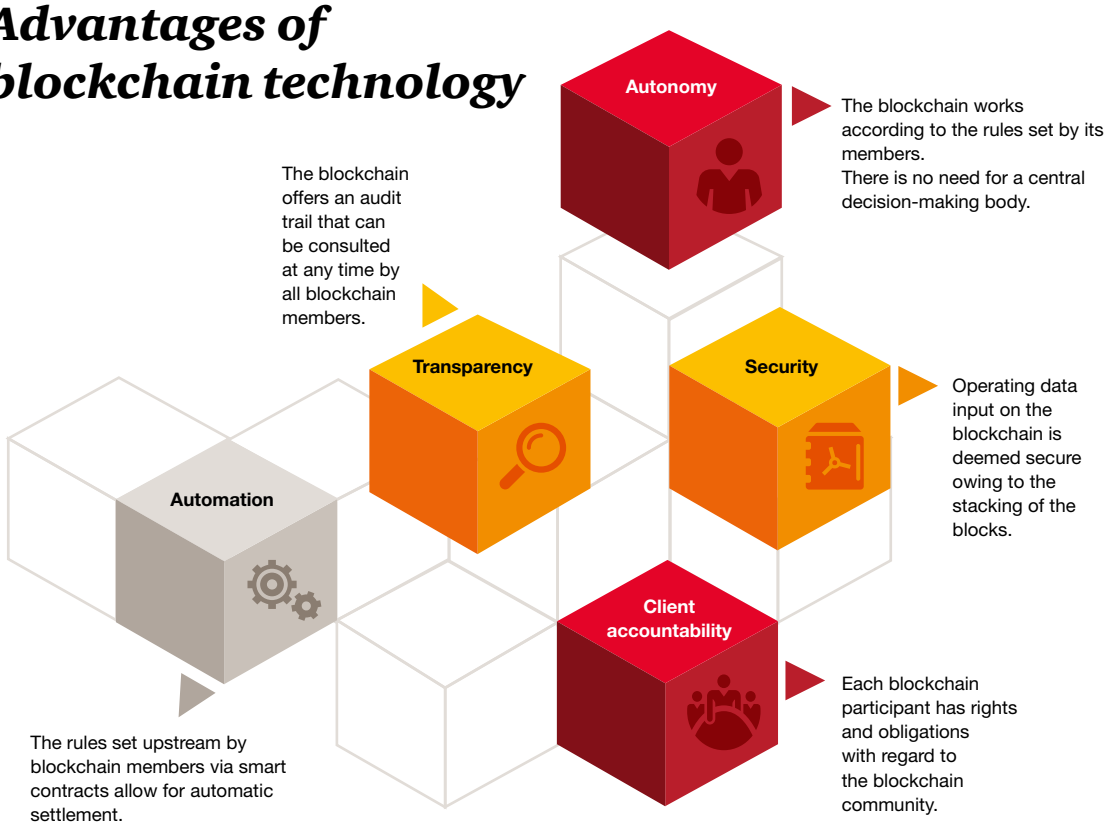
These **two pillars** (**asymmetrical cryptography** and **distributed IT architecture**) make it possible to create a secure environment that establishes a new basis for trust and allows for new ways of exchanging data, new types of transactions and new forms of contracts.

[1] Peer-to-peer, often referred to as "P2P", is an IT network model in which each user represents a server. BitTorrent, Inc. democratised this communication protocol.

[2] Computer programme in which the different nodes agree on a result: first, each computer validates certain information and then sends it on to the other participants. Once all of the information has been received, each computer runs the same algorithm in order to select the right result.

[3] See Appendix.

Advantages of blockchain technology



Source : PwC France

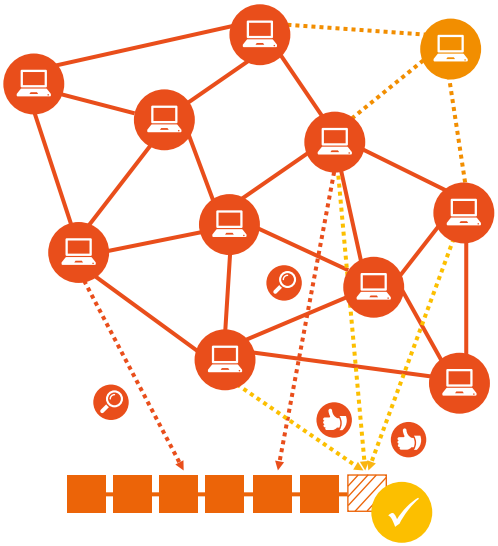
Is blockchain the solution for you?

- ☑ Are multiple parties sharing data?
- ☑ Will multiple parties be updating data?
- ☑ Is there a requirement for verification?
- ☑ Is verification adding cost and complexity?
- ☑ Are interactions time sensitive?
- ☑ Will transactions by different users depend on each other?

If you've answered yes to at least four of these questions, blockchain could be the solution for you.

The 3 categories of blockchain

PUBLIC BLOCKCHAIN 1



Blocks are validated one after another and cannot be modified.

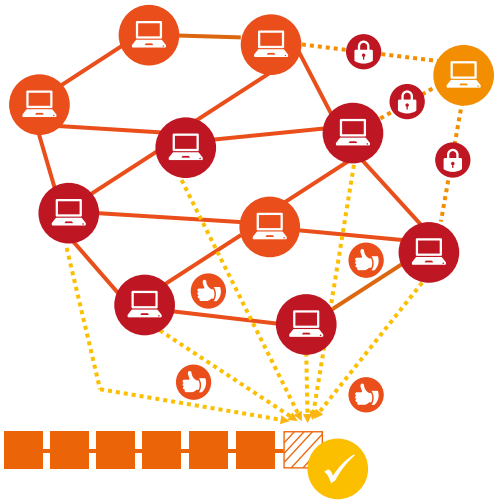
Network nodes

The network is open to any new participants.

All participants can be involved in validating the blocks.

All participants can read the data contained in the blocks.

CONSORTIUM BLOCKCHAIN 2



Blocks are validated one after another and cannot be modified.

Network nodes

Network nodes allowed to participate in the consensus.

New nodes are accepted based on a consensus.

Blocks are validated according to predefined rules (approval from a specific number of nodes).

Read rights can be public or limited to certain nodes.

Private versus public blockchain

Historically, the first public blockchain was Bitcoin, which was launched in 2009. Any computer, regardless of where it is located, can freely access this blockchain and be involved in the process of approving new blocks. New blockchain concepts have emerged since the Bitcoin launch. These new types of distributed ledger offer the advantages of blockchain technology but restrict access to the network and the rights of the different users.

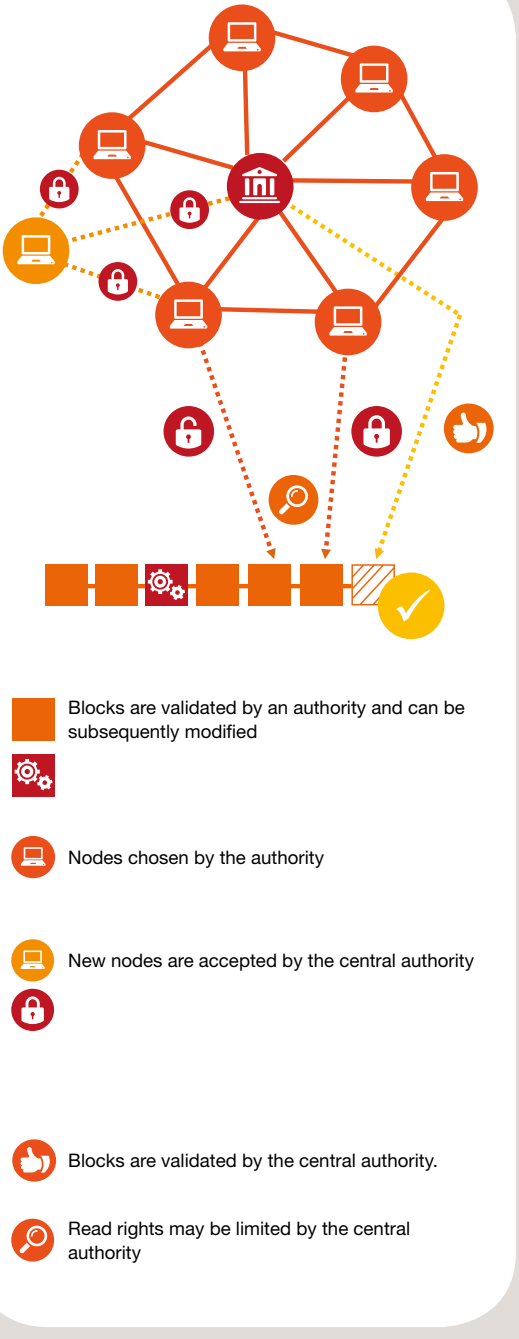
There are currently three categories of blockchain.

