

Blockchain :

Où converge le secteur d'assurance ?



SOMMAIRE

01.

Introduction

02.

Principes de la Blockchain

03.

Smart Contract

04.

Technologie utilisée en blockchain

05.

Cas d'usage de la blockchain en assurance

06.

Conclusion

07.

Annexes

La Blockchain, une promesse d'innovation



La Blockchain est devenue aujourd'hui une thématique incontournable face à l'accélération du processus de digitalisation des entreprises. Afin de comprendre l'engouement suscité par cette nouvelle technologie, la crise financière de 2008 est un déclencheur. Au-delà de la catastrophe économique et de l'instabilité du marché, dès 2008 les développeurs se sont dirigés vers une technologie innovante afin de créer des algorithmes capables de suivre l'origine des transactions de manière infalsifiable.

Si l'industrie de l'assurance française s'intéresse à cette nouvelle technologie, c'est parce qu'elle promet des changements profonds et révolutionnaires dans la gestion des transactions. Elle permet de transmettre et de stocker des informations transparentes et sécurisées grâce à un système informatique innovant organisé comme un réseau pair-à-pair. Un ensemble d'ordinateurs, appelés les « nœuds », sont interconnectés. Chacun d'eux conserve la copie des transactions effectuées.

La blockchain se définit comme un registre distribué, dit « a distributed ledger ».

A fortiori, le temps a fait évoluer notre philosophie. En observant les grands opérateurs de la fintech, nous constatons qu'il ne s'agit pas de changer le système actuel. À l'inverse, il faut rationaliser le système et le sécuriser. Nous devons permettre un dialogue dans un monde interconnecté.

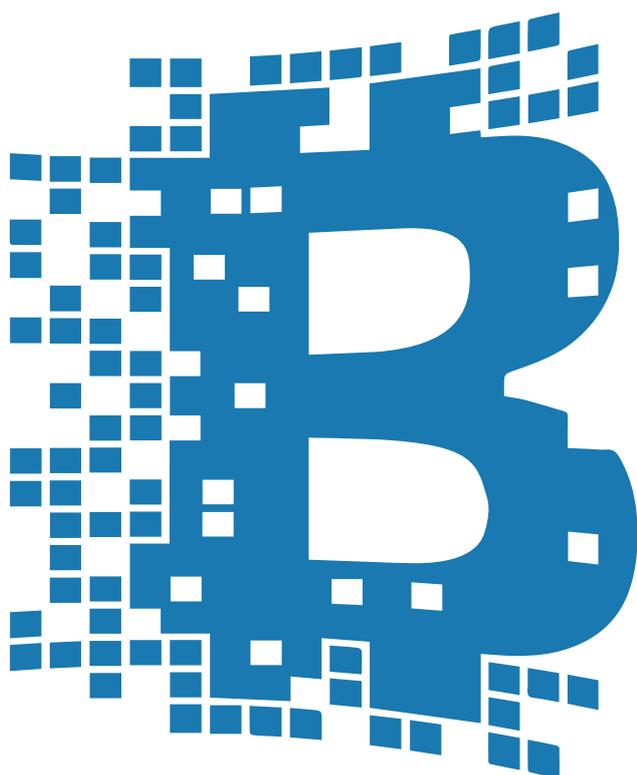
Au coeur de la blockchain, le consortium R3 regroupe un grand nombre d'institutions financières qui demandent à être développées.

02. PRINCIPES DE LA BLOCKCHAIN

Définition

La blockchain est une suite de blocs, chaque bloc est une structure qui regroupe un certain nombre de transactions. Leur création et leur gestion se font par un réseau basé sur le Cloud, distinct, régi par des règles convenues entre ses membres. La Blockchain apporte un registre partagé permettant d'enregistrer la transaction souhaitée et de suivre le mouvement d'un actif de nature tangible (terrain, maison, voiture, liquidités...) ou intangible, à savoir des éléments de propriété intellectuelle (les brevets, les droits d'auteur ou le numérique).

Les transactions dans une Blockchain sont agrégées au sein de blocs digitaux chaînés entre eux. Dans cette structure de données, les transactions validées sont intégrées dans des blocs bénéficiant d'un identifiant « unique » dépendant du contenu. Grâce à une empreinte de hachage, une signature est obtenue. Chaque bloc contient la signature du bloc précédent de la chaîne permettant de garantir l'intégrité de l'ensemble des enregistrements et des données de la Blockchain depuis le premier bloc.



L'architecture Blockchain apporte aux participants la capacité à partager leur registre mis à jour au moyen de répliquations de pair-à-pair, chaque fois qu'une transaction a lieu. La répliquation de pair-à-pair signifie que chaque participant (nœud) du réseau agit à la fois comme un éditeur et comme un abonné. Chaque nœud peut recevoir ou émettre des transactions vers d'autres nœuds. Les données sont synchronisées à l'échelle du réseau lorsque le transfert est effectué. Il est également moins vulnérable puisqu'il utilise des modèles de consensus pour valider les informations. Les transactions sont ainsi sécurisées, authentifiées et vérifiables.

