

[DOSSIER] LA BLOCKCHAIN : FUTUR TIERS DE CONFIANCE ? – LES UTILISATIONS POSSIBLES DE LA BLOCKCHAIN EN ASSURANCE

Nouvelles technologies, Entretien

La blockchain ne cesse d'intriguer et de fasciner. Le Government Office for Science britannique publiait en début d'année un [rapport](#) officiel sur la technologie afin d'en analyser les potentielles applications. Les assurances s'y intéressent également, à l'instar du groupe ALLIANZ, qui a [intégré](#) Everledger, une start-up blockchain, à son accélérateur.

Cette deuxième partie du dossier a pour objectif de décrire les applications possibles de la technologie blockchain au secteur de l'assurance. Elle fait suite à la [première partie](#) qui décrivait les principes de base de la technologie.

A l'occasion de cette seconde partie du dossier, nous avons le plaisir de coopérer avec les fondateurs de [Blockchain France](#), qui répondent à nos questions afin d'amener un éclairage supplémentaire sur le sujet.

Blockchain et smart contracts

Les smart contracts (ou « contrats intelligents ») sont des programmes informatiques qui permettent d'exécuter automatiquement les conditions et termes d'un contrat sans aucune intervention humaine.

Prenons un exemple simple : le testament. Vous souhaitez léguer une somme financière à votre conjoint lors de votre décès. Il vous suffit de définir les termes du contrat (montant, nom du destinataire, ...) et, lors de votre décès, le smart contract déclenchera automatiquement la transaction qui pourra être

enregistrée sur la blockchain.

Un tel procédé implique de définir deux nouvelles notions.



Tout d'abord, nous avons développé dans notre premier article la notion de blockchain en matière de transactions.

Il faut savoir que la blockchain peut techniquement enregistrer **n'importe quelle information**, telle que l'identité d'une personne, mais aussi des brevets, des données médicales, voire même votre [ADN](#).

De plus, de nouvelles entités spécialisées opérant avec la blockchain permettent de s'assurer que les conditions d'un contrat sont réalisées afin de déclencher le smart contract : ce sont les oracles. Dans l'exemple évoqué précédemment, ce sont eux qui vont confirmer que le décès a bien eu lieu, en consultant un registre des décès par exemple (le [RNIPP](#) en France).

L'exemple du testament n'est qu'un exemple parmi d'autres. Les applications des smart contracts à l'assurance pourraient être nombreuses : débloquer des fonds en cas d'hospitalisation, se faire rembourser un billet de train en cas de retard important, indemniser automatiquement un agriculteur qui ferait face à une période de sécheresse prolongée, etc.

Blockchain France décrit dans un [article](#) les avantages des smart contracts de la manière suivante :

*« Ces mécanismes promettent des changements majeurs pour les systèmes d'assurance actuels. En automatisant l'exécution des contrats, **ils permettent aux assurés comme aux assureurs de s'émanciper des phases déclaratives** : formulaires, réclamation, vérification, déclenchement de l'indemnisation... La blockchain, en faisant office de tiers de confiance automatisé, ouvre la*

voie à une diminution des coûts de structure tout en fiabilisant et en accélérant les processus de décision. À terme, cela générerait surtout une plus grande satisfaction des assurés via la mise en place de nouveaux services plus intuitifs et plus rapides.

Il aurait certes été techniquement possible de créer ces processus sans blockchain. Le véritable apport de la technologie blockchain consiste ici à générer la confiance et la sécurité nécessaires pour automatiser les phases déclaratives sans avoir recours à un tiers. Si par le passé les assureurs n'ont pas mis en place ce type de produits, la blockchain apporte aujourd'hui une solution qui pourrait permettre à de nouveaux acteurs de pénétrer ce marché. »



Plus largement, le système bancaire pourrait également profiter des smart contracts. La blockchain et les smart contracts pouvant faciliter grand nombre de transactions financières, plusieurs rapports soulignent son intérêt potentiel dans le règlement automatisé de dividendes ou de coupons par exemple. Un tel fonctionnement permettrait également une réconciliation plus simple des informations qui seraient sauvegardées dans un unique registre distribué. En rationalisant et en sécurisant les processus métiers, la blockchain et les smart contracts permettraient aux banques de réaliser une réduction des coûts conséquente.

