UCLouvain

LOUVAIN
School of Management

Louvain School of Management

La Blockchain : quel avenir pour le secteur de l'assurance belge et européen ?

Auteur : Marian Felis
Promoteur : Pierre Devolder
Année académique 2021 - 2022
Travail de fin d'études (TFE) en vue d'obtenir le titre d'
Ingénieur de gestion à finalité spécialisée
Horaire de jour

Le sujet du mémoire, à la fois original et innovant, m'a permis de découvrir le fonctionnement de la technologie de la blockchain ainsi que certains aspects du secteur de l'assurance. Je tiens donc à remercier mon promoteur, M. Pierre Devolder, pour la confiance accordée lors du choix et de la rédaction de celui-ci.

J'aimerais également remercier M. Denys Bornauw et M. Guillaume Braibant qui m'ont tous deux accompagné dans la compréhension de la technologie et dans la mise en œuvre du PoC.

Ensuite, je souhaiterais remercier tous mes interlocuteurs et, plus particulièrement, M. Patrick Sergysels, Mme Patricia Boydens, M. Koen Vingerhoets ainsi que M. Tobias Ambühl qui ont partagé leurs expériences personnelles et m'ont permis de mettre mes résultats en perspective.

Finalement, je remercie ma famille et mes amis qui m'ont accordé un soutien inconditionnel depuis le choix du sujet jusqu'à la relecture du mémoire.

Table des matières

Table des matières I

INTRODUCTION 1

PARTIE I : LA BLOCKCHAIN 3

1. Qu'est-ce que la technologie de la blockchain ? 3

1.1. Quelle est la genèse de la blockchain ? 3

1.2. Qu'est-ce qu'un bloc ? 7

1.3. Qu'est-ce que la chaine ? 11

1.4. La blockchain est un registre d'informations distribué 12

1.5. Les différents types de consensus 14

1.6. Les différents types de blockchains 18

1.7. La cryptographie 19

1.8. Le bitcoin en guise d'illustration du fonctionnement de la technologie 22

2. Les atouts/forces de la technologie blockchain 26

2.1. La blockchain comme registre distribué 27

2.2. La blockchain supprime les intermédiaires 28

2.3. La blockchain permet la tokenisation 30

2.4. La blockchain comme nouvelle économie numérique décentralisée 31

3. Les faiblesses de la technologie 31

3.1. La blockchain, une technologie nouvelle et complexe 31

3.2. La blockchain, une technologie inefficiente 33

3.3. La blockchain, une technologie volumineuse 34

3.4. La blockchain, une technologie qui présente des risques de cybersécurité 34

3.5. La blockchain, une technologie qui pose des questions juridiques 36

PARTIE II : LA BLOCKCHAIN DANS LE SECTEUR DE L'ASSURANCE 39

1. Etat des lieux du secteur de l'assurance en Belgique et en Europe 39

2. Quelques domaines d'application de la technologie blockchain appliquée au secteur de l'assurance 42

2.1. Réduction des coûts et optimisation de la gestion 43

2.2. Création de nouveaux produits 54

2.3. Réassurance 57

3. Proof of Concept 61

3.1. Objectif du PoC 61

3.2. Les difficultés rencontrées dans la souscription traditionnelle d'un contrat d'assurance 61

3.3. Insurme : une nouvelle façon de souscrire à un contrat d'assurance 62

4. Enquête 67
CONCLUSION..... 71
ANNEXES..... 74
1. Méthodologie utilisée pour la création du PoC..... 74
2. Fonctionnalités de l'application 75
3. Fonctionnement et exigences des fonctionnalités..... 77
4. Démonstration 80
5. Outils d'évaluation de compatibilité entre un projet et la technologie blockchain..... 92
6. Interviews 94
BIBLIOGRAPHIE 103

INTRODUCTION

Le Bitcoin, les cryptomonnaies, les NFTs, ces termes ne vous sont certainement pas inconnus. Nous entendons quotidiennement parler de ces nouvelles technologies, plébiscitées par certains et décriées par d'autres. Quoiqu'il en soit, selon CoinMarketCap (2022), la valeur de marché mondiale des cryptomonnaies s'élevait, fin juillet 2022, à près de 1100 milliards d'euros, soit plus de deux fois le PIB belge.

Ces innovations ont un point commun, elles sont mises en œuvre via la technologie de la blockchain. Cette technologie dispose, selon certains, du potentiel pour révolutionner le monde digital de demain.

Le monde de la finance s'y intéresse d'ores et déjà. La Banque Européenne d'Investissements a lancé sa 1ère émission obligataire via la blockchain Ethereum en 2021.

Assez logiquement, nous nous sommes donc posé la question de savoir si cette technologie avait des applications actuelles ou potentielles dans le secteur de l'assurance.

La première partie du mémoire est consacrée à une approche théorique du fonctionnement de la technologie. Nous y développerons des concepts tels que les blocs d'information, la chaine de blocs, les fonctions de cryptage et de hachage ainsi que les protocoles de validation appelés consensus.

Au sein de cette même partie, nous identifierons les principaux atouts de cette nouvelle technologie. Nous verrons comment la mise en œuvre d'un registre distribué permet la création d'un écosystème collaboratif duquel résulte une désintermédiation, une automatisation des processus et, par conséquent, une réduction des coûts.

Nous y analyserons également les faiblesses de cette nouvelle technologie. La blockchain de type publique et ouverte est maintes fois décriée pour la consommation énergétique qui résulte de son processus de validation. Nous verrons que des solutions existent pour y répondre.

La technologie étant relativement récente, elle est perçue comme complexe et le nombre de personnes qui la maitrise reste insuffisant pour espérer un développement significatif à court terme.

Finalement, nous évoquerons les risques juridiques et cybernétiques qui sont inhérents à toute nouvelle technologie.

La deuxième partie du mémoire a pour objet de déterminer si et comment cette technologie pourrait être appliquée dans le secteur de l'assurance. Nous débuterons cette section en faisant un état des lieux du secteur.

Au travers d'exemples pratiques ou d'analyses prospectives, nous illustrerons comment les avantages décrits dans la partie 1 sont susceptibles d'être mis en application. En particulier, nous nous intéresserons à l'optimisation de la gestion et à la réduction des coûts, à la création de nouveaux produits rendus possible par la technologie et aux applications existantes ou en développement dans le secteur de la réassurance.

Pour démontrer que la technologie est fonctionnelle, nous avons réalisé un « proof of concept ». Nous avons conçu une application d'appel d'offres et de souscription d'un contrat d'assurance de responsabilité civile familiale en ayant recours à la technologie Ethereum. Une vidéo en ligne permet de visualiser son fonctionnement.

Enfin, au sein de la rubrique intitulée enquête, nous résumerons les échanges que nous avons eus avec des acteurs du secteur de l'assurance ou de la consultance blockchain. Ils nous aideront à mettre le sujet en perspective et à identifier à quel stade la technologie se trouve actuellement en Europe.

Nous conclurons ce mémoire en répondant à la question suivante : « la technologie de la blockchain est-elle suffisamment mature pour envisager des applications concrètes à court terme dans le secteur de l'assurance belge et/ou européen? ».

PARTIE I : LA BLOCKCHAIN

1. Qu'est-ce que la technologie de la blockchain ?

Pour introduire le concept technique qu'est la blockchain, nous pouvons formuler une analogie simpliste.

La blockchain pourrait être comparée à un grand livre d'informations. Tout comme un livre est composé de nombreuses pages reliées entre elles, la blockchain est composée d'un ensemble de blocs reliés entre eux.

Ce livre ne serait pas rédigé par un seul auteur mais par plusieurs auteurs rassemblés dans une salle. Ce public d'auteurs contemplerait une scène où des intervenants viendraient tour à tour lire leur phrase. Chacun des auteurs rédigerait sa version du livre, phrase après phrase. Ils conserveraient ainsi une version du livre.

Au terme de chaque page, les auteurs compareraient leur version respective. Si plus de 50% des auteurs présentaient une version identique, cette version serait retenue comme étant la version officielle. Les auteurs ne disposant pas de cette version, s'aligneraient dès lors sur celle-ci qui serait rajoutée à la copie du livre de chacun *(Bennett & Decker, 2020).*

Cette analogie permet de comprendre le fonctionnement simplifié d'une blockchain. Au sein de la première partie du mémoire, nous développerons les aspects techniques de cette technologie.

1.1. Quelle est la genèse de la blockchain ?

Commençons par poser un cadre historique à la technologie Blockchain. A défaut de ce que la majorité pense, l'histoire de la technologie blockchain commence bien avant l'invention du Bitcoin par Satoshi Nakamoto en 2008. Elle voit le jour en 1991 quand deux chercheurs, Stuart Haber et W. Scott Stornetta, ont introduit pour la première fois la notion d'une chaine de blocs cryptographiquement sécurisée *(Iredale,2020)*. Leur solution avait pour objectif de permettre l'horodatage des documents de façon à ce que ceux-ci ne puissent plus jamais être antidatés ou altérés. Leur solution fut améliorée en 1992 par l'ajout de la technologie dite arbre de

Merkle, technologie inventée elle-même en 1979 par Ralph Merkle *(Sheldon, 2021)*. Cette technologie augmenta l'efficacité de la solution en permettant de rassembler plus de documents en un seul bloc. Nous verrons le fonctionnement de l'arbre de Merkle plus en détail dans la partie 1.2 de ce mémoire.