02. PRINCIPES DE LA BLOCKCHAIN

Caractéristiques d'une Blockchain

La base de données constituée est entièrement cryptée et sécurisée. Elle distribue les données au moyen d'une d'organisation, appelée "nœud" ou "mineur". Selon qu'elle est publique, ouverte à tous ou privée, avec accès et utilisation limitée à certains acteurs, la blockchain est partagée entre ses différents utilisateurs, sans aucun intermédiaire. Chacun peut ainsi contrôler la validité d'une information ou d'une inscription dans les blocs de la chaîne ; garant de traçabilité et d'inaltérabilité.

Consensus

Pour qu'une transaction soit valide, tous les participants doivent s'accorder sur sa validité.

Provenance

Les participants savent d'où provient l'actif et de quelle manière ses propriétaires ont changé au fil du temps.

Immuabilité

Aucun participant ne peut falsifier une transaction après qu'elle ait été enregistrée dans le registre.

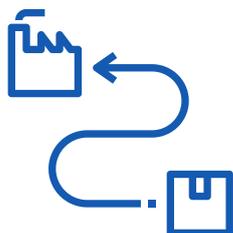
Finalité

Un registre unique et partagé constitue un emplacement auquel chacun se réfère pour déterminer la propriété d'un actif ou la mise en œuvre d'une transaction.

02. PRINCIPES DE LA BLOCKCHAIN

1. IDENTIFICATION

6. TRACABILITÉ

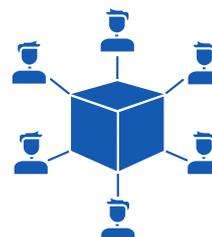


Chaque nouveau bloc ajouté à la blockchain est lié au précédent et une copie est transmise à tous les « nœuds » du réseau.



L'identification de chaque partie s'effectue par un procédé cryptographique.

2. ENVOIE



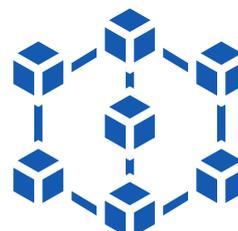
La transaction est envoyée à un réseau (ou « nœud » de stockage) d'ordinateurs situés dans le monde entier.

5. VALIDATION



La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées.

3. NOEUD



Chaque « nœud » héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées.

5. DÉCHIFFRAGE



Les données sont déchiffrées et authentifiées par des « centres de données » ou « mineurs ».

4. CONSENSUS



Le système de sécurisation repose sur un mécanisme de consensus pour tous les « nœuds » à chaque ajout d'informations.

03. TECHNOLOGIE UTILISÉE EN BLOCKCHAIN

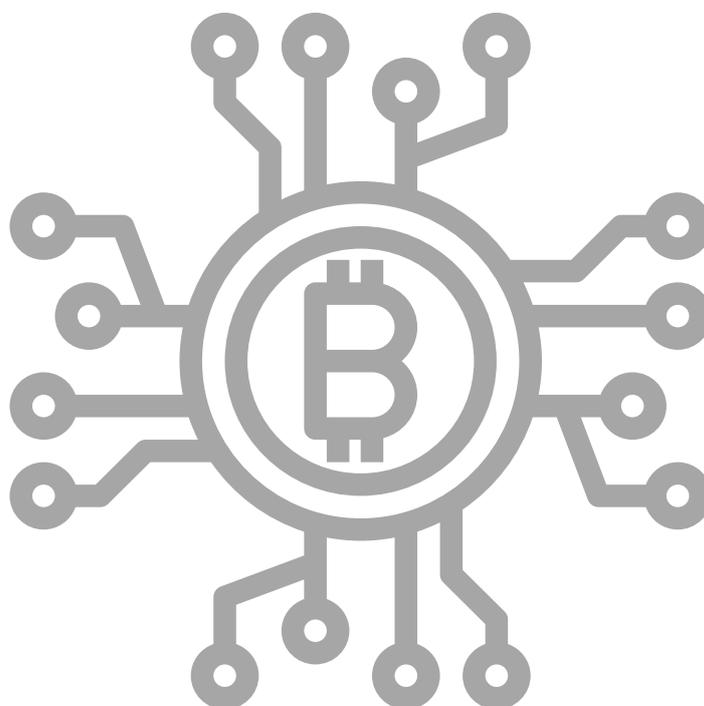
La logique d'une transaction en Blockchain

La blockchain est une technologie des registres distribués, ou DLT (**Distributed Ledger Technology**), qui regroupe les systèmes numériques qui enregistrent des transactions d'actifs et leurs détails dans plusieurs emplacements à la fois.

Pour effectuer une transaction en blockchain, un processus est mis en place. Le point de départ est l'émission de la transaction par une personne "A", ensuite les acteurs de la blockchain reçoivent une copie de ladite transaction pour la vérifier et enfin valider les détails à l'aide des algorithmes de traitement automatique.