Pouvez-vous nous présenter Blockchain France ?

BF : Blockchain France est à la fois un média sur la blockchain (production de contenu pédagogique sur notre site), une entreprise qui propose des formations sur la blockchain, et une association qui va prochainement

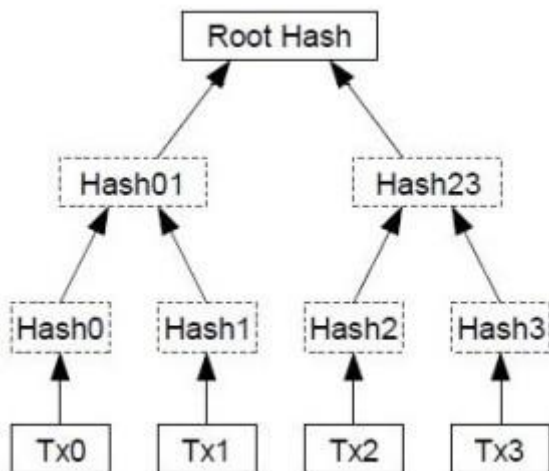
devenir un think tank.

Son objectif est de faire connaître le potentiel de la blockchain et ses enjeux à la fois technologiques, business et éthiques, et de contribuer au développement de l'écosystème blockchain en France. Le 14 janvier dernier, l'équipe de Blockchain France, composée de quatre entrepreneurs d'ESCP Europe, a ainsi organisé la première grande conférence en France sur le sujet, sous le Haut Patronage du Ministère de l'Economie. De façon plus générale, Blockchain France cherche à expliquer avec pédagogie les ressorts du "phénomène blockchain", sans parti pris et sans en occulter les limites, au travers de plusieurs initiatives : formations aux entreprises, "master class" grand public, organisation ou participation à des événements autour de la blockchain.

La blockchain peut techniquement enregistrer n'importe quel type de données. Etant donné que ce ne sont pas des transactions, comment ces informations sont-elles enregistrées sur la blockchain ?

BF : Les informations (comme un document pdf) sont mises sous forme de "hash" (une série de lettres et de chiffres) via un algorithme (par exemple le SHA 256). Ce hash fait ensuite partie des métadonnées d'une transaction.

Il est possible de faire des "hash de hash" et ainsi de certifier de nombreuses informations différentes en une seule transaction (voir [arbre de Merkle](#)).



Exemple simplifié d'arbre de Merkle

Les smart contracts sont-ils hébergés par la blockchain ? Passent-ils par une phase de minage pour être inscrits dans un bloc ?

BF : Les smart contracts ne sont pas à proprement parler des transactions. En général, il y a 2 types de comptes : des comptes détenus par des tiers (vous, moi), contrôlés par des clés privées, et des comptes de contrats, contrôlés par leur code, qui sont créés lors de la rédaction du contrat. Un compte de tiers n'a pas de code et ne peut effectuer des transactions qu'en les signant avec sa clé. Pour les comptes de contrat, à chaque fois que ce compte reçoit un message, son code s'active, et il réalise ses fonctions (envoi de transactions, création de nouveaux contrats, etc.). Seul l'état du contrat est stocké sur la blockchain, c'est-à-dire l'historique de transactions qui est le témoin de l'exécution (ou de l'inexécution) de celui-ci.

Si un smart contract implique une transaction financière (testament par exemple), le montant de la transaction est-il placé dans un compte neutre en attendant l'exécution des termes du contrat ?