Public blockchains: all participants are able to access the database, store a copy, and modify it by making available their computing power. Bitcoin, for example, is a public blockchain.

Consortium blockchains: these are open to the public but not all data is available to all participants. User rights differ and blocks are validated based on predefined rules. Consortium blockchains are therefore "partly decentralised". R3 consortium, which brings together 70 of the world's largest financial institutions to pilot the technology using a semi-private blockchain, is a good example of this category.

Private blockchains: these are where a central authority manages the rights to access or modify the database. The system can be easily incorporated within information systems and offers the added benefit of an encrypted audit trail. In private blockchains, the network has no need to encourage miners to use their computing power to run the validation algorithms. As an example, Crédit Mutuel Arkéa chose a private blockchain to share its customer data among the group's different entities[4].

PRIVATE BLOCKCHAIN 3



Source : PwC France

[4] http://www-03.ibm.com/press/us/en/pressrelease/50087.wss

"Before setting up a private blockchain, you need to ask yourself whether a database is more suited to your needs."

Sébastien Choukroun,
PwC France Blockchain Lab

02

Six examples of blockchain concepts applicable in insurance

Blockchain technology has a wide variety of use cases in insurance, and the examples discussed below are just the tip of the iceberg. Our[5] aim, however, is to shed light on the possible impacts on the insurance value chain.

Smart contracts

A smart contract is a contract between two or more parties that can be programmed electronically and is executed automatically via its underlying blockchain in response to certain events encoded within the contract.

The data needed to execute the contract may be located outside the blockchain. In this case, a new type of trusted third party known as an "**oracle**" pushes this information onto a certain position in the blockchain at a given time. The smart contract reads the data and acts accordingly (execution/non-execution). For example, in the case of cancellation insurance for a train journey, the oracle supplies information about the train's arrival time (which can be taken from the carrier's website or from a GPS sensor fitted on the train).

The company Ledger proposes a hardware oracle solution that allows information to be pushed onto the blockchain in real time[6]. These hardware oracles use a series of sensors (connected devices, the IoT) to track events. There is huge potential here: in 2015, there were already over 5 billion connected devices; this should rise to 20 billion by 2020, for an estimated world population of under 8 billion.

There is a two-fold benefit of using smart contracts associated with the IoT:

1. Automation and autonomy of management processes based on data reported by connected devices and needed to fulfil the conditions for executing the smart contract.

2. Infinite and immutable data history based on a ledger that records all data (including data provided by connected devices). For both the insurance firm and its customers, this acts to guarantee transparency and simplicity, since the related data is present and secure on the blockchain without any action by either party.

Smart contracts therefore offer great potential, particularly in helping to accelerate the development of new models such as on-demand or just-in-time insurance.

On-demand insurance, which can be activated and deactivated at the customer's request, is an increasingly popular product, particularly thanks to the boom in the sharing economy. New players are positioning themselves in this niche, including for example the InsurTech Cuvva, which allows drivers to arrange insurance in just a few minutes when borrowing a car[7]. Beyond this easy example, smart contracts can facilitate and help develop insurance cover in the sharing economy. With blockchain and the IoT, the insurance policy, claim and settlement can be automatically activated provided that the shared asset carries a sensor that can detect the start or end of the insured customer's journey, or any other event triggering an insurance claim or payout. A company called Slock.it is even trying to build the future infrastructure of the sharing economy by enabling anyone to rent, sell or share anything – with no intermediary but with insurance[8] that can be activated/deactivated by means of a smart contact[9]. Based on this principle,

[5]The views and opinions expressed in this paper are those of the authors.
[6] The type of insurance will still be decided by the user.
[7]https://www.ledger.fr/2016/08/31/hardware-oracles-bridging-the-real-world-to-the-blockchain/
[8]https://cuvva.com/about
[9]footnote https://slock.it/technology.html

DocuSign and Visa have already piloted a smart contract for the purchase, finance lease or operating lease of a connected vehicle, where the smart contract is fitted into the dashboard[10]. This partnership aims to facilitate and speed up the process of obtaining the associated paperwork, particularly for insurance, using a purely online solution.

In insurance and reinsurance, several major players have already shown an interest in smart contracts through:

- Partnerships/acquisitions of equity interests. AXA Strategic Ventures took part in a US$ 55 million round of fund-raising for Blockstream, a start-up and partner of PwC. This young company is a renowned specialist[11] in implementing sidechains, or "blockchains underlying a blockchain", which give secure access to applications not available on the initial blockchain (e.g.: micro-transactions on Bitcoin).
- Pilot schemes such as Allianz Risk Transfer's collaboration with Nephila (an investment fund specialised in climate risk). These companies successfully piloted smart contract technology with the aim of accelerating[12] and simplifying transaction processing along with the claims and settlement process between investors and insurers in the natural catastrophe insurance segment.

Among those firms without a PoC or partnership, many have already begun analysing the technology or are at least tracking developments.

[10]https://www.docusign.com/press-releases/docusign-showcases-smart-contracts-payments-prototype-built-for-visas-connected-car
[11]https://www.axa.com/en/newsroom/news/axa-strategic-ventures-blockchain
[12]http://www.agcs.allianz.com/about-us/news/blockchain-technology-successfully-piloted-by-allianz-risk-transfer-and-nephila-for-catastrophe-swap

Oracles as seen by Éric Larchevêque, CEO of Ledger:

Oracles are a fundamental component of any smart contract.

They are in fact trusted automated intermediaries.

Currently, there are three types of oracle:

1. Oracles for online data
2. Consensus oracles
3. Local oracles

Certain physical data can only be gathered by sensors (temperature, power output, etc.). The local oracle works as a secure meter. It is an autonomous IoT, with no data feedback required. Information is transferred peer-to-peer in the form of transactions on the blockchain.

To guarantee data security, a smart card is used. Oracles can be audited and certified. One weakness exists however: the party setting up the system must be a trusted player.

Overhaul of the customer experience and management process via a smart contract

WITHOUT a smart contract

Contractualisation →

Quote
A customer requests a quote for home insurance.

Purchase of insurance
The customer accepts the quote and purchases the insurance.

Hurricane in Miami

WITH a smart contract

=

Enhanced customer experience

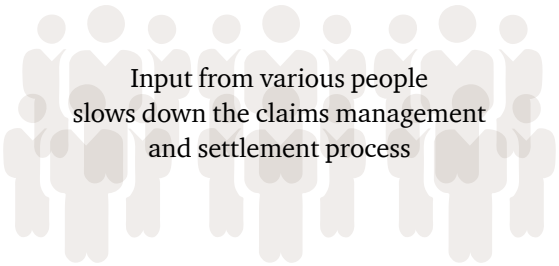
Contractualisation →

Quote and purchase of home insurance for the customer.

Purchase of insurance
The client accepts the quote and purchases the insurance.

Hurricane in Miami

Automatic quote for home insurance thanks to customer information available on the blockchain (existing customer).



Input from various people slows down the claims management and settlement process

Claim management

Customer claim
The customer must submit all of the documents required for settlement.

Assessment
An expert must travel to the site to inspect the damage.

Negotiation of the settlement amount

Settlement

Between several months and several years

Claim management

A GPS device determines whether the house is in the affected area. A drone may be sent to the site.

The weather oracle sends information on the hurricane to the blockchain in real time.

Assessment
An expert must travel to the site to inspect the damage.

Negotiation of the settlement amount

Settlement

Less than a week

Settlement is automatically triggered if the conditions of the smart contract are met. This is determined based on information provided by the weather oracle and the connected devices used to assess the claim.

Source : PwC France

Peer-to-peer insurance

Peer-to-peer (P2P) insurance has been around for some time. And yet practices have evolved since Friendsurance[13] introduced a new distribution model in 2010, with blockchain technology bringing new opportunities thanks to the principle of the decentralised autonomous organisation (DAO).