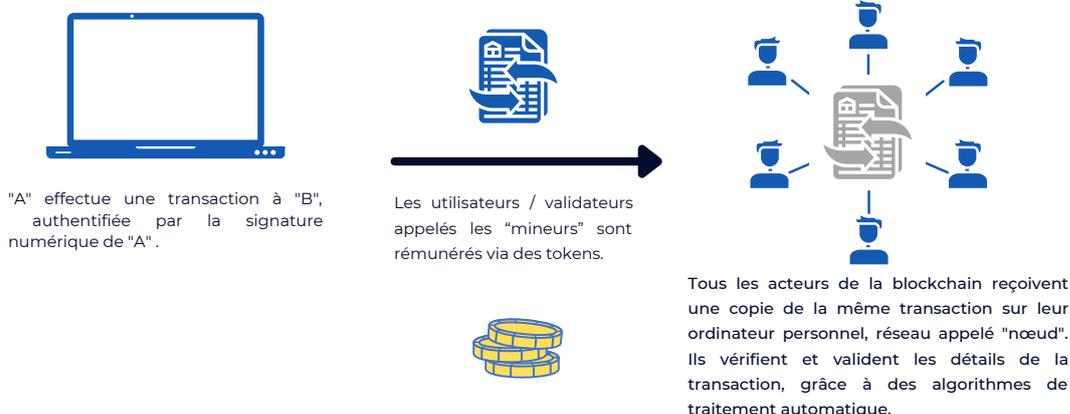
Après validation, les transactions sont regroupées dans des blocs. Chaque bloc porte un "hash" qui atteste de sa validité, c'est l'étape de minage.

Ainsi le nouveau bloc peut s'enchaîner au dernier bloc validé de la chaîne de façon immuable.



La technologie repose sur un système de pair-à-pair décentralisé : les données ne sont pas hébergées par un serveur unique, mais distribuées entre les utilisateurs sans intermédiaire.

03. TECHNOLOGIE UTILISÉE EN BLOCKCHAIN



Étape de minage

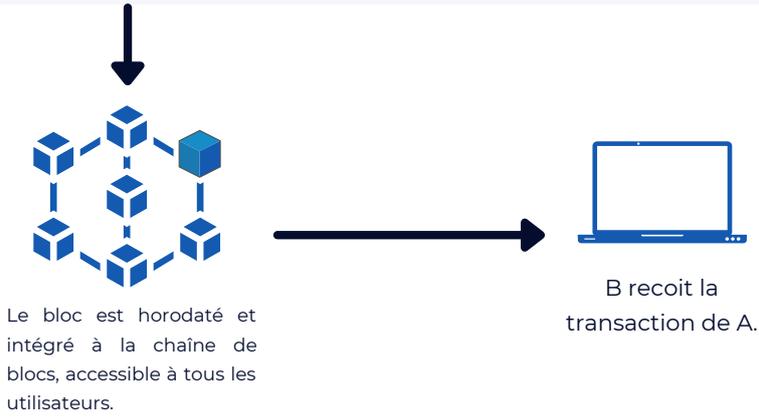
Les transactions, une fois validées, sont regroupées dans des blocs. Ces blocs sont créés par des utilisateurs volontaires de la blockchain. Chaque bloc porte le marquage numérique (un code, appelé hash) issu du bloc précédent de la chaîne qui atteste de sa validité et un hash nouvellement créé. Cette opération (hashage) est réalisée par un algorithme, qui demande du temps et de la puissance de calcul.

Trouver le bon hash

L'objectif du hashage est de trouver le « bon » hash, c'est-à-dire la combinaison valide qui pourra s'enchaîner au dernier hash connu de la chaîne de blocs, à la manière d'un Lego. Tous les mineurs sont en compétition pour trouver le hash « magique ». Le mineur ayant trouvé le bon hash est « récompensé » (paiement en cryptomonnaie par exemple).

MAJ de la blockchain

Le nouveau bloc peut alors s'enchaîner au dernier bloc authentifié de la chaîne de manière immuable. Une fois l'information inscrite dans la blockchain, il est quasi impossible de la modifier ou de la supprimer. La blockchain est alors à jour.