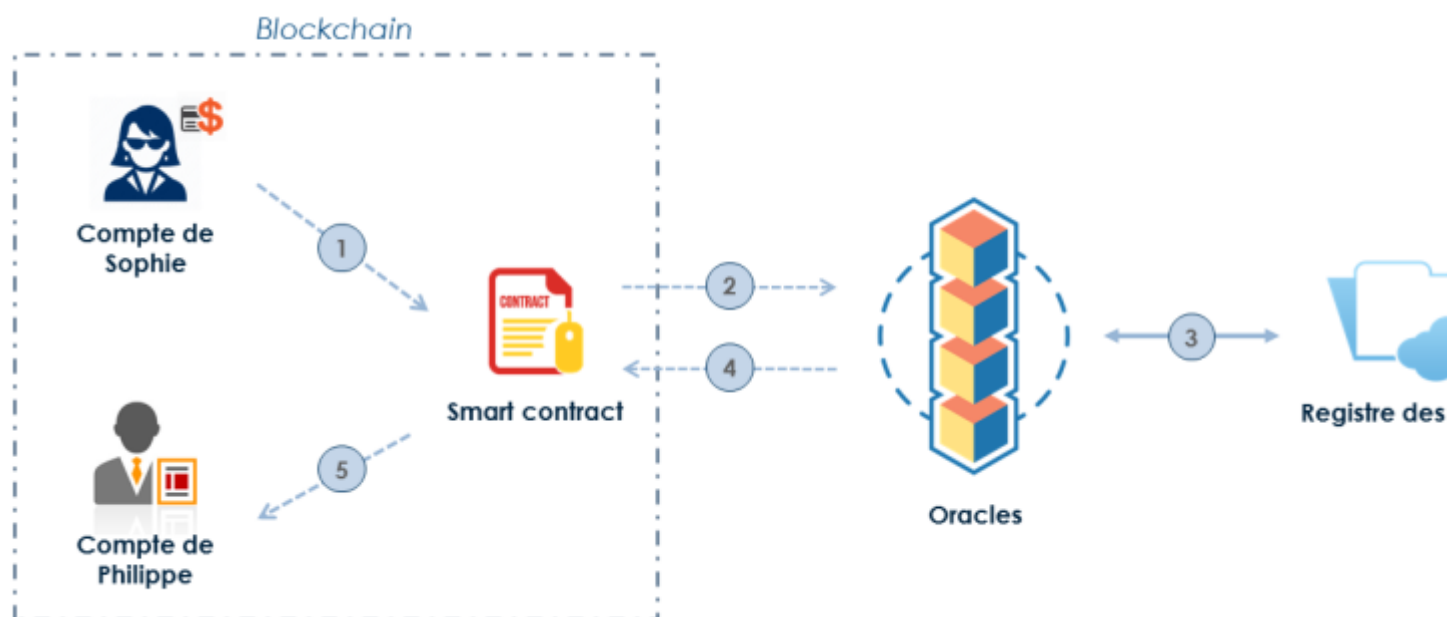
BF : Les cas sont multiples ; dans le cas d'un testament,

je n'aurais pas envie que l'argent soit bloqué sur un compte pendant X années. Selon ce qu'on écrit dans le contrat et selon les autorisations d'accès aux différents comptes, on peut imaginer un contrat qui, une fois mon décès certifié, dispose de l'accès à mon compte, et répartisse l'héritage selon mon testament

Pourquoi utiliser les oracles plutôt que la blockchain seule ?

BF : Les oracles permettent de faire des choses que la blockchain ne permet pas : ils peuvent puiser de l'information des réseaux sociaux ou de n'importe quelle base de données à laquelle ils sont reliés, et ainsi intégrer certains éléments déclencheurs des smart contracts au sein de la blockchain. Ils sont externes à la blockchain, mais ils y sont tout de même reliés.

Voici un schéma simplifié du fonctionnement dans le cas d'un testament :



Sophie crée un contrat qui doit transférer 100€ à Philippe si elle décède.

Le smart contract transfère les conditions du

contrat aux oracles.

Les oracles consultent une liste des décès dans la base de données du [RNIPP](#).