En 1995, Stuart Haber et W. Scott Stornetta décidèrent de créer une société de certification, baptisée Surety. L'activité principale de l'entreprise était ainsi de créer un tampon cryptographique pour documents numériques au moyen d'un logiciel nommé AbsoluteProof. Les documents des clients vont être hachés et horodatés de façon à créer un identifiant permettant de les authentifier de manière unique et dans le temps. L'ensemble de ces identifiants va être conservé dans un grand registre détenu par Surety. Pour prouver que ce registre n'est pas modifié en interne, Haber et Stornetta ont alors décidé de publier, de manière hebdomadaire, un hash (une empreinte) rassemblant tous les nouveaux identifiants ajoutés au registre. Internet n'étant alors que dans ses prémices, il leur a semblé plus pertinent de publier leur base de données dans la rubrique « Annonces et objets trouvés » du New-York Times.


NOTICES & LOST AND FOUND
(5100-5102)

Universal Registry Entries:
Zone 2 -
dS8492cgVOFAoP9kvE1XzMOrQ
HgEwzkVbVafNvIkUz99qvq8/ME
p5y9EFSG8XxzMBalGQQ==
Zone 3 -
JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuqLK
durxHQV5pSHLqBGPRlv+mg==
These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.
www.surety.com 571-748-5800

Figure 1 : Le hash de la première blockchain dans le New York Times

En publiant chaque semaine le hash des identifiants des documents dans le New York Times, Haber et Stornetta permettent au public de connaitre l'historique des documents certifiés par leur entreprise. De plus, il devient quasi impossible de modifier de manière malveillante le registre les regroupant. En effet, le New York Times tire en moyenne 570 000 exemplaires quotidiens, pour modifier le registre il faudrait pouvoir fabriquer et faire circuler à plus grande échelle de faux journaux mentionnant une chaine de hachage différente *(Oberhaus, 2018).*

En 2004, Hal Finney introduit le concept de RPoW («Reusable Proof of Work » pour «Preuve de travail réutilisable ») *(Binance Academy, 2021).*

Le RPoW a résolu le problème de la double dépense en conservant un registre de la propriété des jetons et en introduisant le concept de preuve de travail. Nous verrons le concept en détail dans la partie sur les différents types de consensus (1.5) et celui de jeton dans la partie (2.3).

Le problème de la double dépense désigne le fait que les mêmes unités d'une devise numérique peuvent être dépensées plus d'une fois (Wikipédia, 2020).

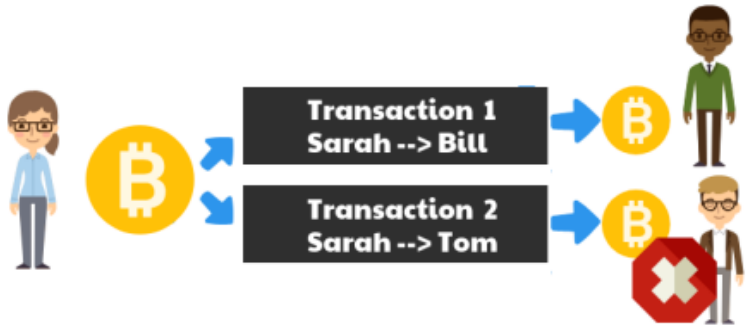


Figure 2 : Double dépense, Blockchain Training Alliance 2020

En 2008, le pseudonyme Satoshi Nakamoto, utilisé par un individu ou un groupe d'individus encore inconnus aujourd'hui, publie le livre blanc[1] du très célèbre système de paiement électronique décentralisé de pair-à-pair appelé Bitcoin. Le Bitcoin est une innovation fondée sur une combinaison de techniques préexistantes. Il est la première application concrète de la blockchain telle qu'on la connait aujourd'hui. L'avancée apportée par le Bitcoin est une amélioration de la solution au problème de double dépense. Il remplace le protocole informatique précédemment utilisé, RPoW, par un protocole peer-to-peer décentralisé ayant comme objectif de tracer et vérifier les transactions *(Binance Academy, 2021)*. Par son ajout de la décentralisation ainsi que de son explication de la technologie blockchain dans le livre blanc du Bitcoin, Satoshi Nakamoto ouvre la porte des cryptomonnaies et étend les

[1] Satoshi Nakamoto, 2008 : bitcoin.pdf

possibilités d'application concrète de la technologie blockchain. Le premier bloc de la blockchain Bitcoin est miné le 3 janvier 2009.

Au cours des années 2013 à 2015, certains développeurs ont estimé que le Bitcoin n'exploitait pas toutes les opportunités que la technologie blockchain avait à offrir. Préoccupé par les limites du Bitcoin, Vitalik Buterin lança donc en 2013 une nouvelle blockchain publique, nommée Ethereum, ayant pour objectif d'augmenter les fonctionnalités de la blockchain. Ethereum se veut plus malléable que le Bitcoin notamment en permettant aux utilisateurs d'enregistrer d'autres actifs que des transactions monétaires. Elle permet d'y stocker tous autres types de données ainsi que des contrats. Cette invention marque le début d'une nouvelle ère dans l'histoire de la blockchain en introduisant notamment les « smart contracts » ou contrats intelligents, dont nous verrons le fonctionnement et l'utilité dans la suite de ce mémoire *(Iredale, 2020)*.

L'histoire de la technologie blockchain ne s'arrête pas là. Ces dernières années se démarquent par une prise de conscience générale du potentiel de la technologie et par une multiplication des projets en lien avec celle-ci. Nous pouvons notamment retrouver une explosion du nombre de projets publics dans le secteur des cryptomonnaies ou encore dans celui des plateformes tel que Hyperledger[2]. Nous assistons également à un nombre grandissant de projets privés au sein des entreprises qui tirent parti de cette technologie pour améliorer leur efficacité *(Iredale,2020)*. Selon l'enquête mondiale de 2021 menée par Deloitte sur la Blockchain, 73 pourcents des personnes interrogées conviennent que leur organisation respective perdrait une opportunité d'avantage concurrentiel si elle n'adopte pas la blockchain dans les années qui viennent.

Il est difficile de prévoir l'avenir d'une technologie d'autant plus que l'histoire de la blockchain est si courte. Cependant, au vu de l'augmentation des recherches et des investissements qui sont faits dans celle-ci, la blockchain ne peut que continuer de s'améliorer dans les années à venir

[2] The Linux Fondation, 2014: HL_Paper_HyperledgerOverview_102721.pdf

1.2. Qu'est-ce qu'un bloc ?

Un bloc est composé de deux parties : une partie entête (bloc header) et une partie qui contient des transactions.

Le bloc se remplit progressivement par de nouvelles transactions horodatées et validées. Les transactions dont nous parlons ici peuvent être des transactions en cryptomonnaies mais également des interactions avec des contrats ou de manière plus générale des transactions contenant n'importe quel type de donnée que nous voudrions stocker dans un bloc. Ces transactions sont placées les unes à la suite des autres. La première transaction de chaque bloc doit identifier la rémunération du mineur du bloc. Nous reviendrons sur le concept du minage ultérieurement.

La rémunération peut prendre 2 formes, soit via la création de nouveaux jetons (ex: de nouveaux Bitcoins) soit par imputation de frais de transactions *(Lars, 2019)*. Les deux formes de rémunération peuvent coexister.

L'entête quant à elle est un résumé des informations du bloc. Elle est généralement constituée des éléments suivants :

- L'identifiant ou Hash du bloc précédent : il permet de relier les blocs entre eux.
- L'horodatage : la date et l'heure du minage.
- La racine de Merkle : elle présente un hash unique qui synthétise l'ensemble des transactions.
- La version du protocole utilisé, les blockchains peuvent évoluer et ainsi changer de protocole au fil des années.

De plus, d'autres données spécifiques à la méthode de consensus ou à la technologie employée par la blockchain peuvent également se retrouver dans l'entête. Les données supplémentaires les plus communément retrouvées sont les suivantes :

- La difficulté de minage : elle représente la difficulté des conditions de minage d'un bloc.

- Le nonce : il s'agit de l'abréviation de « number only used once ». Le nonce est le nombre que les mineurs de la blockchain essayent de trouver dans une blockchain basée sur la méthode de validation dite Proof of Work *(Nakamoto, 2009).*

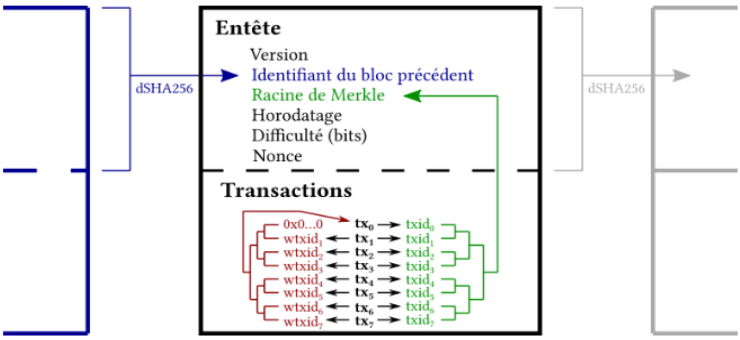


Figure 3 : Entête simple provenant de la blockchain Bitcoin, Lars 2019

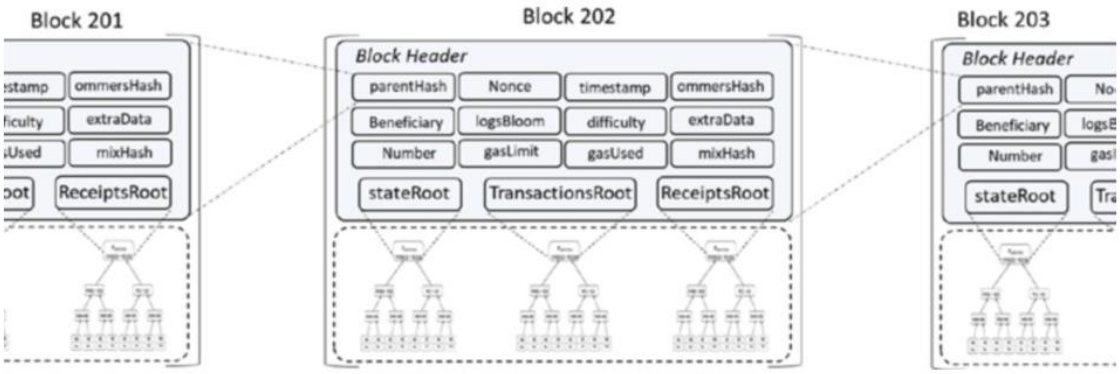


Figure 4 Entête plus complexe provenant de la blockchain Ethereum, Supernova 2018