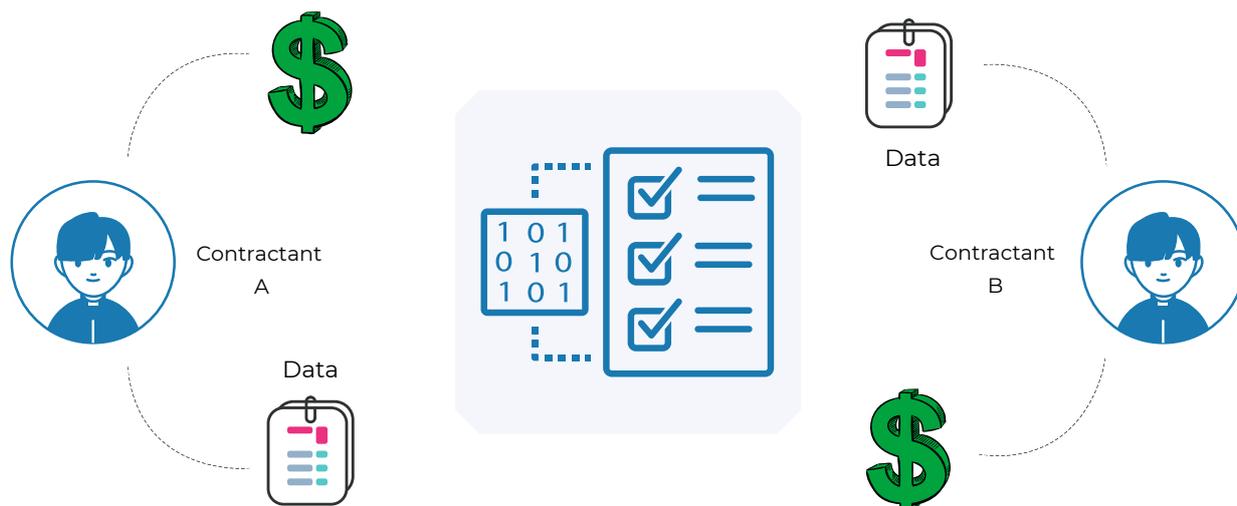
04. SMART CONTRACT

La "smart contract" : un produit prometteur de la Blockchain

L'usage le plus connu de la blockchain est celui des cryptomonnaies. Ces crypto-actifs sont des devises électroniques, virtuelles et chiffrées qui n'ont aucune forme physique. Ces devises s'échangent sur la blockchain, sous contrôle du système informatique et d'un ensemble d'utilisateurs qui le compose. Contrairement à la monnaie réelle, aucune autorité centrale, telle que la banque, ne contrôle les flux.

Un autre usage de la blockchain serait la smart contract ou contrat intelligent. Par sa capacité de chiffrement et par sa maîtrise de la chaîne contractuelle sans la présence d'intermédiaire, la smart contract pourrait révolutionner le secteur financier.

Les « smart contract » et les « oracles » d'éternum pourraient faciliter le processus de contractualisation des assureurs grâce à leur capacité d'exécution automatique des conditions générales d'un contrat. Quant aux oracles, ce sont des entités spécialisées (DAO) ; elles vérifient si les clauses de contrats sont respectées et elles gèrent les données des smart contracts.



- Quel usage pourrions-nous faire de la **smart contract** ?

04. SMART CONTRACT

La "smart contract" : un produit prometteur de la Blockchain

Le contrat intelligent ou le smart contract est un contrat numérique basé sur des programmes informatiques qui enregistrent et exécutent les conditions d'un contrat quand son échéance arrive à terme, leurs caractéristiques étant au préalable clairement définies. Ce type de contrat vient de la fusion de deux procédés techniques, à savoir l'informatisation du contenu contractuel et le recours à la technologie de la chaîne de blocs.

Les contrats intelligents peuvent comporter différentes clauses contractuelles susceptibles d'être, en tout ou en partie, directement applicables et/ou exécutoires de manière automatique. Les termes du contrat (des lignes de code) sont enregistrés sur la Blockchain et exécutés automatiquement : ils ne sont pas modifiables a posteriori (inviolables) mais restent consultables par les parties prenantes. Ils sont appelés des contrats « données-orientées ». Ils sont plus efficaces que les contrats électroniques dans la mesure où un ou plusieurs termes sont exprimés par les contreparties de manière à être lus et exécutés par un ordinateur. Leur finalité est d'apporter une meilleure sécurité et de diminuer les coûts et les délais par rapport aux contrats traditionnels.

Trois Points Clés

1

Un contrat intelligent ou smart contract est un contrat entre deux personnes sous forme de code informatique inscrit sur la blockchain et stocké dans une base de données publiques. Les données du contrat ne sont pas modifiables.