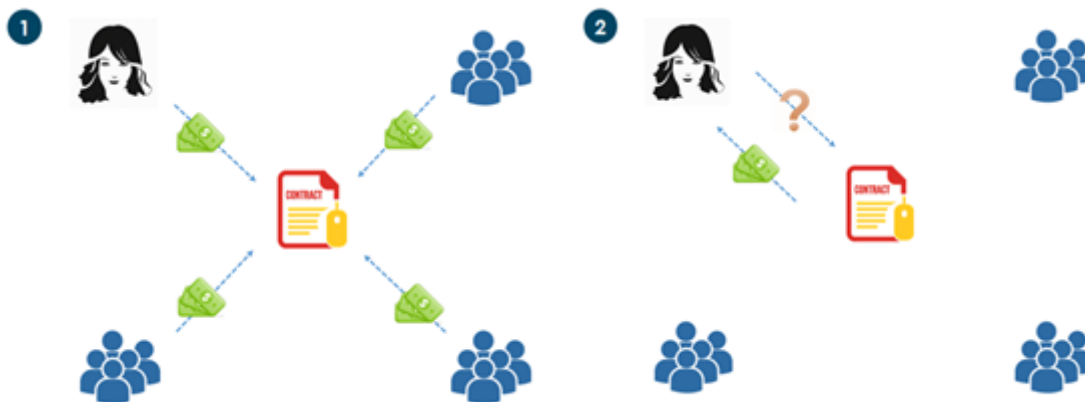
Si le décès de Sophie est confirmé, les oracles génèrent une transaction sur laquelle ils apposent leur signature et la transmettent au smart contract.

La transaction est soumise aux mineurs pour validation puis inscrite dans la blockchain, confirmant ainsi le transfert à Philippe.

Les organisations décentralisées autonomes

Les organisations décentralisées autonomes (DAO en anglais) sont des entités opérant de manière autonome dans la blockchain.

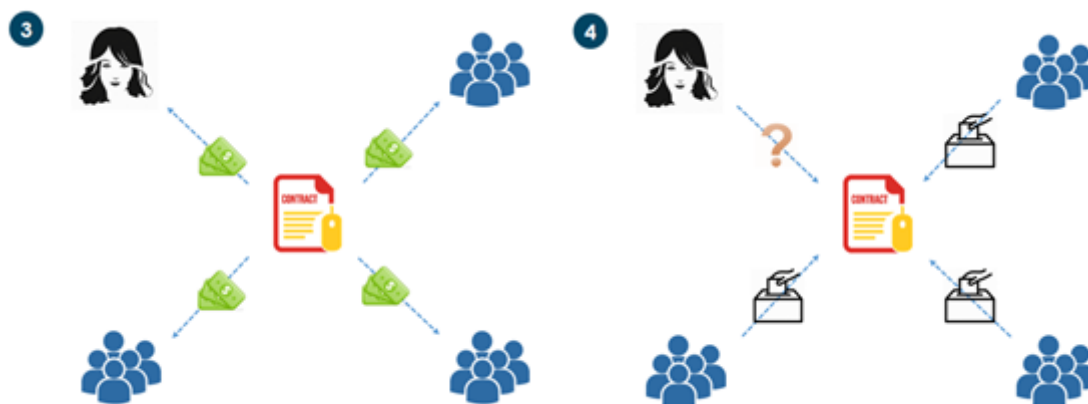
Prenons un exemple concret. Blockchain et smart contracts pourraient permettre de mettre en place une organisation décentralisée autonome qui ferait figure d'assurance peer-to-peer. Concrètement, voici comment cela pourrait fonctionner :



Tous les individus qui souhaitent être assurés sont prélevés d'un montant mensuel qui est défini dans le code du smart contract

Cécile a un accident et a besoin d'être indemnisée pour pouvoir réparer sa voiture. On peut imaginer deux procédés possibles : soit le smart

contract est capable de s'assurer que Cécile a bien eu un accident (en s'appuyant sur des oracles par exemple) et peut l'indemniser, soit l'indemnisation de Cécile est soumise au vote des assurés qui décident si oui ou non celle-ci est justifiée.