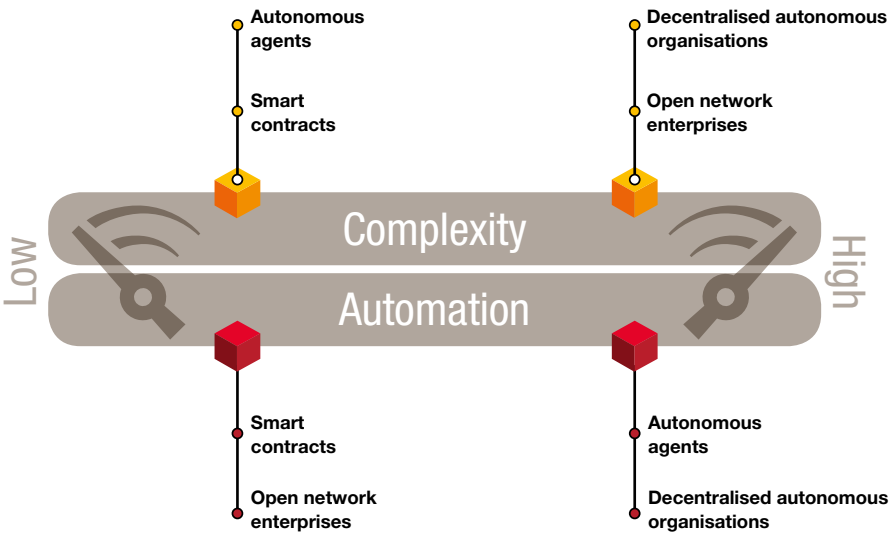
Smart contracts represent the first level of the decentralised application and they often involve human input, particularly when the contract is to be signed by a number of different parties. If the smart contract interacts with other contracts, it can also contribute to an "open network enterprise" (ONE). When ONEs are combined with the notion of an autonomous agent (programmes that make decisions without human input), a DAO, or an organisation that generates value without a traditional management structure, is created.

DAOs enable P2P insurance to be rolled out on a large scale, thanks to their capacity to manage complex rules among a significant number of stakeholders. Both incumbent insurers and new players could therefore position themselves more easily on this fledgling P2P insurance market. After all, P2P is ultimately nothing more than a new vision of risk pooling, the idea at the very heart of all insurance.

[13] This German portal brings together communities of 15 people (families and friends) via social networks. Members who take out traditional individual policies (legal liability, home, mobile device insurance) with Allianz or Axa pool their insurance into a common "pot" which then pays out for any small claims or for the deductible. Customers receive a cashback for responsible claims behaviour.

https://www.friendsurance.com

[14] https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/



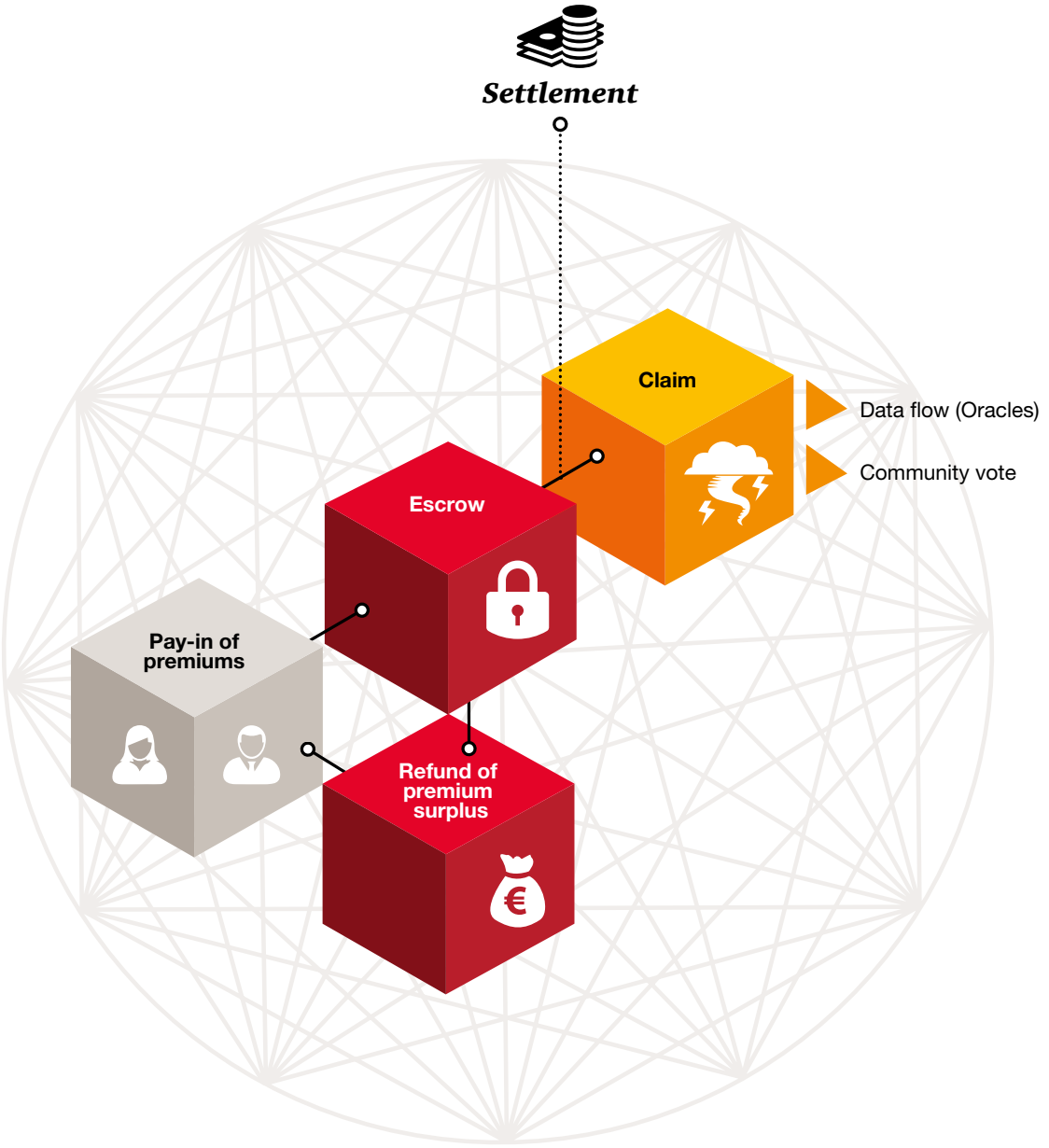
Source : PwC France

The French start-up Wekeep for example, offers to pool insurance premiums for non-mandatory insurance within a smart contract signed by several different parties[14].

Following a claim, settlement would be based on two conditions:

- Confirmation of the insured event via tangible data.
- Agreement of the other members in a vote.

In this type of arrangement, no member holds the funds collected at any time and no central organisation has decision-making power. The claim is settled if the majority (or a predefined percentage) of the members agrees.



Index-based insurance

Index-based insurance is insurance linked to an underlying index such as rainfall, temperature, humidity or crop yield. This approach addresses the limits of traditional crop insurance in rural regions of developing countries, for example, by reducing management and settlement costs. In a region such as Africa, where insurance penetration is just 2% there is genuine scope for this type of insurance to gain in popularity[15].

However, despite the multiple benefits of such insurance, putting in place an index-based product remains complex and costly. Considerable resources and technical expertise are essential in order to develop such products, particularly the infrastructure needed to gather data.

By basing such insurance on smart contracts, index-based products would be automated, simpler and cheaper. A smart contract between a farmer and an insurer may for example stipulate that payment is due after 30 number of days without rainfall. The contract is fed by reliable external data (e.g., rainfall statistics compiled by national weather services) supplied by oracles (see section 2.1), and payment is triggered automatically after 30 days' drought with no need for an insurance claim from the insured party or for an expert on-site assessment. This type of mechanism could represent an alternative to traditional agricultural insurance.

[15] www.proparco.fr/webdav/site/proparco/shared/PORTAILS/Secteur_prive_developpement/PDF/SPD25/Revue_SPD_25_FR.pdf

Possible use in industry agreements

The IRSA Agreement in France – or agreement for the direct compensation of the insured and recourse between car insurance firms – seeks to facilitate the settlement of damages in the event of a traffic accident. Created in 1968 and signed by most insurance firms in France, the IRSA Agreement is key in defining liability for an insured event and in settling insurance claims.

The agreement applies to traffic accidents in France involving at least two landborne vehicles insured by member companies. The principle is simple: "Irrespective of the type of traffic accident and the nature or amount of the damage, member companies undertake, prior to seeking recourse, to compensate their own customers to the extent of their compensation rights, as per the provisions of general legislation."

After an expert has assessed the damage, the insurer determines the liability of its customer and directly compensates the customer for any damage and injury caused. Compensation is directly based on France's traffic regulations, and the liability determined is often in line with the provisions of general legislation. The insurer then seeks recourse against the insurer(s) of the opposing party on the basis agreed between the insurance firms:

- If the amount of damages is below €6,500 excluding VAT, recourse is based on a fixed amount of up to €1,354 excluding VAT if the insured is fully liable. The recourse effected is proportionate to the share of liability of the insured.
- If the amount of damages is above the €6,500 threshold, recourse is based on the actual amount of damages.

The main purpose of the IRSA Agreement is to speed up the settlement process for insured parties based on a common scale, and to ensure that insurance firms settle claims from their customers.

This is a typical situation in which several players are organised around a consensus process based on automatic mechanisms. We could imagine it as a consortium-type blockchain in which the approval process would be controlled by a limited number of selective nodes. For example, participating insurers could agree and organise the blockchain in such a way that a given block must be approved by at least 10 members in order to be valid. In this arrangement, not only is there a limited, selective number of participants involved in the approval process, but the notion of majority rule no longer applies.