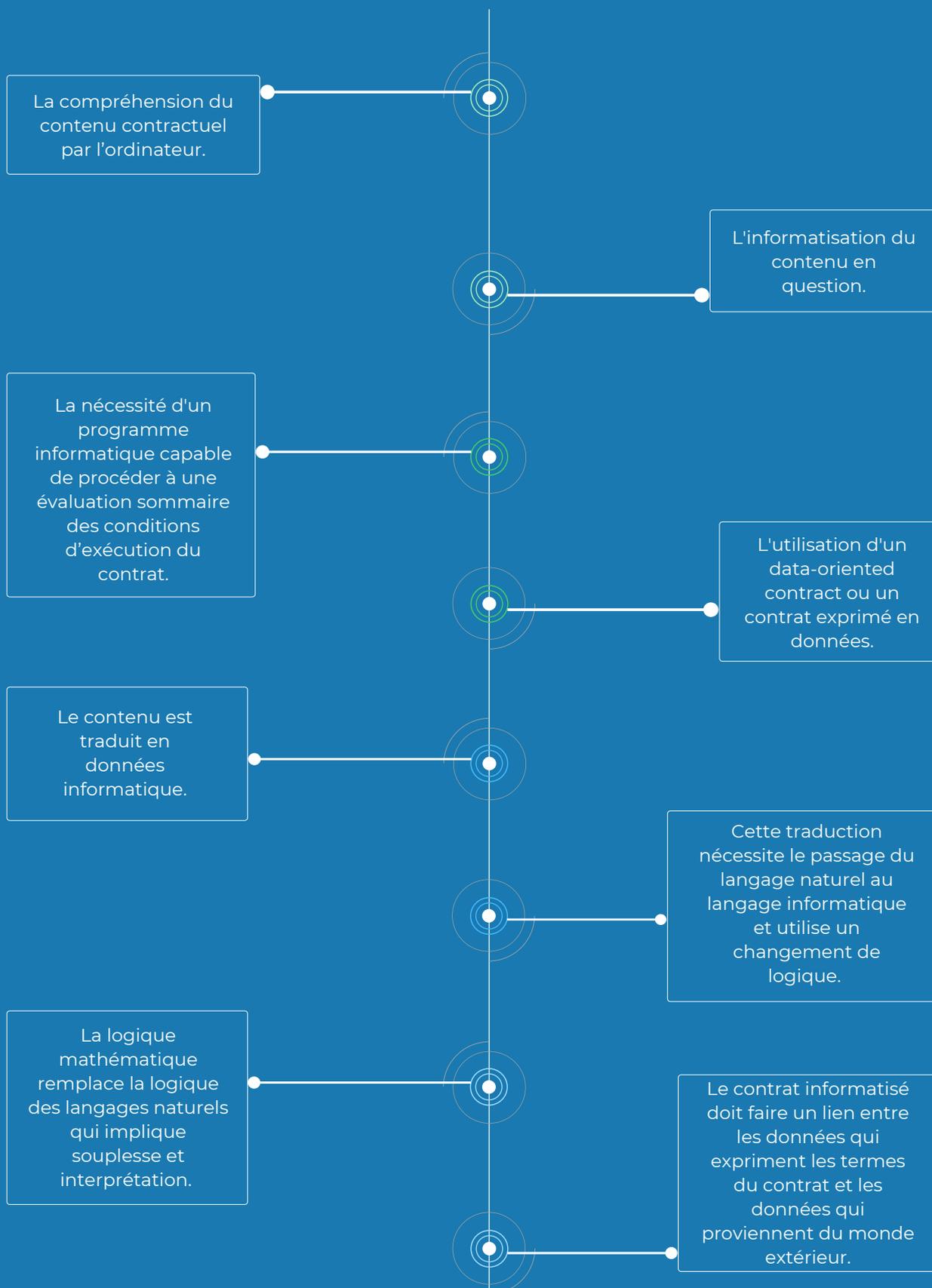
2

L'exécution de plusieurs lignes du code d'un contrat nécessite la rémunération de mineurs. Cette rémunération se fait avec un petit pourcentage des frais appelé, "gas".

3

Les transactions ne se produisent que lorsque les conditions de l'accord sont remplies et vérifiées, il n'y a pas de tiers, ce qui aide à bâtir une confiance totale entre les parties.

04. SMART CONTRACT



05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE

La blockchain peut sembler abstraite sans exemples concrets. Cette technologie donne un nouvel élan grâce à des systèmes d'assurance automatisés fondés sur les smart contracts et les entités appelées "oracles" au niveau des assurances peer to peer. De nombreux projets utilisant des blockchains ont d'ores et déjà vu le jour.

L'exemple souvent cité est celui de l'assurance dite "indicielle" ou "paramétrique", autrement dit l'assurance liée à un indice tel que la température.

Le contrat est alimenté par des données externes fiables qui permettent aux oracles de déclencher automatiquement le paiement après n jours, sans l'intervention d'un expert, sans déclaration nécessaire ou revendication de l'assuré.

Nous avons choisi de présenter un certain nombre de cas d'usage destinés à illustrer le potentiel de cette technologie complexe et à montrer l'étendue de ses possibilités.

Quelques exemples d'assureurs ayant lancé des applications dans l'univers de blockchain :



Développement d'un produit d'assurance sur la base d'un paramètre indépendant, les paiements liés aux sinistres sont déclenchés automatiquement lorsque le seuil convenu est atteint, sans enquête prolongée sur le sinistre.



Développement d'un smart contract en juin 2016. Le « natural catastrophe swap » permet le paiement automatique d'une indemnité à son détenteur en cas de catastrophe naturelle.



En septembre 2016, le Groupe a créé un prototype de compte de réassurance en vue d'évaluer l'opportunité de recourir à la technologie Blockchain dans le cadre du projet Ruschlikon.