3. À la fin de l'année, le capital qui n'a pas été utilisé est automatiquement redistribué aux assurés

4. Cécile considère que le montant qui est prélevé mensuellement est trop élevé. Elle propose au réseau de diminuer la cotisation mensuelle. Chacun des assurés dispose d'une voix pour voter. Si la majorité accepte la proposition de Cécile, le smart contract adapte alors son code pour prélever une cotisation mensuelle moins élevée.

Cet exemple d'assurance peer-to-peer illustre parfaitement l'avantage majeur de la blockchain : générer de la confiance, être une « trust machine », comme la décrit [The Economist](#), qui ouvre la voie vers des applications au potentiel incommensurable. On peut néanmoins présager que les organisations décentralisées autonomes ne se mettront pas en place du jour au lendemain, mais plutôt qu'elles représenteront le dernier stade d'évolution d'organisations décentralisées. Qu'en est-il de l'assureur ? L'exemple précédent ne le cite

pas à un seul moment et pourrait presque faire croire à sa disparition. Les assurances n'en demeurent pas moins des experts en gestion du risque. Elles disposent d'une expérience et de données qui leur permettent d'apprécier les niveaux de risques, les besoins en capital, etc. La blockchain et les smart contracts n'annoncent donc pas une mort de l'assureur, mais plutôt une évolution de son rôle, de gestionnaire du risque à conseiller en gestion du risque.

Le principe de fonctionnement autonome et décentralisé est parfaitement compréhensible dans l'exemple de l'assurance peer-to-peer. En revanche, comment les assurés accèderaient-ils au service ? Une interface/un portail web est requis et doit nécessairement être contrôlé par quelqu'un. Cela n'est-il pas contradictoire au principe de décentralisation et d'autonomie ?

BF : C'est exact, les assurés doivent nécessairement pouvoir accéder au service via une interface web. A priori, ce rôle resterait cependant relativement faible, puisqu'une partie de la gestion de l'interface pourrait être assurée par les DAO eux-mêmes. On peut également très bien imaginer un scénario dans lequel ce sont certains assurés qui assument ce rôle de gestion de l'interface (leur rôle serait alors plus comparable à celui de délégués ou d'un syndic de copropriété qu'à celui d'un véritable "intermédiaire").

Dans tous les cas, le fait que l'interface web soit "gérée" par un tiers ne veut pas dire que le service est "contrôlé" par ce tiers. L'interface web n'est qu'une vitrine ; il n'est pas le cœur de la machine. Le véritable contrôle est celui du code source de la blockchain, de la validation des transactions, et du code des smart contracts.

Comment imaginez-vous l'évolution des compagnies d'assurance si de telles organisations venaient à se mettre en place ? Doit-on s'attendre à une diminution importante de leurs bénéfices ?

BF : Si ce genre de services venait à être proposé par de nouveaux acteurs, il est probable que les grandes sociétés d'assurance aient du souci à se faire, car cela concurrencerait directement certains de leurs produits. Mais il est également possible que ces sociétés s'adaptent et intègrent ce genre de services à leurs offres, moyennant une restructuration interne (un peu sur le même schéma que les grandes banques avec l'intégration des banques en ligne, par exemple).

Notons également qu'aujourd'hui, certains types d'assurances (les assurances dites "obligatoires" comme les assurances automobile ou de responsabilité civile) sont réglementés, et qu'en conséquence, de telles assurances gérées par un DAO n'ont aucune valeur juridique (à moins que le DAO ne soit labellisé par une structure juridique qui réponde aux exigences légales du monde des assurances). Outre les problématiques techniques, il faudra donc aussi attendre l'adaptation de notre système législatif pour que les DAO puissent devenir "mainstream" et bouleverser vraiment le secteur de l'assurance.

L'ÉQUIPE BLOCKCHAIN FRANCE:

Fondateurs :



Claire Balva



Clément Jeanneau



Alexandre
Stachtchenko



Antoine Yeretizian

Dossier publié par InsuranceSpeaker, le 29/03/2016

Lien : <https://www.insurancespeaker-wavestone.com/2016/03/dossier-blockchain-futur-tiers-de-confiance-utilisations-possibles-de-blockchain-assurance/>