In such a context, by acting as an automated trusted third party, the blockchain could clearly help to lower overhead costs while at the same time accelerating management processes and making them more secure. However, for industry agreements, the cost of setting up such an arrangement could be an obstacle, since all participants need to be able to connect their IT processes to such a system.

Other similar industry agreements exist, explaining the recent interest shown by the French Insurance Federation (FFA) in blockchain technology.

Reinsurance

Over the past few years, most major insurance groups have set up internal reinsurance mechanisms, often in conjunction with the introduction of Solvency II. The use of internal reinsurance enables capital requirements to be reduced for individual entities since the risk is transferred to a captive reinsurer, which may be a separate entity, or a department within the holding company. The insurance group can therefore gain in capital efficiency as diversification is concentrated at the level of the captive.

Internal reinsurance mechanisms often entail swift and complex exchanges of information in accordance with regulatory or fiscal requirements. These information exchanges may involve third parties such as brokers or professional reinsurers which supply internal transfer pricing for insurance **at arm's length.**

Insofar as there is a natural internal consensus for this type of situation, it may be possible to organise information flows for the internal reinsurance via a private blockchain.

By automating the execution of reinsurance treaties through smart contracts, the entities concerned (e.g., group subsidiaries) would no longer need to be involved in the "declarative" phases of insurance (contracts, claims reporting, verification, settlement trigger, etc.).

"There would be a whole host of benefits, including a simplified governance structure, auditability, lower costs, greater speed, and confidentiality. In the context of internal reinsurance, blockchain technology offers real potential for reducing transaction costs and improving reliability for insurance groups."

Emmanuel Dubreuil, Partner, PwC France
Advisory Property & Casualty/Reinsurance

Since the mechanism would be rolled out on a relatively small, intra-group scale, IT system investments would be limited.

In intra-group reinsurance, the Blockchain Insurance Industry initiative, or B3i, launched in October 2016 by five of Europe's leading insurers and reinsurers (Aegon, Allianz, Munich Re, Swiss Re and Zurich Re) aims to launch a retrocession proof-of-concept (PoC).

In February 2017, B3i was boosted by the addition of ten more international insurers and reinsurers operating in Asia, Europe and North America (Achmea, Ageas, Generali, Hannover Re, Liberty Mutual, RGA, Scor, Sompo, Tokio Marine and XL Catlin). The results of the PoC are expected to be available in the summer of 2017.

Additional insight from Régis Delayat, Senior Digital Advisor to the SCOR Chairman

In June 2016, SCOR launched a PoC for the exchange of reinsurance accounts with a view to specifically assessing the feasibility of using blockchain technology. The PoC was launched under the aegis of the Ruschlikon initiative, a global community of some 50 insurers, reinsurers and brokers committed to implementing e-administration and driving an efficient and modern market. Assisted by the start-up ChainThat, in two months SCOR successfully piloted exchanges of technical reinsurance accounts between two brokers and SCOR using a private blockchain based on Ethereum.

This first PoC enabled SCOR to gain further blockchain expertise from both an IT and business standpoint (the project involved a multidisciplinary team of around ten people), and to confirm the technology's potential for "disrupting" all interactions within the insurance ecosystem. Its decision to join the B3i industry initiative as from the end of 2016 was a natural follow-on from this project. The aim for SCOR is not so much to confirm the feasibility of blockchain from a technical point of view (since this has already been largely addressed by the Ruschlikon PoC) but to answer questions about security, confidentiality, performance and scalability, and ultimately to identify use cases going forward.

The B3i PoC is making swift progress with significant input from participants. Initial results are expected in the summer of 2017.

The speed with which the market is organising B3i-type initiatives is an excellent indicator that a threshold has been crossed and the potential impact of blockchain technology has been recognised. This could have a snowball effect on the market, driven by leading insurance and reinsurance firms. Each firm will nevertheless decide on its own approach, depending on its priorities. The same applies for work on integrating the technology within proprietary information systems, which will probably require two types of exchanges to be hosted simultaneously for a certain period of time.

Insurers, reinsurers and brokers from the Ruschlikon community are strong advocates for the digitalisation of all exchanges between stakeholders, and the results obtained so far have been convincing. However, volumes are still too low. Use of the blockchain will be a considerable driving force, with significant productivity implications for all players in the ecosystem.

In addition to the tests being undertaken by market players, we are also counting on the task forces being set up within associations and regulatory bodies to help drive home the message and make blockchain an industry-leading technology in insurance, reinsurance and brokerage.

B3i's prototype - known as Codex 1 - is intended to automate catastrophe reinsurance processes. It will bring together insurance companies, brokers and reinsurance companies on the same blockchain. The first live demo is scheduled for Sept 2017 at the Monte Carlo conference.

Transforming asset management

Asset management is a highly regulated industry and involves a significant degree of interaction between its various intermediaries. The distributed ledger technology could improve process efficiency in this industry as well as cooperation between the industry's different stakeholders.

This is already underway in Luxembourg, where 10 major financial institutions came together in the Fundchain initiative to explore the impacts of blockchain technology on the asset management market. PwC is involved in this initiative in order to define applicable use cases[16].

Several applications based on the specific characteristics of blockchain technology are currently being analysed:

- **The removal of intermediaries from asset transfers** by the blockchain relies on a tamper-proof ledger. Transactions can be verified and traced without the need for a trusted third party. Since there is less human input, the risk of error is substantially reduced.
- **Reduction of settlement/ delivery and compliance costs** following market transactions as well as custodian costs for collective investment undertakings. The blockchain can provide certification for each stage of the process, allowing a significant reduction in overhead and operating costs at this level. Although traders may react in nanoseconds, settlements can take several days. Spanish bank Santander believes that blockchain technology will allow banks to save US$ 20 billion each year by reinventing the back office[17].

Illinois start-up Blockchainiz is currently developing projects in this area, working in particular with leading banks to reduce their reconciliation costs in asset management. For all compliance issues, the data needed to ensure compliance with applicable regulations may be written onto a blockchain that can be accessed and audited by all parties or by authorised parties, as applicable.

A new method of pricing assets: the blockchain should help to reduce fraud risk and to refine risk assessments thanks to its role as a distributed ledger enabling all parties to obtain the data they need. This could pave the way for a faster, more efficient asset pricing process.

[16] http://fundchain.lu/

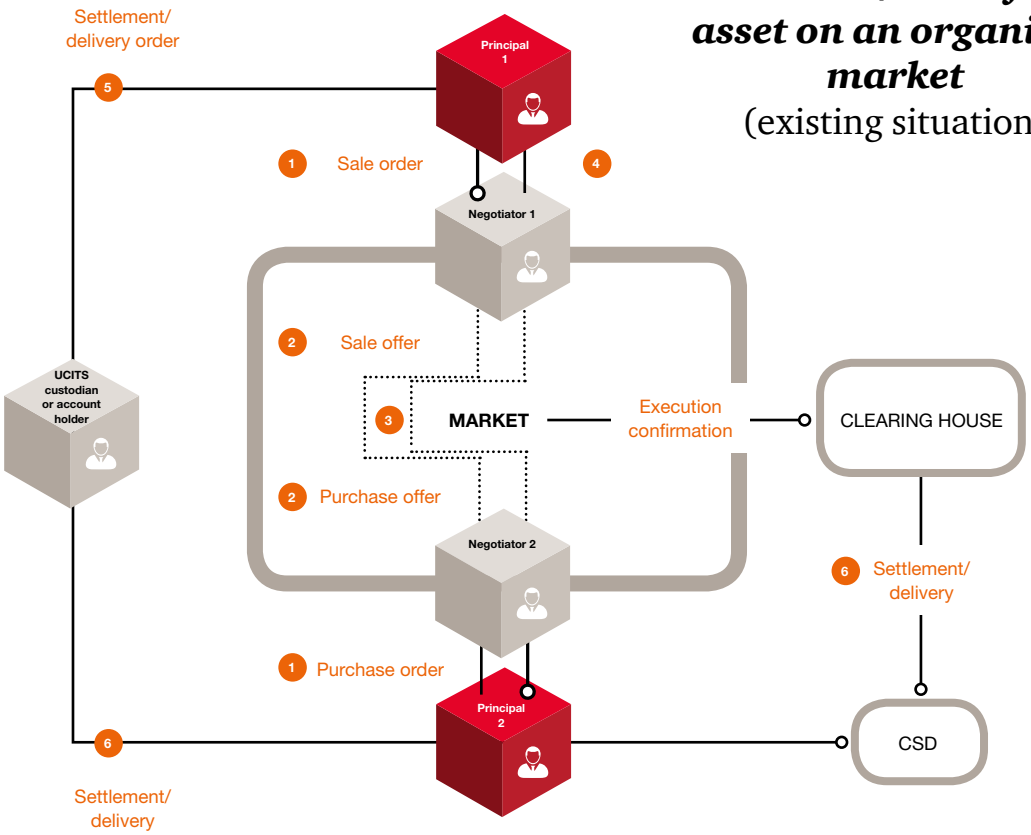
[17] http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

It is hoped that using a blockchain (offering secure and transparent information about assets) in combination with a smart contract will simplify market transactions and remove the need for intermediaries.