1.2.1. Fonction de hachage cryptographique

Une fonction de hachage a pour objectif de prendre une donnée en input et d'en extraire une empreinte numérique de taille fixe, appelée hash *(Pavel, 2019).* La donnée initiale servant d'input peut prendre différentes formes allant du simple fichier texte en passant par une image ou même un film. Elle devra cependant être transformée en texte binaire avant que la fonction de hachage puisse lui être appliquée.

Figure 5 : Fonction de hachage, Pavel 2019

Une bonne fonction de hachage répond à certaines propriétés *(Manuel, 2011, p7-9)*:

- La résistance à la préimage: une fonction de hachage est à sens unique. Il est facile de calculer le hash d'un texte mais il est pratiquement impossible de retrouver le texte d'origine sur base de son hash.
- La résistance à la collision : l'empreinte numérique, hash, est pratiquement unique. La probabilité d'avoir un hash identique pour deux inputs différents doit être pratiquement nulle.
- L'effet avalanche : une variation même infime du texte en input provoque un changement drastique sur le hash.

Nous invitons le lecteur à se connecter sur le lien suivant : SHA256 Online (emn178.github.io). Il permet de se familiariser avec le concept du hachage.

A titre d'exemple, nous avons réalisé les hachages suivants avec la fonction de hachage Sha-256, utilisée dans le bitcoin :

- Le hash de la phrase « l'utilisation de la blockchain dans l'assurance » est :
  526d35f88c87c81fb7176303c5cacc737c3e6af32db09650b75f8de0815eaa98

- En substituant un R majuscule dans le mot assurance, le hash de la phrase « la blockchain dans l'assurRance » devient:
  8bcb9e20d9c64fab3c47f564012179660f11f618ae37789e1da56eb35d527bd8
  Ceci démontre qu'une modification mineure dans la phrase engendre un hash totalement différent.

- Le hash de la phrase « Fiat et pariter eodem autem tertiam diligendi fiat qui probo sint ferri quasi quanti aequaliterque quibus tertiam erga benevolentiae pariter autem erga in et amicum amicis amicis sententias tres se » est:
  2fdd64e8daf5ea11e96bad798d944b0804632b8d59494cec169d49f67b70ff0c
  Ceci démontre que quel que soit la longueur du texte haché, le hash présente une taille fixe.

La technologie blockchain utilise la fonction de hachage de plusieurs manières différentes. Celle-ci joue notamment un rôle dans la construction de la chaine mais également dans les signatures électroniques. Nous reviendrons plus en détail sur ces différentes utilisations par la suite.

1.2.2. L'arbre de Merkle

Nous avons vu qu'un bloc est rempli de transactions et que celles-ci sont placées dans un certain ordre. L'arbre de Merkle a pour objectif de relier ces transactions entre elles afin de trouver une empreinte unique les regroupant. Cette empreinte est appelée « racine de Merkle ».

Prenons un exemple pour mieux comprendre comment cette racine est calculée. La figure 6 ci-dessous représente un arbre calculé sur base d'un bloc contenant 6 transactions (TX1, TX2, TX3, TX4, TX5, TX6). Dans un premier temps, ces transactions sont hachées afin d'obtenir leur empreintes respectives (H1, H2, etc.).

Les empreintes sont ensuite concaténées et hachées deux par deux (H1+H2 = H1,2).

Les étapes sont ensuite répétées jusqu'à ce que toutes les transactions soient hachées et réunies dans une seule empreinte, appelée racine de Merkle.

Si le nombre d'empreintes se trouve être impaire, la dernière empreinte doit être combinée avec elle-même pour continuer le processus. Dans notre exemple, H5,6 sera combiné avec lui-même pour former H5,6,5,6 *(Lars, 2020)*.

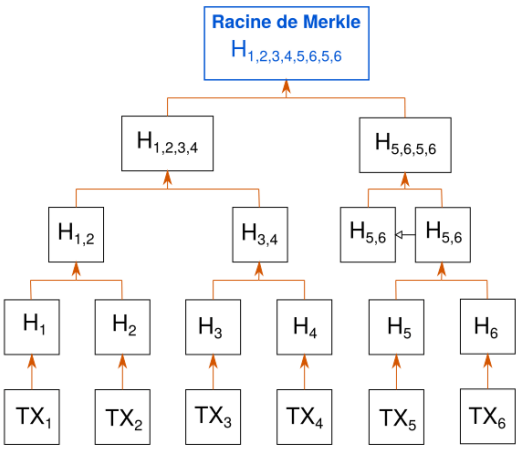


Figure 6 : Arbre de Merkle, Lars 2020

La racine de Merkle sera placée dans l'entête du bloc. Elle permet de vérifier facilement si une transaction du bloc a été altérée. La vérification se fait en comparant les racines de Merkle des différentes copies d'un même bloc diffusées dans le réseau. En se basant sur les propriétés du hash vues précédemment, la moindre modification d'une transaction engendrerait un changement important du résultat de la racine de Merkle.

1.2.3. L'identification d'un bloc

La dernière notion importante d'un bloc concerne son identification dans la chaine. Un bloc peut être identifié de deux façons.

La première consiste à identifier le hash du bloc. Il permet d'identifier un bloc et les données comprises dans celui-ci. Il représente l'empreinte numérique du bloc. Il se calcule en introduisant toutes les données comprises dans l'entête du bloc au sein d'une fonction de hachage *(Antonopoulos, 2015)*. Cette fonction est spécifique à chaque blockchain et est déterminée dans son protocole.

La deuxième manière d'identifier un bloc consiste à déterminer sa hauteur. Elle représente la position d'un bloc dans la chaine. Le premier bloc de la chaine, appelé bloc genesis, porte la hauteur 0. Le deuxième bloc aura une hauteur de 1, le troisième une hauteur de 2, et ainsi de suite.

1.3. Qu'est-ce que la chaine ?

Maintenant que nous avons défini ce qu'est un bloc et ce dont il est composé, intéressons-nous au chainage de ceux-ci. Souvenons-nous que l'un des éléments principaux présent dans l'entête d'un bloc est le hash du bloc précédent. Nous savons que le hash représente l'empreinte numérique d'un bloc, calculé sur base de toutes les données contenues dans celui-ci. Il permet ainsi d'identifier un bloc sur base de son empreinte.

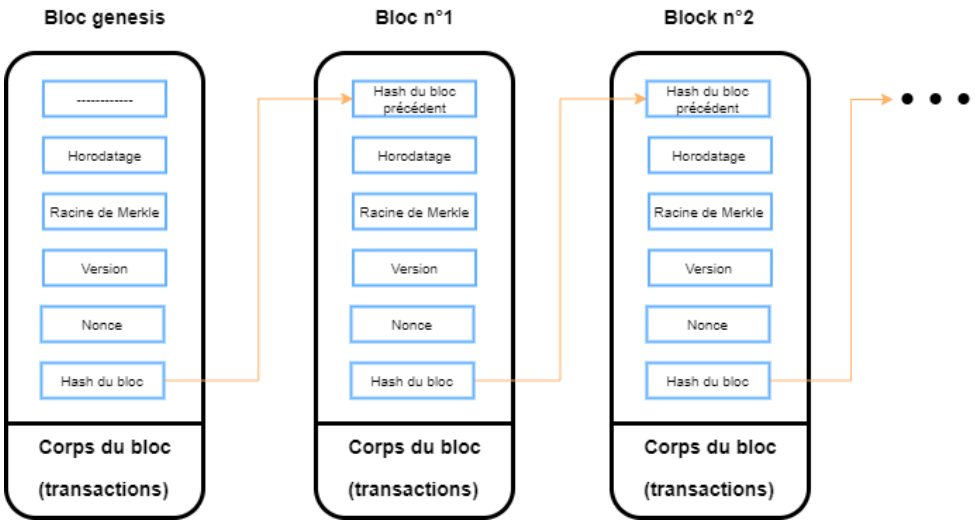


Figure 7 : Chaine de blocs

Le schéma ci-dessus démontre comment les blocs validés sont placés les uns à la suite des autres et sont reliés, chainés entre eux par leur hash respectif. Mis bout à bout, ces blocs vont donc former un grand livre regroupant les transactions et/ou les données comprises dans les différents blocs.