Le Crédit Mutuel Arkéa et IBM ont mis en place un écosystème de données afin de favoriser une meilleure connaissance de chaque dossier client pour proposer un service de meilleure qualité.

05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE



AXA Global Parametrics, la filiale du groupe AXA dédiée au développement de l'assurance paramétrique s'est intéressée au sujet de la blockchain. Son approche se base principalement sur l'utilisation d'un modèle d'assurance innovant basé sur les technologies et les méthodes de traitement du Big Data afin d'élargir le champ des éléments assurables. Elle utilise une méthode simple : le produit d'assurance est conçu sur la base d'un paramétrage indépendant. Les paiements liés aux sinistres sont déclenchés automatiquement lorsque le seuil convenu est atteint, sans enquête prolongée sur le sinistre.

Fizzy (2017) est la première assurance française basée sur la Blockchain



AXA a rapidement mis au point un produit utilisant à la fois l'approche paramétrique et la blockchain, modulable et accessible aux particuliers.

L'idée est d'offrir aux voyageurs un produit automatisé dédié aux retards d'avion en se basant sur un smart contract. Il s'appuie sur des données relatives aux retards de vol provenant de tiers et procède immédiatement à l'indemnisation dès l'atterrissage. Ce processus mit fin aux longs questionnaires, aux déclarations de sinistre et aux attentes de paiement. Un an de travail fut établi pour la conception du produit « fizzy » lancé par AXA en septembre 2017 .

Malgré ses avantages, l'offre Fizzy a rencontré un succès limité avec seulement quelques centaines de polices vendues depuis son lancement. Une difficulté de la commercialisation s'est présentée en raison de l'intermédiaire d'entreprises partenaires, comme des compagnies aériennes, des agences de voyages ou encore des opérateurs de carte de paiement.

05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE



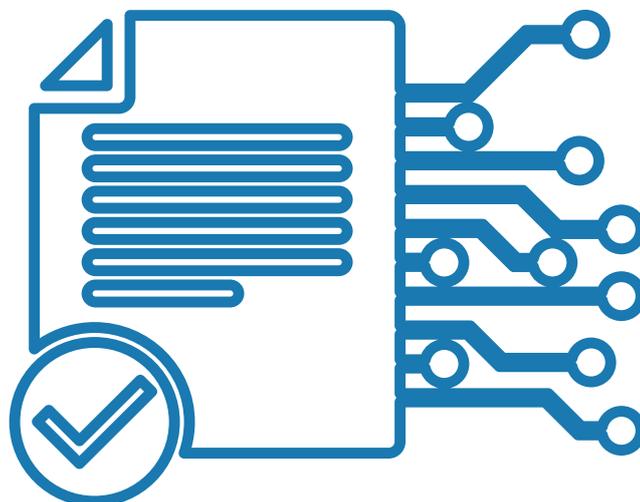
Allianz a annoncé la réalisation d'un smart contract en juin 2016. Le « natural catastrophe swap » permet le paiement automatique d'une indemnité à son détenteur en cas de catastrophe naturelle.

Allianz Risk Transfer et Nephila Capital Ltd. ont utilisé la technologie des contrats intelligents blockchain pour effectuer un échange de catastrophe naturelle.

Les obligations et les swaps de catastrophe transfèrent un ensemble spécifique de risques, y compris les risques de catastrophes naturelles comme les typhons et les ouragans, d'un assureur à d'autres assureurs ou investisseurs.

La technologie de contrat intelligent basée sur la blockchain accélère le processus de gestion des contrats, des obligations et des swaps de chat. Chaque contrat officiel sur l'infrastructure ouverte et partagée contient des données et des codes auto-exécutables inhérents au contrat.

Lorsqu'un événement déclencheur se produit qui remplit les conditions, le contrat intelligent blockchain accède aux sources de données des participants, puis détermine et active les paiements à destination ou en provenance des parties au contrat.



05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE



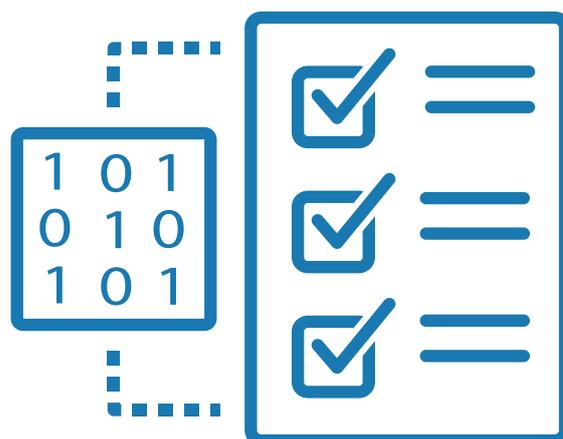
SCOR a mis en œuvre une première application interne de la technologie Blockchain, souple et rapide à mettre en œuvre, qui simplifie et accélère les interactions. Le statut des données est partagé en temps réel par les partenaires commerciaux impliqués et peut contribuer à réduire efficacement les coûts.