Smart contracts enable the settlement/delivery process (4) to be automated once the parties to the contract have exchanged their terms (3).

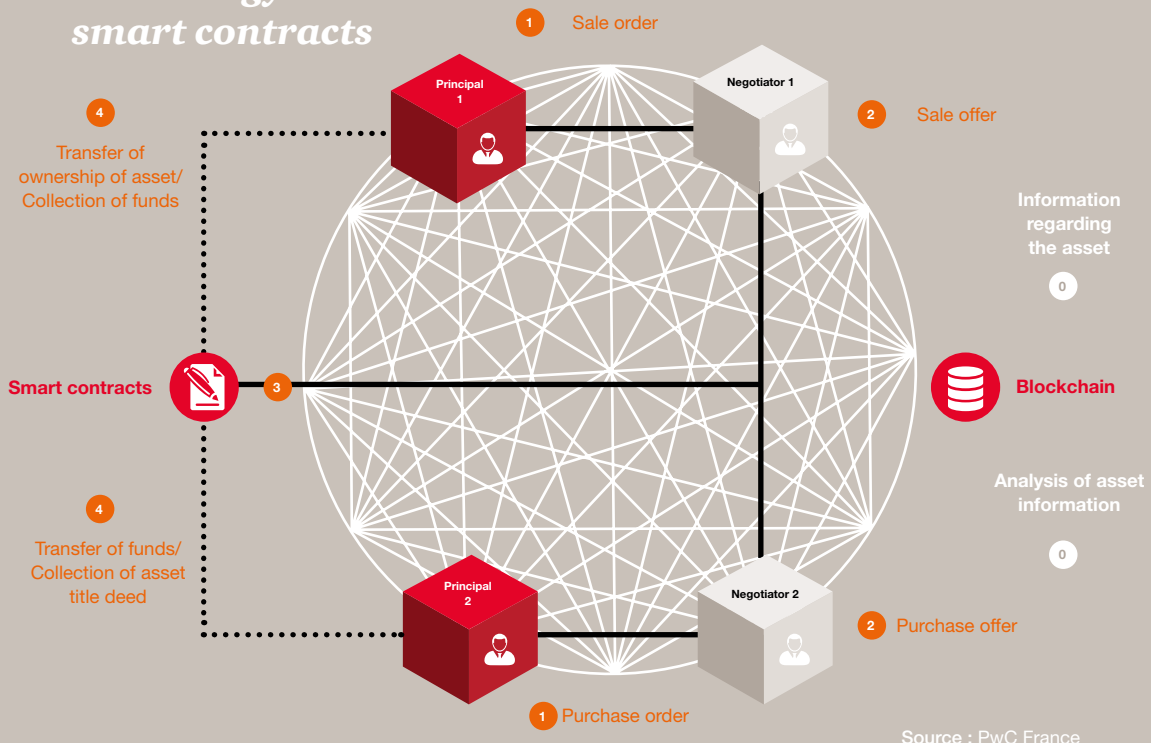
The blockchain provides transparent information on the assets to be sold (0). This information can be accessed at any time, with any changes reflected almost in real time, thereby improving risk management and asset pricing.

Purchase/sale of an asset on an organised market
(existing situation)



Possible change in the asset purchase/sale process

Asset purchase/sale based on blockchain technology and smart contracts



Source : PwC France

Patrick Hennes, Director in PwC Luxembourg's FS Consulting department, takes a look at Fundchain, a unique initiative in Luxembourg focused on the asset management value chain

Fundchain was launched in the summer of 2016 by ten of Luxembourg's leading financial institutions – Banque International du Luxembourg (BIL), BNP Paribas, CACEIS, European Fund Administration (EFA), HSBC, ING Luxembourg, Pictet, RBC Investor & Treasury Services, and Société Générale Bank & Trust – with the participation of PwC Luxembourg, University of Luxembourg and the start-up Scorechain.

The primary aim of the initiative was to develop a proof-of-concept for the application of blockchain, distributed ledger technology and smart contracts in the area of asset management.

Fundchain was organised in different phases and coordinated by PwC Luxembourg. The scenario was as follows:

- Interview-based analysis of current industry "pain points", determination of success factors for the initiative and definition of an example application.
- Blockchain training sessions for all participants in order to guarantee common understanding and take-up of this new technology.
- Common and bilateral collaborative workshops in order to define the particulars of the example application.
- A hackathon to finalise development of the example application and consider its impacts (regulatory, financial, integration) in the production environment.

What was the example application?
After ten or so interview sessions, 12 applications were presented to the steering committee, culminating in a vote on which application to develop. The example application selected was called the **Smart Transfer Agent (Smart TA)**.

The **Smart TA** marks the first step towards a new vision of the asset management value chain. It manages the liability side of operations, i.e., investors, security purchases and sales, and the unwinding of cash and securities transactions.

The **Smart TA** runs on a private Ethereum blockchain and transactions are managed by smart contracts. Different stakeholders in the value chain can access the blockchain through a shared application which manages access rights and the type of information that each stakeholder may access. The stakeholders are the investor, the fund manager, the fund accountant and the regulator.

The stakeholders each have their own node on the blockchain and can access the shared ledger.

What are the findings of the initiative?
The main finding was that the proof-of-concept was a success. Transactions in fund units can be performed on a blockchain with a shared ledger in real time, with the unwinding of cash and securities transactions also performed in almost real time.

Today, Fundchain is in its second phase and has begun to define a new series of goals. Building on its successful proof-of-concept, Fundchain has now chosen to build a product that is viable in the production environment. The initiative is also looking for new international partners, particularly from the asset management industry.

Two major challenges remain:

- Preparation of a detailed report about the initiative and its findings with a view to obtaining a memorandum of understanding from the regulator and supervisory authority to work within a simplified regulatory framework.
- Preparation of specific use cases. Since we are probably at the peak or even just past the peak of the initial blockchain euphoria, we believe that now is the right time to develop use cases with detailed business plans and detailed technical and regulatory impact assessments.

03

What are the benefits of blockchain?

The initial use of blockchains in the corporate environment has been primarily aimed at reducing costs. Here, we discuss five practical examples of what blockchain technology can offer, namely a reduction in KYC costs, lower risk of fraud and insured property theft, a decrease in the need for human input, better pricing for insurance products, and the development of new markets.

Reduction in KYC costs

In the insurance and banking industries and the public sector, the requirement to compile documentation on customers and stakeholders ("Know Your Customer", or KYC) is a costly, time-consuming process which could well be transformed by distributed ledger technology.

A variety of documentation is in fact compiled for a given customer in each organisation, without any of this information being exchanged.

The existing data centralisation model makes organisations particularly vulnerable. The number of cyber-attacks is on the rise and with it, the theft of millions of customers' personal data. Yahoo: 1 billion accounts hacked in 2013, 500 million in 2014; eBay: 145 million hacked in 2014; LinkedIn: 117 million in 2012; JPMorgan: the accounts of 76 million retail customers and 7 million institutional customers hacked in 2014[18]. On the blockchain, data is not stored on a central database and information is protected.

Blockchain technology would lead to substantial gains by pooling processes through a shared, encrypted database. Goldman Sachs considers that consistent, coordinated use of blockchain technology in banking could save the industry between US$ 3 billion and US$ 5 billion a year in KYC and anti-money laundering (AML) costs [19].

Thanks to InterchainZ, a project borne out of a joint initiative between PwC KYC Centre of Excellence and the company Z\Yen, a KYC database prototype has been created using blockchain technology.

The idea is to store and encrypt customer data and verify[20] all those consulting their documentation as well as any changes made (marriage, death, etc.). Customers are given an individual encryption key which they then choose whether or not to make available to financial institutions.

[18] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[19] http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf

[20] http://www.zyen.com/what-we-do/mutual-distributed-ledgers/interchainz.html

The institutions will then be able to access certain documents and data allowing them to identify the customer in a secure, reliable manner. Customers may then contract insurance or open an account in an instant.

Without going so far as pooling data between insurers, banks, brokers and so on, this technology will already help to significantly reduce costs (although the cost savings should be considered alongside the required investment outlay) for groups and their subsidiaries.

This has been illustrated by the partnership between IBM and Crédit Mutuel Arkéa, which recently announced that they had completed their first blockchain project to improve the bank's ability to verify customer identity.