1.4. La blockchain est un registre d'informations distribué

La définition de la blockchain selon le ministère de l'Economie et des Finances française est la suivante : *« Une blockchain est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie »*

Il reste plusieurs notions comprises dans cette définition qui doivent encore être traitées dans ce mémoire. Commençons par la notion de partage.

Selon Vitalik Buterin *(2017)*, fondateur d'Ethereum, les blockchains sont :

- Décentralisées politiquement : celles-ci ne sont pas contrôlées par une seule personne, un seul organisme.

- Décentralisées architecturalement : celles-ci sont partagées au travers d'un réseau d'ordinateurs connectés entre eux via le web. Il n'existe dès lors pas de point unique qui centralise l'information et qui est susceptible d'être défaillant.
- Centralisées logiquement : il existe une seule version commune et validée de chaque blockchain. Tous les acteurs du réseau gardent une copie de l'état de la blockchain. Chaque blockchain constitue une entité. Si une blockchain est découpée, les deux blockchains résultantes seront, par définition, différentes.

Il existe 3 types de réseaux, les réseaux centralisés, décentralisés et distribués. Le graphique ci-dessous permet de mieux comprendre leur différence. Dans un réseau centralisé, toute l'information produite par les utilisateurs est traitée via un gestionnaire unique. Dans un réseau décentralisé, celle-ci est traitée via plusieurs gestionnaires qui se partagent le maintien du réseau. Finalement, dans un réseau distribué, chaque utilisateur peut directement participer au réseau et à sa gestion.

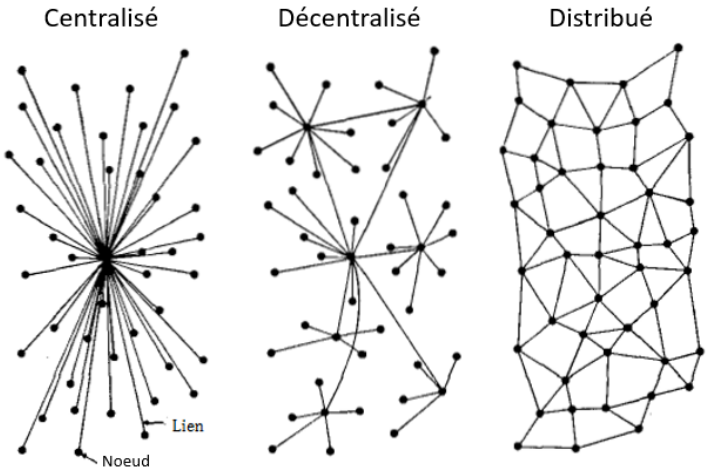


Figure 8 : Les différents types de réseau

La blockchain est une technologie dite distribuée. Les utilisateurs qui participent activement au maintien et à l'intégrité du réseau sont appelés « nœuds ». Dans un réseau distribué les nœuds sont connectés entre eux en temps réel *(Vergne,2020).*

Vitalik Buterin *(2017)* nous donne également 3 raisons qui poussent à choisir la décentralisation :

- La tolérance aux pannes : la décentralisation architecturale rend les pannes accidentelles quasi improbables. Ceci est dû à la démultiplication des composants sur lesquels le système repose.
- La résistance aux attaques : un système décentralisé est plus compliqué à attaquer. Il ne repose pas sur un point central. Plus de 50% des nœuds doivent être attaqués pour mettre à mal le réseau.
- La résistance à la collusion : au vu du grand nombre de particuliers qui participent dans la gestion d'un système distribué, il est difficile pour eux de s'entendre d'une manière qui leur profite aux dépens des autres participants.

1.5. Les différents types de consensus

Le rôle principal des acteurs ou nœuds du réseau consiste à maintenir et à garantir l'intégrité de celui-ci. Pour se faire, plusieurs méthodes, appelées protocole de consensus, basées sur une validation faite par la majorité (>50% des acteurs) existent. Celles-ci permettent de vérifier et valider l'authenticité des transactions et de chaque bloc compris dans la chaine.

1.5.1. Proof-of-Work

Le protocole de consensus **Proof-of-Work** (PoW), aussi appelé preuve de travail, est le plus utilisé. Depuis 2009, celui-ci a démontré son efficacité et sa résistance aux tentatives d'attaque. Il est notamment utilisé par le Bitcoin et l'Ethereum (sous sa version actuelle).

Lorsqu'un bloc est prêt à être soumis au consensus, soit après un laps de temps, soit lorsque celui-ci est complet, les nœuds du réseau vont rentrer en compétition pour résoudre un problème afin de valider le bloc de données. Dans ce protocole, les nœuds sont appelés mineurs. Ils doivent deviner par un processus d'essais-erreurs, appelé minage, le nonce (nombre) permettant de valider le bloc. Les données comprises dans l'entête du bloc et le nonce présumé sont introduites dans une fonction de hachage cryptographique. Si le hash obtenu correspond au niveau de difficulté de minage, le mineur a réussi à résoudre le problème. Le niveau de difficulté de minage correspond à des conditions qui doivent être présentes dans le hash. Par exemple, dans le cas du bitcoin, le niveau de difficulté correspond

au nombre de « 0 » par lequel le hash du bloc doit commencer, appelé leading zero. Ce niveau de difficulté est ajusté par le réseau en fonction du nombre de mineurs et de leur puissance de calcul.

Lorsqu'un mineur trouve un nonce adéquat, il partage sa solution avec les autres nœuds du réseau. Ceux-ci vérifieront la validité du nonce trouvé en hachant les données de bloc accompagnées de ce nonce. Ils vérifient également que les données soient valides. Si la solution est valide, ils confirmeront que le nonce est correct.

Lorsque 51% ou plus des mineurs sont d'accord avec le nonce proposé, les transactions sur le bloc du gagnant sont considérées comme correctes et le mineur ayant réussi le minage sera récompensé. Comme expliqué précédemment dans la partie « qu'est-ce qu'un bloc », la récompense peut se matérialiser par l'octroi de nouveaux jetons et/ou par le paiement de frais de transaction.

A l'inverse, si une majorité n'est pas atteinte, le mineur ne perçoit aucune récompense. Le processus d'essais/erreurs engendre alors uniquement de lourdes dépenses énergétiques.

Sur base de la théorie des jeux, le consensus par preuve de travail incite chaque nœud à se comporter de manière honnête. Tout participant malhonnête devra en effet supporter des dépenses réelles pour estimer un nonce qui ne sera pas validé par le réseau.

Une fois un bloc et ses données validés, les nœuds n'ayant pas la version correcte remplaceront leur version personnelle par celle entérinée par la majorité.

Il est également important de noter que dans un consensus PoW, au plus le nombre de nœuds est élevé, au plus la sécurité est renforcée et le temps nécessaire pour vérifier les transactions est augmenté *(Bennett & Decker, 2020)*.

Finalement, dans certains réseaux volumineux, il est possible que deux blocs soient minés et partagés exactement au même moment (A et B). Le temps de propagation des versions à valider pouvant être variable, une partie du réseau peut se retrouver avec un bloc valide (A) et l'autre partie avec l'autre bloc (B) également validé. Le réseau se retrouve dès lors avec deux bouts de chaine, tous les deux valides et validés. Ce phénomène est appelé « fourche » ou « fork » en anglais. Dans le cas d'un fork dit léger (soft fork), la solution se résout rapidement. Chaque nœud du réseau continue son travail sur le segment de chaine qu'il considère comme valide. Les nœuds ayant le bloc A comme valide essaient de prolonger ce segment de chaine et inversement pour les nœuds ayant le bloc B. Lorsqu'une des deux chaines arrive à prolonger son segment d'un bloc, en y ajoutant par exemple un bloc valide C, celle-ci, étant la plus longue, est considérée comme principale. Les mineurs de l'autre segment vont alors abandonner leurs calculs et continuer la chaine principale constituée du bloc C *(Pavel, 2019)*.

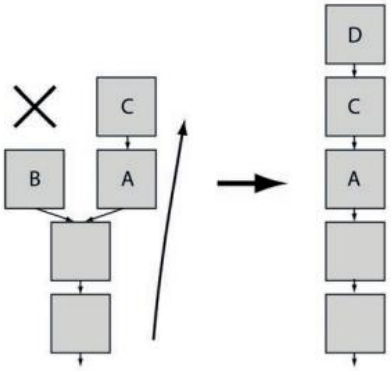


Figure 9 : Soft Fork, Pavel 2019

Lorsque très exceptionnellement, le réseau n'arrive pas à se mettre d'accord sur une décision, un hard fork s'opère. Un exemple de hard fork pourrait être un désaccord sur une modification du protocole. Ce fut le cas en 2017 lors de la création du bitcoin cash. Il résulte de la scission de la chaine historique du bitcoin en deux chaines distinctes.

1.5.2. Proof of Stake

Le protocole de consensus **Proof-of-Stake** (PoS) est un système de consensus plus récent que celui du Proof-of-Work. Il a été proposé comme alternative permettant de réduire les coûts et d'accroitre les performances du mécanisme de consensus PoW. Pour se faire, il supprime le problème à résoudre utilisé dans la validation d'un bloc.