C'est une base de données sécurisée, partagée par l'ensemble des participants à une transaction déterminée.

En septembre 2016, le groupe SCOR a créé un prototype de compte de réassurance en vue d'évaluer l'opportunité de recourir à la technologie Blockchain dans le cadre du projet Ruschlikon.

Le projet Ruschlikon rassemble des assureurs, des courtiers et des réassureurs du monde entier. Son objectif consiste à optimiser les coûts administratifs et à améliorer le service aux clients. Le projet Ruschlikon vise à développer l'automatisation des processus administratifs par la mise en œuvre des messages standards ACORD pour les comptes techniques, les déclarations de sinistres et les comptes financiers, parallèlement à l'application des « Bonnes Pratiques » établie par la communauté Ruschlikon.

Le projet rassemble plus de 50 entreprises ; AIG, Aon Benfield, Guy Carpenter, Lloyd's, Munich Re, SCOR, Swiss Re, Willis Towers Watson et XL Catlin composent son comité de pilotage.



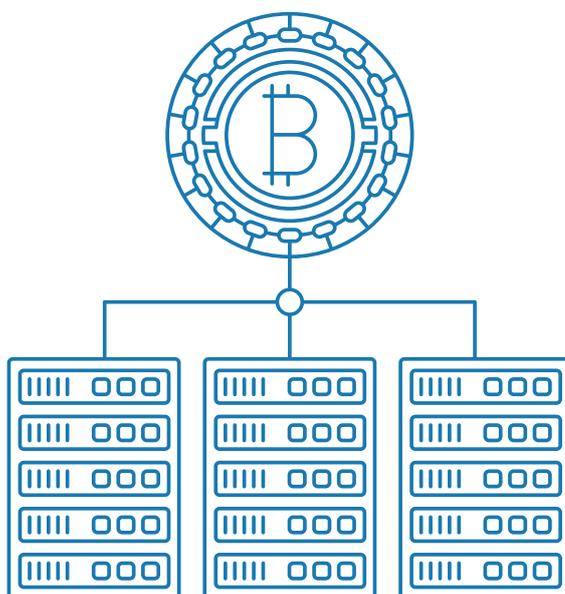
05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE



Le Crédit Mutuel ARKEA et IBM ont mis en place un écosystème de données afin de favoriser une meilleure connaissance de chaque dossier client pour proposer un service de meilleure qualité. Le même registre peut ainsi former une véritable institution assurantielle à partager avec chaque client concerné, afin de renforcer la confiance entre les deux parties et faciliter le partage d'informations clients entre distributeurs, assureurs et réassureurs. En respectant la nouvelle réglementation européenne concernant la protection de données, ce projet devra s'adapter de sorte à être entièrement «RGPD Compliant».

Le Crédit Mutuel Arkea identifie ses clients avec la Blockchain

Le Crédit Mutuel Arkea a démarré un test avec IBM pour développer un réseau opérationnel. Celui-ci devait permettre aux équipes, avec les bonnes permissions, d'afficher les informations identitaires des clients qui suivent le processus KYC. L'objectif du projet est d'améliorer la satisfaction des nouveaux clients en éliminant les longues procédures de souscriptions aux produits de la marque.



05. CAS D'USAGE DE LA BLOCKCHAIN EN ASSURANCE

Smart-Property

La Blockchain révolutionne les contrats grâce à la Smart-Property qui permet d'assigner et transférer la propriété d'un bien immatériel dans le cas d'un titre de propriété ou d'une part d'actif financier, ou physique. C'est ainsi que le principe de token immobilier fut inventé pour permettre la désignation d'un seul détenteur d'une partie de la propriété.

Assurance vie

Une blockchain peut également être utilisée pour faciliter l'efficacité de la conformité d'une loi. Afin de répondre aux obligations de la loi Ekert qui impose aux assureurs de distribuer les sommes conservées des contrats d'assurance vie en déshérence aux ayants droits, les assureurs utilisent désormais de manière expérimentale un système d'oracles pour vérifier le décès des assurés à fréquence régulière. Chaque décès donne lieu à une indemnisation automatique des bénéficiaires du contrat.

Le Smart Contract

POUR L'ASSURANCE HABITATION

Le Smart Contract pourra également être utilisé dans certains aspects de l'assurance habitation grâce au développement des capteurs et autres objets connectés dans les domiciles, ce que nous appelons "maisons connectées". Par exemple, dans le cas de ruptures de canalisation ou de pertes d'aliments congelés dues à une coupure de courant ou à une panne d'appareil. Dans ces cas de figures, l'information serait directement envoyée depuis le capteur au Smart Contrat, ce qui générerait un remboursement automatique.