The result of this successful pilot is an operational prototype based on a private blockchain network that provides an overview of customer identity in accordance with KYC requirements for all group entities.

Banks and insurers have various systems that separately manage customer identity for the different services they provide. As a result of this successful pilot, Crédit Mutuel Arkéa group and IBM are working to bring together the different silos of customer data by creating a single cross-business KYC platform to inform all of the bank's processes, helping to reduce unnecessary duplication of information and requests. Blockchain technology identifies and uses all valid existing data already stored in the bank's multiple systems of record, such as those relating to loan applications, life insurance enrolments and bank account openings.

In this instance, blockchain technology helps reduce costs by decreasing the need for personnel focused on KYC tasks, shortens processing time and therefore improves the customer experience. Reputational risk, which is a major concern for insurers, is also significantly reduced. Blockchains therefore help to simplify administrative processes and deliver efficiency gains. Customers receive better service, human error is avoided, and costs are reduced (the costs associated with processing such data are eliminated).

Lower risk of fraud and theft of insured property

Blockchain technology will also help organisations to tackle fraud. As an example, Everledger, which emerged from the start-up accelerator programme implemented by insurer Allianz France, has developed a certification system for luxury products that uses a mix of private blockchain/public blockchain technology[21]. Everledger uses a blockchain to create a global registry for precious stones. Specifically, Everledger inputs 40 characteristics for every stone recorded (cut, colour, clarity, etc.). This represents 40 metadata components which are then used to create a unique series number. This number will be laser-engraved on the stone and added to the relevant blockchain[22]. Once the database contains sufficient data (over one million diamonds had already been recorded at end-2016), if sellers cannot provide encrypted proof that they own the rights to the precious stone, it will be very difficult to sell. Any stones that are not engraved with the serial number or on which the engraving is difficult to see will lose substantial value.

By creating a global, tamper-proof registry, Everledger is making an effective contribution to the fight against theft and fraud, which costs insurers an estimated US$ 50 billion every year.

An equivalent example can be found in the directors' and officers' liability insurance market, which insures business leaders for actual or alleged errors that may be committed during the exercise of their duties, such as publishing inaccurate financial statements, failing to comply with legal provisions, and failing to pay salaries, severance or taxes.

Making financial transactions - and even companies' published financial statements - secure would help to increase transparency and therefore mitigate risks for a market with a total theoretical capacity of over €500 million.

[21] https://www.everledger.io/#do

[22] Source: The blockchain explained by Netexplo.

Automation of tasks with zero added value

Thanks to blockchain technology, processes can be automated and rendered more secure by eliminating the need for certain instances of human input.

A practical example of this is natural catastrophe insurance, which can be arranged using smart contracts as has been successfully piloted by the Allianz group since June 2016. The group's settlement system simply requires two items of information that are incorporated into the programme:

- The event must have been declared a natural catastrophe.
- The location of the insured event must correspond to the region recorded as having suffered a natural catastrophe.

The aim is to avoid a repeat of Storm Xynthia (February 2010), when most victims were no longer in possession of the documents needed to submit their claims and had to wait over a year to receive their insurance payout. This type of incident, as well as being costly and protracted, tarnishes insurers' reputations and makes customers wary of the insurance system.

The Allianz group's use of a system based on a smart contract for reinsurance ("natural catastrophe swap") improves the way in which claims are dealt with while reducing human input (since the contract is automated). When an event occurs that meets predefined conditions, all eligible catastrophe insurance contracts are automatically executed thanks to a code. This code also directly activates insurance payouts without the need for the customer to supply the requisite paperwork. However, the principle prohibiting unjust enrichment of a claimant on occurrence of an insured event is still applied.

As is the case for KYC teams, third-party administration and claim costs can be significantly reduced.

Better pricing

Recent advances in pricing have shown how static and dynamic behavioural factors influence risk, with insurers increasingly trying to capture these behaviours. Behavioural information could be compiled by connected devices and exchanged on a blockchain, so that prices would be almost constantly adjusted and optimised based on real-world information reported by the blockchain in real time. This remains a very innovative area, which still needs significant analysis and research.

Irrespective of blockchain technology, the insurance industry will inevitably evolve in a world where voluntary data sharing and the ability to assess customers' behaviour and risk profiles on an ongoing basis will result in dynamic pricing and in dynamic, flexible and personalised insurance products and risk management.

Although blockchain-based dynamic pricing is clearly not for the immediate future, the impact of the technology on prices could be felt much sooner.

Underwriting, pricing and claims management processes may for example become faster and more efficient by deploying rules within smart contracts, which, in itself, would affect the competitiveness of the solutions on offer.

Emergence of new markets

Blockchain technology will enable new lines of insurance to be developed or expanded, as well as emerging markets to be reached. Today, 40%[23] of the world's population possesses neither a bank account nor insurance, particularly in Africa, Asia and South America.

A wider variety of insurance products and services

Using blockchain technology, insurers will be able to more quickly develop personalised products and services and enhance their insurance offer.

One trend in travel insurance for example is to offer insurance payouts in real time in the event of a covered claim. This is the value proposition developed by Berkshire Hathaway Travel Protection for instance[24]. Such positioning means that the insurer must connect its systems to those of airline companies (to obtain information on flight delays or cancellations for example) and then identify in its customer database those customers affected by the flight in question. This would then proactively open a claim which would entitle the customer to a prompt payout.

With blockchain technology, this value proposition could be managed in a fully automated manner, thereby reducing costs. InsurETH, based on an Ethereum smart contract and the result of a hackathon launched in 2015, has positioned itself precisely on this type of market[25].

In this case, blockchain technology enables the fast-paced development of new services linked to a given product range. By combining data from contracts, claims and customer documents in general, the blockchain will also speed up the development of personalised insurance.

[23] Source: World Bank Financial Inclusion Database 2015.

[24] https://www.bhtp.com/blog/our-new-products-reinventing-travel-insurance-again

[25] http://insureth.mkvd.net/

Growth in emerging markets

Blockchain technology will also enable companies to reach new geographical markets, especially in developing regions in Asia and Africa. Thanks to the low incremental costs associated with smart contracts, new insurance products should be able to be developed in these countries.

As mentioned earlier, insurance penetration in Africa remains low. At the same time, the mobile telephony market has enjoyed explosive growth over the past few years, with over 70% of sub-Saharan African individuals now owning a mobile phone[26]. This has led to the development of mobile-based payments via telecom operators, which are increasingly usurping the role of banks. The most striking example of this is Vodafone's hugely successful M-Pesa, launched in Kenya in March 2007[27]. This mobile phone-based payment system already has more than 20 million users and sees over US$ 19.7 million transferred through its network each day.

The insurance sector could also capitalise on the boom in new technologies to develop across Africa. Blockchain technology can help to simplify underwriting and information gathering processes, since those with an account would not need to show ID or present their bank details. A smart contract could be set up for a blockchain linked to customers' mobile data, triggering an automatic settlement process should an insured event occur.

In many African countries, a substantial portion of the population does not have an official address. This causes numerous administrative headaches, since the lack of property rights generates problems with inheritance, limits the use of lending and makes it hard to take out any home insurance. Thanks to blockchain technology, simple GPS coordinates written onto a server would serve as the basis for a tamper-proof land register that can be accessed by all users, thereby facilitating the arrangement of home insurance.

Several other applications for distributed ledger technology have already been identified.

Blockchain technology would make contract subscriptions easier, such as in corporate insurance, for which a formidable amount of documentation needs to be provided (type of collateral, presence of alarms, type of windows, etc.) and often requires the on-site presence of an expert appraiser. In the future, insurers could help municipalities and construction/housing development companies to create DAOs using blockchain technology to store construction data or references used for security purposes. Companies would find it easier to take out insurance in these markets where there is still relatively little coverage.

[26] http://www.proparco.fr/webdav/site/proparco/shared/PORTAILS/Secteur_prive_developpement/PDF/SPD25/Revue_SPD_25_FR.pdf

[27] https://www.mpesa.in/portal/customer/AboutMpesa.jsp

04 Foreseeable risks

The distributed ledger represents a clear opportunity for players in the insurance industry. However, several issues relating to market trends and technological change need to be considered. First, we need to take into account, as of today, the new competitive landscape that will emerge from the use of blockchains, as well as the need to rethink governance structures. Second, we must not overlook the fact that the development and use of this technology will require changes to the applicable legal environment. Lastly, one of the most critical issues today is scalability.

A new competitive landscape

Some InsurTechs have capitalised on opportunities created by blockchain technology, as illustrated in the various examples outlined above.

A recent PwC study (Opportunities await: How InsurTech is reshaping insurance)[28] shows that 90% of insurance companies are concerned about competition from InsurTechs. Stephen O'Hearn, PwC Global Insurance Leader, sums up the situation:

"There is a risk of missing an opportunity to deliver customers a similar experience to one they already receive from retail and technology companies. InsurTech will be a game changer for those who choose to embrace it. Insurers have unrivalled access to consumer data and using cutting-edge technology to thoroughly analyse it could result in significant benefits for the company."