Le protocole PoS se base sur le principe qu'au plus un utilisateur a d'intérêts dans la blockchain, au plus il sera appliqué dans la recherche d'un hash valide. Dans le consensus

Proof of Stake, tous les nœuds souhaitant participer au minage d'un bloc vont déposer une mise dans un fonds. Un nœud participant est alors choisi aléatoirement au moment du consensus. (Certaines blockchains utilisant le PoS augmentent les chances d'être choisi en fonction de l'importance de la mise. D'autres prennent également en compte la durée depuis laquelle les jetons misés sont en possession du participant.) Le nœud choisi hache les données comprises dans son bloc et les partage aux autres participants. Ensuite, les nœuds du réseau parient sur la validité des transactions et le hash du bloc proposé.

Si la majorité valide le bloc, le nœud gagnant ainsi que tous ceux qui ont parié sur sa validité sont récompensés. A l'inverse, si la version du bloc proposée par le nœud aléatoire n'est pas validée par la majorité, celui-ci perd sa mise initiale et un autre nœud est sélectionné pour retenter le process *(Poelstra,2015)*.

Tableau 1, récapitulatif des différences majeures entre le Proof-of-Work et le Proof-of-Stake :

PoW	PoS
Travailler pour une récompense	Parier pour une récompense
Très énergivore	Faiblement énergivore
Réduit la vitesse des transactions	Augmente la vitesse des transactions
Nécessite de puissants ordinateurs	Nécessite des fonds à parier
A déjà largement fait ses preuves	Technologie plus récente

1.5.3. Autres protocoles de consensus

- Proof of Activity : un mélange entre PoW et PoS. Des blocs vides sont minés sur base du PoW et les transactions qui les composent sont ensuite validées par le PoS.
- Proof of Burn : même principe que le PoS sauf que les jetons misés sont détruits, ils ne sont pas récupérés par la suite.
- Proof of Authority : certains nœuds sont désignés comme gestionnaire de la blockchain et ce sont eux qui valident les transactions et les blocs (Surtout dans des blockchains privées).

1.6. Les différents types de blockchains

Lorsque nous pensons aux blockchains, nous pensons à une technologie parfaitement décentralisée et transparente comme précédemment décrite dans ce mémoire. Ces blockchains sont dites publiques et ouvertes. Cependant, certaines activités ou certains secteurs économiques ne sont pas compatibles avec ce type de blockchains. Ces secteurs ou ces activités nécessitent un caractère plus privatif. Dès lors, des blockchains permissionnées ont été imaginées. Elles permettent de limiter les acteurs qui peuvent lire ou écrire les informations contenues dans la blockchain *(Guegan, 2017)*.

Qui peut écrire de nouvelles informations sur la blockchain ? La réponse à cette question va déterminer si nous parlons d'une blockchain publique ou d'une blockchain privée. Dans le cas d'une blockchain dite publique, n'importe qui peut ajouter de l'information et même devenir un nœud validateur de la chaine. Dans le cas d'une blockchain privée, les fondateurs du système devront sélectionner les acteurs qui pourront participer à l'écriture et la validation des données.

Qui peut lire les informations contenues dans une blockchain ? La réponse à cette question va déterminer si nous parlons d'une blockchain ouverte ou d'une blockchain fermée. Dans une blockchain ouverte, n'importe qui peut observer le registre. Dans une blockchain, fermée, une autorisation est nécessaire pour pouvoir y accéder *(Lars, 2020)*.

Tableau 2, exemples concrets des différents types de blockchain :

Blockchain	Lecture ouverte	Lecture fermée
Ecriture ouverte (Publique)	Exemple : • Cryptomonnaies (Bitcoin) • Jeux vidéo	Exemple : • Un suffrage public

Ecriture fermée (Privée)	Exemple : • Traçabilité des produits • Publication légale des comptes d'entreprises	Exemple : • Partage des données clients dans les secteurs financier ou médical

Il est cependant important de préciser que les solutions restent modulables. Il est, par exemple, possible d'ajouter certaines permissions sur des blockchains publiques ouvertes. Nous constatons néanmoins que les projets de blockchain mis en œuvre par les entreprises privées sont généralement du type permissionné. En effet, ces dernières craignent une transparence totale et l'absence de permission.

1.7. La cryptographie

Le mot « crypto » signifie « secret » en grec. La cryptographie consiste pour un expéditeur à chiffrer son message, masquant ainsi son contenu vis-à-vis des tiers. Le destinataire déchiffrera ensuite le message pour découvrir l'information contenue dans celui-ci.

La cryptographie se base sur 4 piliers de la sécurité *(Dr R.Djellab, 2018)* :

- Confidentialité : l'information ne doit être accessible qu'aux entités (personnes ou machines) autorisées
- Intégrité : l'information ne doit pas changer entre son expéditeur et son destinataire
- Authentification : le destinataire doit pouvoir vérifier que l'information vient de l'expéditeur
- Non-répudiation : les entités ne doivent pas pouvoir nier un engagement ou une action préalable

La cryptographie par chiffrement symétrique est l'un des systèmes cryptographiques le plus simple. Un algorithme de chiffrement symétrique utilise la même clé (la même technique) pour chiffrer et déchiffrer le secret. Par exemple, si Alice veut envoyer un message à Bob, celle-ci chiffre son message au moyen d'une clé. Lorsque Bob reçoit le message, celui-ci peut simplement le déchiffrer au moyen de la même clé.

Par cette méthode, la sécurité n'est respectée qu'à la condition que la clé de chiffrement ne soit connue que par Alice et Bob et que ceux-ci se la soient échangée auparavant.

Cette technique de cryptage présente un défaut majeur, les deux parties doivent se connaitre et s'envoyer de manière sécurisée la clé permettant de déchiffrer les secrets. Afin de palier à ce défaut, les blockchains utilisent la cryptographie asymétrique. Celle-ci se base pour les opérations de chiffrement et déchiffrement sur l'utilisation d'une paire de clés (la clé publique et la clé privée) générées à l'aide d'algorithmes de cryptage. La clé privée est gardée précieusement par son propriétaire. Liée à cette clé privée, il existe une clé publique qui est largement distribuée. Si nous reprenons l'exemple précédent, lorsque Alice souhaite envoyer un message secret à Bob, celle-ci chiffre le contenu du message avec la clé publique de Bob. Bob, étant propriétaire de la clé privée, lui seul pourra déchiffrer le message. Ainsi, les clés publiques permettent de chiffrer un message et les clés privées permettent de le déchiffrer.

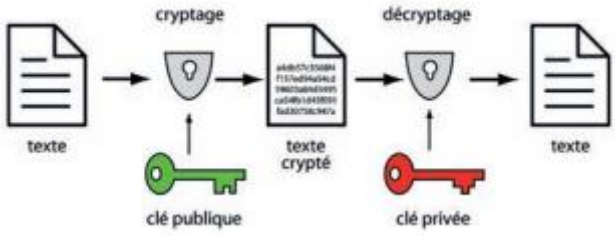


Figure 10 : Cryptographie asymétrique, Pavel 2019

Dans certains cas tel que celui de la signature électronique expliquée ci-dessous, il est également possible de chiffrer un message avec sa clé privée qui pourra être déchiffré au moyen de la clé publique liée.

La blockchain publique utilise la cryptographie principalement pour :

- Sécuriser l'identité de l'expéditeur des transactions (anonymat + authentification+ non répudiation)
- S'assurer de la protection des données (intégrité + confidentialité)

Pour assurer ces deux objectifs, les blockchains utilisent la signature électronique. Celle-ci associe la cryptographie asymétrique et une fonction de hachage. Pour signer électroniquement un document, il faut premièrement passer ce document dans une fonction de hachage afin d'en extraire son empreinte numérique, le hash. Ensuite, ce hash est encrypté à l'aide de la clé privée. La clé privé étant unique et individuelle, celle-ci authentifie l'expéditeur. C'est cet encryptage qui sert de signature du document. Au moment du transfert de celui-ci, l'expéditeur envoie donc le document original plus le hash de celui-ci encrypté comme signature au destinataire.

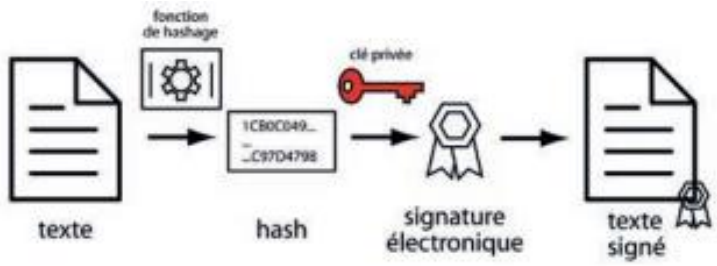


Figure 11 : Signature électronique d'un texte, Pavel 2019

A la réception des documents, pour vérifier l'intégrité et l'authenticité des documents, le destinataire va effectuer deux opérations. Premièrement, à l'aide de la clé publique, il va décrypter la signature afin d'obtenir le hash du document extrait par l'expéditeur. Ensuite, à son tour, le destinataire va passer le document reçu dans la même fonction de hachage utilisée par l'expéditeur. Si les deux hashes obtenus coïncident, le document est intègre et authentique. Sinon, soit le document lui-même, soit la signature ont été modifiés durant la transmission *(Pavel 2019)*.