Voitures connectées

Avec le développement des véhicules connectés, dans la filière automobile, un nombre exponentiel de données vont être collectées : usure des équipements, habitudes du conducteur, historique des anciens propriétaires, ... etc.

Le stockage de toutes ces données personnelles au sein d'une Blockchain permettra un suivi fiable et infalsifiable du véhicule connecté, tout en protégeant la vie privée du conducteur selon les normes de la RGDP.

L'idée derrière est de créer une fiche numérique du véhicule connecté, stockée dans une plateforme de données cryptées et certifiées afin de les exploiter commercialement pour donner naissance à des contrats sur mesure.

L'ensemble des données à disposition permettra de calculer de façon très précise la sinistralité potentielle du conducteur et du véhicule, grâce à l'échange de nombreuses informations en temps réel.



06. CONCLUSION

L'intérêt porté à la blockchain grandit de jour en jour, surtout avec l'envolée des prix des cryptomonnaies et les hauts niveaux de rentabilité constatés sur les marchés financiers. Preuve de l'intérêt croissant pour cette technologie : la dernière initiative en date baptisée « B3i » impliquant cinq grands assureurs et réassureurs européens. Le néerlandais Aegon, les allemands Allianz et Munich Re, ainsi que les suisses Swiss Re et Zurich se sont alliés pour étudier « si la Blockchain pouvait être utilisée pour développer des standards et des processus » pour un usage dans tout le secteur et « catalyser des gains d'efficacité ».

Parmi ceux qui n'ont pas encore réalisé des partenariats, nombreux sont ceux qui ont entamé des réflexions. Cependant, il faut noter que les assureurs travaillent sur ce sujet depuis début 2016.

Des initiatives sérieuses et concrètes commencent à émerger, notamment la Société Générale Assurances et le Groupe Covéa qui viennent de s'allier à « The Blockchain Groupe ». Ils rejoignent le consortium fondé en 2020. L'idée est d'avoir un pass sécurisé par les NFTs qui permettra la visualisation et la certification d'un véhicule dans la filière automobile.

Projection et espérance veillent sur cette nouvelle technologie croissante et exponentielle. Le volet réglementaire semble à date moins impliqué dans la standardisation des normes qui devra encadrer ses technologies.

Plusieurs problématiques émergent :

- Dans quelle limite les difficultés juridiques ou techniques retardent l'apparition de projets Blockchain pour les assureurs ?
- Comment la Blockchain sera un facteur non négligeable dans la concurrence entre les assureurs et les réassureurs ?

07. ANNEXES

Une transaction : Structure de données qui encode le transfert des valeurs (tokens) entre les utilisateurs de la blockchain.

Le pair-à-pair ou peer-to-peer : Modèle de réseau informatique d'égal à égal entre ordinateurs qui distribue et reçoit des données ou des fichiers. Le P2P facilite et accélère les échanges entre plusieurs ordinateurs au sein d'un réseau.

Hash : Fonction qui permet d'obtenir une empreinte numérique unique par fichier.

Mineur : Intervenant actif du réseau qui sélectionne des transactions et participe à leur validation.

Utilisateur de la Blockchain : Participant possédant les autorisations nécessaires pour rejoindre le réseau et effectuer des transactions avec d'autres participants.

Développeur Blockchain : Programmeur chargé de créer les applications et les contrats intelligents qui permettent aux utilisateurs Blockchain d'effectuer des transactions sur le réseau. Les applications servent de lien entre les utilisateurs et la Blockchain.

Le consortium R3 : Consortium qui regroupe plusieurs banques et établissements financiers dont le principal but est de développer des applications commerciales pour le secteur financier.

Consensus : Il garantit la validation des transactions avant leur introduction dans la chaîne ; la Blockchain possédant une forte résistance aux tentatives de falsification.

A propos de iConcilio

iConcilio fait référence à un cabinet de conseil indépendant, société de droit français. Pour en savoir plus sur notre structure, consulter www.iconcilio.com/about.

iConcilio fournit des services professionnels dans les domaines du consulting et du financial advisory à ses clients des secteurs public et privé, quel que soit leur domaine d'activité. Notre équipe s'engage à fournir un service de grande qualité afin d'aider nos clients à répondre à leurs enjeux les plus complexes.

Nous mobilisons un ensemble de compétences diversifiées pour répondre aux enjeux de nos clients avec engagement et efficience. Nous intervenons dans les domaines d'assurance en actuariat et gestion des risques, management de projet, nouvelles technologies et veilles réglementaires.

© 2022 ICONCILIO SASU .



EL AIDOUNI
AMINE
ICONCILIO Founder

Actuaire, membre certifié de l'IA et ancien senior consultant du cabinet Deloitte. Il dispose de 7 années d'expérience en conseil auprès des assurances. Il a acquis des connaissances solides en matière d'audit et de conseil en stratégie.



+33 6 65 40 48 98
revue@iconcilio.com



<http://www.iconcilio.com/home>



<https://www.linkedin.com/company/iconcilio-corporate>