To head off this competitive threat, incumbents are starting to set up partnerships.

AXA, for example, launched Kamet, a €100 million InsurTech incubator[29], while Allianz France has invested in SmartAngels[30], a crowdfunding specialist that uses blockchain technology to keep records of securities issued by companies raising funds on its platform.

Governance and maintenance challenges

Although the technology and the definition of specific algorithms (which transform rules and principles into actions) can help set up a certain type of "decentralised" structure, there is still a need to define, put in place and maintain over time a specific governance and management model – a new way of making decisions, approaching an organisation's strategy, defining a community's goals, or determining a company's values. Increased dependence on such rules brings with it specific risks.

[28] http://www.pwc.com/gx/en/industries/financial-services/fintech-survey/insurtech.html

[29] https://www.axa.com/en/newsroom/press-releases/axa-launches-kamet

[30] https://allianz.smartangels.fr/

A semi-private blockchain needs a clearly defined governance structure, including resources that can be pooled to ensure that this structure will be respected over time. Maintenance requirements also need to be planned for.

Deployment on a public blockchain allows governance issues to be bypassed but results in exposure to operational risks such as sudden obsolescence due to a change in the blockchain or the project being abandoned due to a loss of interest among users in the blockchain selected.

An evolving legal environment

Although the blockchain is likely to require changes to the applicable legal environment, blockchain participants today are nevertheless bound by existing rules depending on the application in question. As is often the case with innovative technology, existing legal principles provide a framework for its use, despite the lack of any specific laws and regulations. The absence of specific provisions regarding a new technology does not therefore constitute a legal vacuum.

In France, a legal definition of the blockchain was recently included in Ministerial Order no. 2016-520 of 28 April 2016 on certificates of deposit. This Order amends Article L 223-12 of the French Monetary and Financial Code, which surreptitiously defines the blockchain as a shared electronic recording system allowing for the validation of specific transactions in securities to be exchanged on crowdfunding platforms ("mini-bonds"). Article L.223-13 states that "the transfer of ownership of the mini-bonds results from the input of the sale in the shared electronic recording system referred to in Article L.223-12, which replaces a written contract for the purposes of Articles 1321 and 1322 of the French Civil Code". Recording the issuance of mini-bonds on the blockchain is deemed to constitute a written contract – said written contract being required if the transaction is not to be void – and is therefore binding on third parties.

"We need to be wary of the term 'legal vacuum' when talking about the blockchain, because even though no specific regulations have been introduced for the technology, there are legal principles that, in the initial phase, facilitate innovation and the development of new applications. So the blockchain – like all new technologies – exists within a legal framework. In fact, the consensus protocols established to organise blockchain governance already constitute an agreement between parties. Rather, we should speak of change. The real difficulties lie in the need to (i) establish new classifications and apply an appropriate legal framework to the technology in order not to limit its possible applications, and (ii) take into account the international dimension."

Sandrine Cullaffroz-Jover,
Lawyer and Director
at PwC Société d'Avocats

Legal issues arise particularly when considering the legal validity of smart contracts, which represent the decentralised automated function of the blockchain. The term is misleading, since smart contracts are not contracts so much as IT protocols that trigger the automatic execution of contractual conditions previously set by the parties. In theory, nothing prevents the agreement contained in smart contracts constituting a written contract between the parties, provided that it meets the conditions required for the establishment of an electronic contract. Specifically, this means encoding the steps that provide evidence of acceptance of a given offer and ensuring that the parties are clearly identified, so that the contract is legally valid. However, difficulties arise regarding the very nature of the technology, which is rooted in immutability. For example, how would smart contracts manage contingencies during execution?

Consensus protocols aimed at organising blockchain governance already in themselves represent an agreement between parties. These rules structuring how the blockchain should be used and managed nevertheless have the undesired effect of remaining concentrated in the hands of the encoders, while the blockchain's participants are merely asked to accept them.

A series of internationally standardised technical rules could help facilitate transactions in view of the diversity of the geographical regions and parties using smart contracts.

The international dimension of the blockchain may also require international transfers of personal data, with participants being bound by a specific law.

A consensus protocol governing the use of participants' personal data is therefore essential to guarantee the rights of those concerned and to ensure system security.

Since they appear on a ledger shared across the globe, the information recorded on a blockchain may be consulted in countries with no data protection laws. However, under the European Regulation on Data Protection (Regulation EU 2016/679 with immediate effect as from 25 May 2018), personal data may not be transferred to countries that fail to offer adequate data protection, subject to administrative fines of up to €20 million, or in the case of companies, of up to 4% of their global annual revenues for the previous year.

The technical characteristics of public blockchains can also present sticking points in terms of rights to information, access, modification or erasure (right to deindexation or right to be forgotten) of those concerned by the data processed. Blockchain consensus protocols would also need to include a mechanism for obtaining prior consent from the parties concerned.

The launch of "The DAO" (Decentralized Autonomous Organisation) perfectly illustrates the immutable nature of public blockchains. The DAO is a type of decentralised investment fund that functions in a horizontal manner. Participants initially invest to build up the fund. Subsequently, other participants together assess the viability of the projects submitted and decide whether or not to finance them.

In June, a participant managed to exploit a known flaw in the blockchain's original code to siphon off the funds held by the decentralised organisation (at the time, the amount stolen represented more than 3% of all Ethers on the market). This smart contract was supposed to be public and immutable, and accordingly managed with no human input.

Note: In thinking about this incident, it is important to bear in mind that the problem was not with the Ethereum blockchain itself but with the algorithms underlying the DAO platform.

This incident gave rise to lively discussions, particularly regarding blockchain immutability and the potential legal validity of the IT code underpinning the DAO project. On one hand, part of the Ethereum community supported a "code is law"-type solution, considering the transaction carried out without The DAO's knowledge "legitimate" since it followed the predefined rules. On the other, many supporters of a solution more in keeping with the "spirit of the contract" considered that the code had no legal value and that therefore the hacker's actions, reflecting unlawful use of the blockchain, should be cancelled in order to allow the shareholders of The DAO to recover their investments. This solution implied backtracking to the block containing the disputed transaction (the transfer of funds by the hacker to his or her address) and the creation of a new block (to replace the former block) transferring the funds to an address where investors could only withdraw their investments in exchange for their DAO tokens (tokens representing their shares in The DAO).

This solution, widely reported in the media, led to a "hard fork" in the Ethereum blockchain. When the Ethereum foundation intervened to replace the old block with the new block and new rules, participants had two possibilities:

- To validate the new block with the new rules.
- To reject the new block and continue to accept blocks based on the previous system.

Two parallel chains were created, similar to a fork. What is interesting is that the hard fork solution activated in July 2016 gave rise to two blockchains that still exist today, even though most experts believed only one of the chains could survive.

On one side, the "Ethereum" (ETH cryptocurrency) blockchain was created when part of the community followed the block put in place by the Ethereum foundation, allowing The DAO investors to recover their Ethers, Ethereum's cryptocurrency.

On the other side, the "Ethereum Classic" blockchain represents the other part of the community, which rejected the proposed new rules.

What can be learned from this incident is that a blockchain operates on a consensus basis. Although the hard fork incident led to a breakdown in the consensus, most other decisions are consensus-based. In November 2016 for example, "Spurious Dragon", a fourth hard fork on the Ethereum blockchain, was implemented in a response to DoS attacks on the Ethereum network. The previous hard fork known as "Tangerine Whistle" addressed urgent network health issues concerning the execution of operating codes.

This hard fork was deployed without any problems and the resulting new chain became the "reference" blockchain.

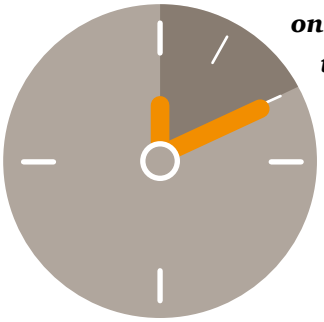
It is likely that thoughts about the legal environment will be influenced by cryptofinance centres of expertise such as the one being built in the Canton of Zug near Zurich. Zug is looking to reinvent itself as "Crypto Valley" and attract future start-ups in this new industry. In May 2014, Johann Gevers, founder of Monetas (a universal smart contracting platform) chose Zug as the location for the Digital Finance Compliance Association (DFCA), an initiative that offers the industry an opportunity to build the most favourable regulatory environment in the world. Switzerland in fact enjoys a unique regulatory landscape thanks to its decentralised structure and the possibility it offers companies of setting up and deploying self-regulated organisations (SROs) that define industry standards. Zug today represents a hub for testing and developing blockchain technology in a stable, enduring legal environment.