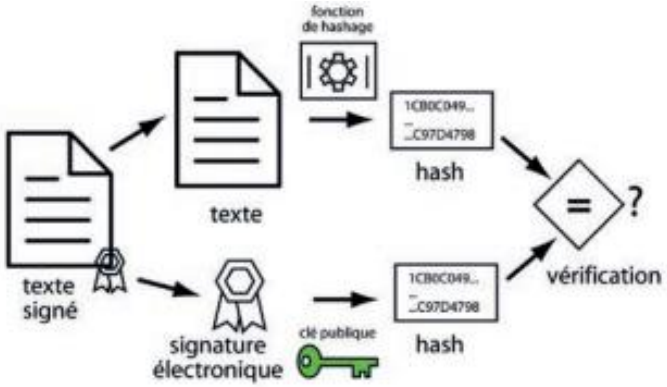


Figure 12 : Vérification de l'authenticité et de l'intégrité d'un texte signé électroniquement, Pavel 2019

1.8. Le bitcoin en guise d'illustration du fonctionnement de la technologie

A ce stade du mémoire, les notions importantes pour la compréhension d'une blockchain simple ont été définies. Nous illustrerons le fonctionnement de cette technologie en présentant les caractéristiques de la plus célèbre des blockchains publiques et ouvertes, le Bitcoin.

Pour simplifier la lecture, nous découperons le fonctionnement du bitcoin en plusieurs étapes. Dans la pratique, de nombreux processus se font en parallèle.

1.8.1. La création d'un portefeuille

Celui qui souhaite réaliser une transaction en bitcoins, doit préalablement se constituer un portefeuille. Le portefeuille ne contient pas de bitcoins. Il contient les clés privées, publiques et les adresses de l'utilisateur.

La séquence est la suivante :

- à l'initiative de l'utilisateur, une clé privée est générée par un algorithme de cryptage,
- au départ de la clé privée, la clé publique est également générée à l'aide d'un algorithme de cryptage,
- enfin, l'adresse de l'utilisateur est générée en hachant la clé publique *(Narayanan et al., 2016, p42)*.

La séquence est relativement facile à calculer, mais la remonter est pratiquement impossible.

Ce processus permet de garantir l'anonymat des utilisateurs. Ils communiquent exclusivement via les adresses contenues au sein de leur portefeuille.

1.8.2. Effectuer une transaction en bitcoins

Imaginons qu'Alice veuille transférer 0.1 Bitcoin à Bob.

Dans son instruction, Alice présentera les informations suivantes :

En entrée, Alice indique l'adresse via laquelle elle dispose des fonds nécessaires pour effectuer la transaction (1 Bitcoin dans notre exemple),

En sortie, elle indique :

- le nombre de Bitcoins à attribuer à l'adresse de Bob (0.1 Bitcoin dans notre exemple),
- le nombre de Bitcoins à affecter en guise de rémunération pour valider la transaction (0.0001 Bitcoin dans notre exemple),
- et finalement, le nombre de Bitcoins résiduels à renvoyer sur une de ses adresses personnelles (0.8999 Bitcoin dans notre exemple).

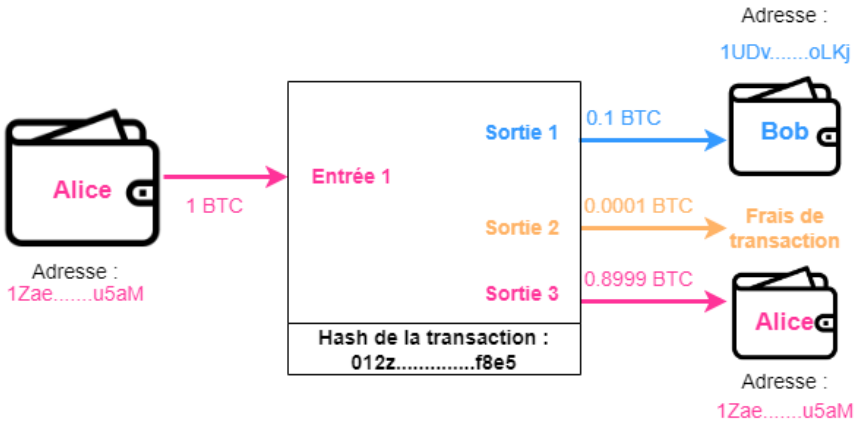


Figure 13 : Exemple d'une transaction simple sur la blockchain Bitcoin

Toutes ces entrées et ces sorties vont finalement être hachées afin d'obtenir un identifiant. Celui-ci permettra à une transaction d'être identifiée de manière unique au sein de la blockchain *(Bit2me Academy, 2021).*

1.8.3. Diffusion de la transaction au réseau

Une fois la transaction signée par Alice au moyen de sa clé privée, celle-ci est partagée dans le réseau pour validation. Elle se propagera de nœud en nœud pour rapidement se répandre dans l'ensemble de celui-ci. Chaque nœud fera une série de vérifications dont :

- l'authenticité de la transaction : vérifier au moyen de la clé publique d'Alice et de sa signature électronique que la transaction provient bien d'elle et que celle-ci n'a pas été modifiée
- la disponibilité des fonds : vérifier qu'il n'y ait pas de double dépense et qu'Alice soit bien la propriétaire des Bitcoins utilisés. Cette vérification se fait grâce au caractère ouvert de la blockchain Bitcoin. L'ensemble de l'historique des transactions passées est disponible.

1.8.4. Constitution des blocs

De leur côté, les mineurs composant le réseau Bitcoin essayeront de rassembler ces différentes transactions au sein d'un bloc. La taille d'un bloc ne peut pas excéder 1 Mo. On y regroupe donc entre 1.000 à 3.000 transactions selon leur taille.

Pour relier les transactions entre elles au sein d'un bloc, la fonction de hachage est utilisée. Nous avons vu comment au départ de multiples transactions, regroupées deux par deux, l'arbre de Merkel permettait de générer un hash unique.

Le mineur constitue ensuite l'entête du bloc en y regroupant les informations suivantes : la racine de Merkel, le hash du bloc précédent, la date et l'heure (horodatage), le niveau de difficulté et le nonce.

1.8.5. Le minage des blocs et la constitution de la chaine

Pour miner les blocs de la chaine Bitcoin, les mineurs utilisent le protocole de consensus Proof-of-Work. Au travers de ce protocole, les différents mineurs du réseau vont entrer en compétition dans l'objectif de trouver un hash de bloc répondant aux conditions de difficulté de minage. Cet hash est calculé en passant l'intégralité des éléments constituant l'entête d'un

bloc par la fonction de hachage SHA 256. Par essai-erreur, en modifiant de façon aléatoire la valeur du nonce, les mineurs finiront par identifier un nonce menant au hash valide.

Dans la blockchain Bitcoin, les conditions de minage sont allégées ou renforcées en fonction du temps moyen de minage des blocs depuis le précédent ajustement. L'objectif attendu est l'ajout d'un nouveau bloc toutes les 10 minutes et l'ajustement de difficulté se fait tous les 2016 blocs, environ toutes les deux semaines. Si la moyenne de minage des 2016 blocs excède 20 160 minutes, alors la difficulté est allégée, et inversement. La vitesse de minage des blocs est ainsi adaptée à la puissance de calcul du réseau.

Lorsqu'un mineur trouve un hash répondant aux conditions, il diffuse son bloc ainsi que sa solution aux nœuds du réseau. Ceux-ci vérifient que les transactions comprises dans le bloc sont valides et que le hash de l'entête du bloc proposé respecte les conditions de minage. Pour exprimer leur acceptation du bloc, les nœuds continueront la chaine et donc le travail de minage en utilisant le hash du bloc accepté comme hash précédent *(Nakamoto, 2008)*.

Le mineur du bloc est récompensé, par des Bitcoins, lorsque son bloc est validé (51% ou plus du réseau le considère comme valide). Cette récompense en Bitcoins se compose d'une rémunération fixe liée à la réussite du minage d'un bloc et des différents frais de transactions compris dans le bloc. Actuellement (juin 2022), la récompense fixe s'élève à 6,25 Bitcoins pour chaque nouveau bloc ajouté à la chaine. Cette récompense s'élevait à 50 Bitcoins par bloc en 2009 et est divisée par deux tous les 210 000 blocs minés, soit environ tous les 4 ans. Vers 2140, la récompense fixe de minage sera alors pratiquement nulle et les mineurs seront récompensés uniquement par les frais de transaction *(Binance Academy, 2022)*.

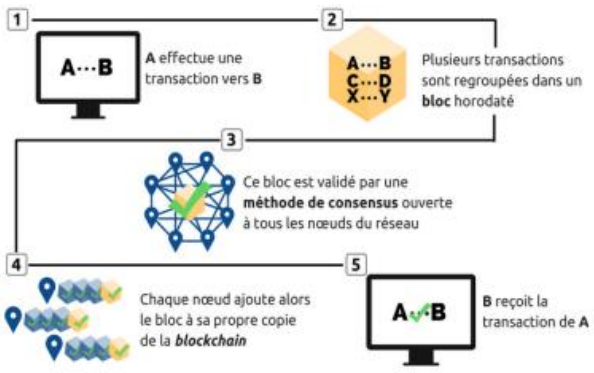


Figure 14 : Transfert d'actif via la blockchain, de La Raudière & Mis, 2018

2. Les atouts/forces de la technologie blockchain

Au sein de la première partie, nous avons étudié le fonctionnement de la technologie blockchain. Elle est clairement novatrice et nous comprenons maintenant mieux l'intérêt que celle-ci suscite ces dernières années.

Selon une enquête menée en 2018 par PWC sur 600 entreprises dans 15 pays, quatre dirigeants sur cinq ont déclaré utiliser la blockchain dans leur entreprise. Un quart des dirigeants déclarent qu'un pilote de mise en œuvre de la blockchain est en cours ou pleinement opérationnel. Près d'un tiers ont des projets en cours de développement et un cinquième sont en mode recherche.