In France, the technological research institute System X based at the Saclay platform launched a Blockchain for Smart Transactions (BST) project in early 2017. Over the next four years, this project will study new services and uses, cost optimisation and also the ethical issues raised by blockchain technology. Specifically, the project will look at mechanisms of digital trust that can give back to customers control over their data. The legal conditions of deploying the blockchain will therefore also be studied as well as the related economic and social conditions.

Scalability

Besides legal limitations, several technical limitations mean that current blockchain technology is difficult to scale up. The Bitcoin blockchain for example (the most secure public blockchain to date) can carry out a maximum of seven transactions per second (far fewer than the thousands of transactions per second carried out on the Visa network), because the protocol only allows blocks of up to 1 MB in size.

This figure can change, but only if agreed by the Bitcoin community, which has seen lively debate on these issues. Owing to the complex governance of this public blockchain, some time is undoubtedly needed before these limitations can be eased through a new consensus.



A delay of ten minutes on average is needed to add a block to the Bitcoin blockchain.

However, new solutions are being implemented to enable the networks to absorb a greater volume of transactions, for example[31]:

- Segregated Witness, a change in the Bitcoin blockchain that enables the usable capacity of each block to be increased.
- Lightning Network, a change in the Bitcoin blockchain that groups together transactions in order to increase the maximum permitted transaction volume.
- Sidechains, which are a means of extending existing blockchains and therefore increasing the maximum permitted transaction volume.
- IOTA, "the blockchain that is not a blockchain", which launched in late 2016 and is set to be the first blockchain naturally able to absorb a large volume of transactions.
- ARDOR, launched in 2017, which also claims to be able to absorb high transaction volumes. However, the design for this blockchain has not yet been unveiled.

It therefore seems that the question is no longer whether blockchains will be capable of absorbing a large volume of transactions, but when they will able to do so.

[31] http://www.pwc.fr/fr/expertises/audit-et-business-assurance-services/business-assurance-services/rvms/blockchain-applications-concrete.html

"The blockchain is set to revolutionise business processes over the next five years, provided that businesses are prepared to incorporate this innovative technology. The biggest risk regarding the blockchain is... not taking any risks."

Marie-Line Ricard, Partner,
PwC Blockchain Lab Leader

Conclusion

If blockchain technology is attracting unprecedented attention from senior management, it is because the potential impact on current business models raises a host of questions.

Blockchains will help to manage increasing global complexity by combining security, decentralisation and transparency. They will give power back to the customer and will help bring new players into the market.

The technical limitations of blockchains must be considered. However, the fact remains that the use cases for which blockchains are paving the way will be deployed regardless, whether with blockchain technology or with an alternative.

For the insurance industry, the number of potential use cases goes well beyond those discussed in this report, with varying impacts on the value chain.

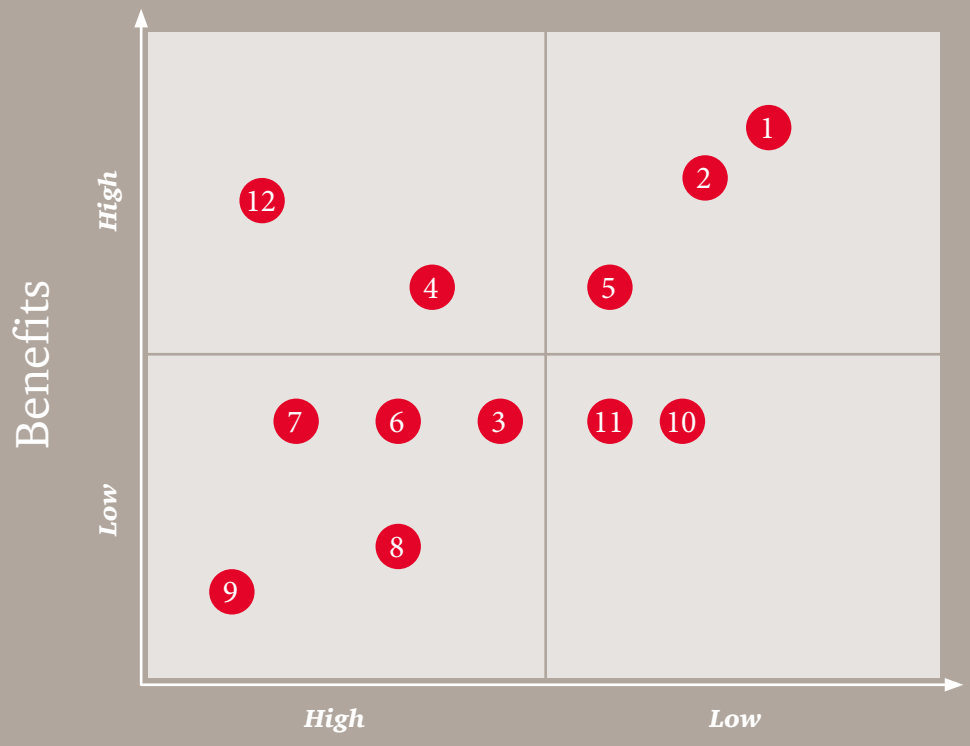
Certain uses seem easier to implement and appear to offer significant benefits, while others may be riskier, particularly in light of the expected rewards.

The scope of possibilities brought about by the blockchain is huge in the insurance industry but will require a period of adaptation and adjustment.

The key challenge for all players, irrespective of their industry, will be to identify the use case that will be of most benefit to them and to explore others if their first choice proves unsuccessful.

Examples of blockchain use cases

1. Contract documentation
2. Claims management
3. Contract eligibility
4. Multi-national insurance policy
5. KYC/AML
6. Inter-firm accounting
7. Sensitive data management
8. Management of exposure in real time
9. Guarantee management
10. Excess of loss reinsurance
11. Personal data management
12. Emerging market



Sources: PwC study, "Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance"

Appendices

01

How a blockchain works

A blockchain is used as a platform for exchange

Each user can carry out a transaction by modifying the ledger. For simple exchanges of tokens, the problem can be summarised by the following information: who – gives what – to whom? So if blockchain participant X wants to send 10 tokens to participant Y, a line that looks like "X_10_Y" is added to the ledger. The nodes ensure that the structure of the entry is correct and that X is solvent. If this is the case, the transaction is gradually sent across the entire network and added to the list of transactions pending.

In each period (an average of 10 minutes for the Bitcoin blockchain and 15 seconds for the Ethereum blockchain), some of the transactions pending are included in one of the blocks in the chain. The party adding a block determines the content of that block.

Users adding blocks to a chain are known as "miners" in reference to the 19th century gold rush. Miners are paid the proposed reward for adding a block plus transaction fees.

When the block is added to the chain and consensus exists regarding the block, it is shared by all network nodes. This gives rise to a unique transaction history.

02

Proof-of-work versus proof-of-stake

Proof-of-work is the consensus algorithm used by the Bitcoin blockchain. Miners provide an external resource – computer power – in order to participate in the block validation process.

Proof-of-stake attempts to move away from the power-hungry mining mechanism. The right to validate blocks is directly linked to the amount of cryptocurrency held.

Acknowledgements

This report was prepared under the supervision of Pauline Adam-Kalfon, Director, PwC Consulting Financial Services, with assistance from Selsabila El Moutaouakil and Corentin Richard.

We would like to thank the following people for their contributions:

- Régis Delayat, Senior Digital Advisor to the SCOR Chairman
- Éric Larchevêque, CEO of Ledger
- Patrick Hennes, Director, PwC Luxembourg Consulting Financial Services
- Sandrine Cullaffroz-Jover, Director, PwC France Société d'Avocats
- Emmanuel Dubreuil, Partner, Partner, PwC France Business Advisory Services
- Marie-Line Ricard, Partner, PwC France Advisory
- Sébastien Choukroun, Senior Associate, PwC France Advisory

Contacts

Pauline Adam-Kalfon
Director, Insurance
PwC France Consulting
pauline.adam-kalfon@fr.pwc.com
https://fr.linkedin.com/in/paulineadamkalfon

Emmanuel Dubreuil
Partner, Actuarial Services
PwC France Business Advisory Services
emmanuel.dubreuil@fr.pwc.com
https://www.linkedin.com/in/emmanueldubreuil

Marie-Line Ricard
Partner, Blockchain Lab Leader
PwC France Advisory
marie-line.ricard@fr.pwc.com
https://www.linkedin.com/in/marielinericard

Jimmy Zou
Partner, France Insurance Consulting Leader
PwC France Consulting
jimmy.zou@fr.pwc.com
https://www.linkedin.com/in/jimmyzou/

Patrick Maeder
Partner, EMEA Insurance Consulting Leader
PwC Switzerland Consulting
maeder.patrick@ch.pwc.com
https://www.linkedin.com/in/pmaeder/