En 2021, l'enquête mondiale de Deloitte sur la blockchain confirme cet engouement autour de la technologie. Le graphique ci-dessous représente le pourcentage des répondants qui sont d'accord avec les différentes déclarations. L'étude a été réalisée auprès de 1280 directeurs financiers (overall) dont 320 dans le secteur de la finance (FSI : Financial Services industry overall) et 70 d'entre eux (FSI Pioneers) pour lesquels l'entreprise a déjà mené à bien un projet lié à la technologie.

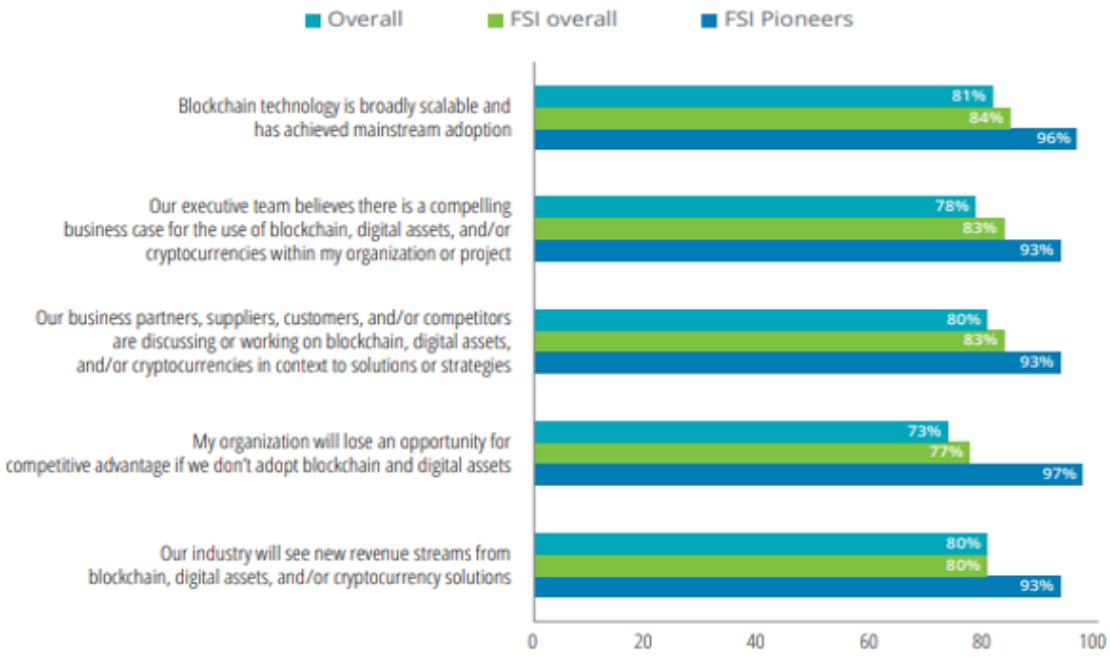


Figure 15 : La considération de la blockchain par les dirigeants financiers, Deloitte's 2021 Global Blockchain Survey

Après plus de dix ans depuis sa première vraie application (Bitcoin) la blockchain commence donc à nous démontrer tout son potentiel. Nous verrons dans cette section les principaux

avantages qu'offre la technologie blockchain publique et ouverte. Il est cependant important de préciser qu'au vu de l'évolution rapide de celle-ci et des investissements qui y sont consacrés, il se peut que d'autres avantages ou applications majeures soient dévoilés dans les années à venir.

2.1. La blockchain comme registre distribué

La technologie blockchain permet la création d'un grand registre infalsifiable et transparent.

Toute donnée validée par un réseau distribué et ainsi inscrite dans un bloc de la chaine est supposée être impossible à modifier ensuite. De plus, le stockage de ces informations horodatées crée au fil du temps un grand registre. Dans le cas d'une blockchain publique et ouverte, il permettra à tout individu de consulter un historique complet des transactions. Dans le cas d'une blockchain permissionnée, la blockchain permettra de garder un contrôle sur les informations contenues dans celle-ci en accordant les permissions qu'à certaines entités.

Plusieurs éléments assurent la sécurité du registre *(Blockchain France, 2016, p 4-5):*

- Les outils cryptographiques : toutes les transactions comprises dans les blocs sont hachées et reliées entre elles par des racines de Merkle. Les blocs eux-mêmes sont également hachés. Ces différents hachages permettent de détecter simplement et rapidement toutes tentatives de modifications.
  De plus, au travers de la signature électronique, il devient impossible de falsifier l'authenticité ou l'intégrité des documents présents dans la blockchain.

- La gestion distribuée du réseau : la technologie blockchain est régie par un réseau d'acteurs (les nœuds). Au travers d'un mécanisme de consensus, celui-ci doit vérifier la validité des différents blocs et des transactions. Pour falsifier une transaction il faudrait contrôler ou corrompre plus de la moitié du réseau afin de la faire valider. Ce qui est pratiquement infaisable dans un réseau largement distribué. De plus, le réseau étant maintenu par un grand nombre d'entités, il n'existe pas de point de défaillance

unique. La technologie blockchain est ainsi fortement résistante aux pannes et attaques techniques. Si un nœud se fait déconnecter, le système continue de fonctionner en toute sécurité.

- La réplication du registre dans les différents nœuds : chaque nœud duplique le registre afin de conserver une copie de celui-ci. Lorsqu'une entité malveillante tente de modifier le registre, la majorité du réseau détecte rapidement une incohérence par rapport à l'historique du registre. La fraude est ainsi repérée et facilement rejetée.

Cet historique horodaté, transparent et sécurisé sera un avantage de taille dans des secteurs où l'irréfutabilité des informations est primordiale *(Berné, 2020)*. La blockchain permet par exemple, la certification de certains objets, d'assurer la traçabilité d'un produit depuis sa production jusqu'à sa vente, l'enregistrement de résultats financiers, …

L'utilisation de ce registre de manière distribuée permet également une grande collaboration au sein d'un écosystème. Ses membres, disposant des autorisations requises, peuvent consulter ou compléter les informations du registre. Ils créent ainsi une base de données unique et partagée *(IBM, n.d .).*

2.2. La blockchain supprime les intermédiaires

La blockchain supprime la notion de tiers de confiance, à savoir une entité unique qui gère le registre, et supprime également les intermédiaires. Ceci a notamment pour conséquence que les écosystèmes gérés via cette technologie peuvent fonctionner 24h/24h. Les opérations peuvent être automatisées (notamment via des contrats intelligents), les erreurs et les frais de vérification en sont donc réduits.

2.2.1. Transfert d'actif

La blockchain permet ainsi le transfert d'actifs, de valeurs au travers d'internet et ce, sans passer par un tiers de confiance. Les premières applications de la technologie, les cryptomonnaies, permettent en effet la création d'un système financier alternatif. Dans ce système, les transactions sont validées par le réseau et les frais de transactions y sont généralement largement inférieurs aux systèmes traditionnels passant par des banques. Le temps nécessaire pour ces transactions en est également grandement réduit. Par exemple, le délai d'une transaction internationale passe d'heures, voire de jours dans les systèmes centralisés traditionnels, à quelques minutes voire secondes dans les blockchains *(Golosova & Romanovs, 2018)*.

2.2.2. Les contrats intelligents

Les « smart contracts » ou contrats intelligents, permettent l'automatisation de différents processus. Ce sont des programmes autonomes présents dans une blockchain. Ils consistent en un code spécifiant des conditions prédéterminées qui, lorsqu'elles sont remplies, s'exécutent automatiquement *(Chainlink, 2021)*. Les données servant à vérifier les conditions de déclenchement du contrat sont importées dans la blockchain par des entités extérieures appelées « oracles ». Les contrats intelligents réduisent l'intervention humaine ce qui permet : d'accroitre la vitesse et l'efficacité des processus, de réduire les couts et de réduire les erreurs d'arbitrage ou les fraudes, …

En guise d'exemple, imaginons un agriculteur qui souhaite assurer ses récoltes contre la sécheresse. Actuellement, il s'adresserait à un assureur qui s'engagerait à lui verser un dédommagement dans le cas d'un déficit de pluie. Cet engagement pourrait être automatisé via un contrat intelligent inséré au sein d'une blockchain. Une entité tierce, extérieur au contrat, servira d'oracle. Dans notre exemple cette entité pourrait être l'IRM (Institut royal météorologique). Quotidiennement, l'IRM communiquerait le niveau de pluviosité au contrat intelligent. Dès la condition remplie (par exemple 30 j consécutifs sans pluie), le contrat intelligent déclenchera automatiquement une indemnisation à l'agriculteur.

L'intérêt de stocker les contrats intelligents dans la blockchain réside dans la garantie que celle-ci propose. Il est impossible pour une des deux parties de venir modifier les termes du contrat *(Blockchain France, 2016)*. Ces contrats pourront dès lors être automatisés.

2.2.3. Un technologie qui supprime le besoin de confiance

Enfin, la blockchain est une technologie dite «trustless ». Les protocoles de consensus assurent le maintien de l'intégrité et l'authenticité du réseau. Ils permettent ainsi de ne pas avoir besoin d'accorder une quelconque confiance. Au travers du système, nous ne devons plus accorder notre confiance à une organisation ou une entité (Binance Academy, 2022).

2.3. La blockchain permet la tokenisation

La tokenisation permet de transformer des actifs indivisible en jetons, appelés tokens. Ces jetons représentent ainsi de manière numérique la propriété complète ou partagée de toute entité ayant une valeur spécifique. La propriété d'actifs physiques initialement indivisibles peut donc être partagée entre plusieurs propriétaires.

Le prix du token créé sera variable et soumis à la loi de l'offre et de la demande.

Par exemple, la propriété d'un appartement ou d'une œuvre d'art d'une valeur de 200 000 euros pourrait être transformée en 200 tokens valant initialement 1000 euro pièce et stockés sur une blockchain. La propriété de ce bien immobilier ou mobilier appartiendrait ainsi aux propriétaires des tokens. Chaque token donnant droit à 0.5 % de la valeur de celui-ci *(Geroni, 2021)*.

Cette technologie est déjà utilisée dans le secteur financier. La banque BNP a récemment (mai 2022) fait savoir qu'elle utiliserait la solution de tokenisation développée par JP Morgan. Depuis la crise de 2008, les banques doivent disposer d'actifs hautement liquides à l'actif de leur bilan. Ces actifs doivent lui permettre de générer très rapidement des liquidités en cas de problème sur les marchés. Habituellement, ces actifs sont composés d'obligations d'états de courte durée. Plutôt que de vendre les positions, JP Morgan propose de les tokéniser. Les tokens servent ensuite de collatéraux permettant à la banque d'emprunter à très court terme.

Le tout est encadré par des contrats intelligents qui vérifient la structure bilantaire et la capacité de remboursement de la banque *(Maire, 2022).*

2.4. La blockchain comme nouvelle économie numérique décentralisée

La blockchain pourrait permettre l'émergence d'une économie plus décentralisée.

Aujourd'hui, un grand nombre de secteurs sont détenus par une poignée d'entreprises centralisées. Si l'on prend l'exemple du web, la majorité du secteur est contrôlé par des géants comme Google, Méta (réseaux sociaux), Amazon (ventes en ligne), …

Le lancement et le développement d'une activité de commerce en ligne sont totalement dépendants de ces géants. Si Google ne référence pas votre site, vous n'aurez aucune visibilité. Si Amazon souhaite développer une gamme propre d'un produit que vous commercialisez, il peut bloquer la vente de votre produit via son site.

Décentraliser ces géants permettrait d'éviter la censure, la vente de données, les modifications de conditions d'utilisations soudaines, … *(Berné, 2020).*

3. Les faiblesses de la technologie

La technologie blockchain présente des avantages certains. Cependant, l'adoption et l'exploitation d'une nouvelle technologie dépendent également de la gestion appropriée des risques associés à celle-ci. Une étude de ses inconvénients et de ses risques majeurs s'impose donc.

3.1. La blockchain, une technologie nouvelle et complexe

La première application concrète de la blockchain date de 2009 avec l'introduction du Bitcoin. Il faut cependant attendre les années 2016-2017 avant de voir un intérêt grandissant pour la technologie et une diversification des projets *(Deloitte, 2018)*. C'est donc, une technologie très récente que peu de personnes ne maitrisent encore.

Les formations permettant de développer les compétences techniques requises sont encore peu existantes en Europe. Certaines utilisations et applications de la technologie demandent des connaissances spécifiques. Par exemple, la programmation des contrats intelligents se fait via un langage de programmation propre appelé Solidity. Les profils qualifiés pour développer la technologie au sein des entreprises se font donc rares et sont difficiles à trouver.

De par son caractère immuable, il est essentiel de faire attention à ce que nous déployons sur une blockchain. Les informations personnelles des utilisateurs stockées sur une blockchain ne pourront plus être supprimées. Il en est de même pour les contrats intelligents déployés par des entreprises et exécutant des tâches automatiquement. Ceux-ci représentent généralement les points les plus vulnérables aux cyberattaques et aux défaillances technologiques. Les contrats intelligents nécessitent des tests robustes et des contrôles adéquats pour atténuer les risques potentiels des processus commerciaux basés sur la blockchain *(Deloitte, 2017)*. Certains d'entre eux sont dotés d'une « kill function » permettant leur désactivation post-déploiement. Il est cependant important de notifier que cela ne supprime pas le contrat, celui-ci reste stocké sur une blockchain. Cela permet simplement d'interrompre son fonctionnement *(Chen et al., 2020)*.

Bien qu'au travers des crypto-monnaies et de certains NFT la technologie commence à se démocratiser, son utilisation est encore réservée aux quelques initiés. Il faudra plusieurs années avant que le grand public commence à l'utiliser. Les outils disponibles ne permettent pas encore d'avoir une expérience client suffisamment simplifiée.

Finalement, les utilisateurs sont seuls responsables. Il n'est pas question d'appeler une entité centralisée afin de récupérer ou de réinitialiser une clé privée. Or, nous avons vu que cette clé privée leur garantit l'accès à la blockchain. Une clé privée perdue équivaut à une perte totale et définitive des actifs qu'elle contenait. Un transfert envoyé à une mauvaise adresse est également définitif. Les plateformes permettent dans certains cas de garder la clé privée pour leurs utilisateurs. Cette pratique peut cependant engendrer des conflits avec la sécurité et la décentralisation qu'apporte la technologie blockchain *(Robin Berné, 2020)*.

3.2. La blockchain, une technologie inefficiente

La technologie ne cherche pas à être efficace, son rôle est d'assurer la sécurité et la transparence des données. Les blockchains (publiques et ouvertes) sont dites inefficientes pour plusieurs raisons.

Premièrement, bien que la désintermédiation qui résulte de l'utilisation de cette technologie accélère le traitement des opérations, son utilisation est encore aujourd'hui un frein pour les applications ayant besoin d'une réactivité instantanée. En effet, les différents protocoles de sécurité, tel que le cryptage, la propagation de l'information au réseau, les protocoles de consensus, demandent plus de temps pour traiter l'information que les méthodes centralisées traditionnelles. Par exemple, la blockchain Bitcoin peut en moyenne traiter 5 à 7 transactions par seconde alors que VISA peut en traiter plus de 1700 *(Georgiadis, 2019)*.

Deuxièmement, la technologie éprouve des difficultés quant à sa scalabilité. La scalabilité d'un produit est sa capacité à maintenir ses fonctionnalités et ses performances lorsque le nombre d'utilisateurs augmente. Le nombre de transactions pouvant être vérifiées et validées ainsi que la place dans les blocs étant limités, certaines surcharges du réseau peuvent apparaitre sur les blockchains les plus populaires. Les transactions prendront alors beaucoup de temps avant d'être réalisées.

Finalement, les protocoles de consensus et particulièrement la preuve de travail (PoW) sont inefficients. Lors du minage d'un bloc, un seul des mineurs verra son travail validé. Le travail de tous les autres mineurs sera donc gaspillé. La compétition étant rude, les mineurs essaient continuellement d'accroître leur puissance de calcul afin d'augmenter leurs chances de trouver un hachage de bloc valide. Cette course associée à l'inefficacité du protocole engendrent de lourdes répercussions énergétiques. Pour prendre un exemple, l'énergie nécessaire pour le fonctionnement du Bitcoin dépasserait la consommation en électricité de nombreux pays tel que l'Irlande, le Nigeria ou encore le Danemark *(Binance Academy, 2022)*.

Pour contrer cette inefficience certaines blockchains font un compromis sur les aspects de sécurité ou les aspects de décentralisation. Les processus de consensus peuvent également évoluer et, par exemple, passer d'un PoW énergivore vers à un PoS plus économe.

3.3. La blockchain, une technologie volumineuse

Au fil du temps, l'historique des transactions enregistrées dans une blockchain s'allonge. Le registre de la blockchain contient dès lors de plus en plus de données. Il devient plus volumineux. Lorsque la taille du registre excède la capacité de certains disques durs, les nœuds concernés se verraient exclus du réseau n'étant plus capable de télécharger et de stocker le registre. Cela a pour effet de réduire le nombre de nœuds et donc de réduire la décentralisation propre à cette technologie.

3.4. La blockchain, une technologie qui présente des risques de cybersécurité

La technologie blockchain est l'une, voire la plus sécurisée du monde aujourd'hui. Cependant, comme toute technologie, celle-ci présente certaines failles.

Une étude complète des risques liés à la technologie a été publiée en 2020 par des chercheurs de l'université de St Pölten en Autriche *(Köning et al.)*. Les risques ont été cartographiés et regroupés en 4 catégories :

- Blockchain structure vulnerabilities : regroupe les risques liés à l'enchainement des blocs.
- Attacks on the consensus mechanism : regroupe les attaques visant à corrompre les protocoles de consensus.
- Attacks on the peer-to-peer system : regroupe de nouveaux risques liés au caractère pair à pair de la technologie.
- Application oriented attacks : nous avons vu que la technologie pouvait être utilisée pour différentes applications. Cette section regroupe les risques propres à ces applications (exemple : les risques spécifiques au minage de cryptomonnaies).

Figure 32 : Synthèse des différentes attaques possibles sur la technologie blockchain, Köning et al. 2020

L'objet de ce mémoire, n'est pas de réaliser une étude complète de ces risques. Nous nous limiterons dès lors à illustrer les principaux risques :

- Vol d'identité : sur une blockchain, les utilisateurs sont définis par leur clé privée. Le vol de celle-ci permet à l'attaquant de prendre le contrôle de l'adresse du propriétaire et de signer des transactions frauduleuses.

- Attaque des interfaces extérieures : plusieurs entités extérieures communiquent directement avec la blockchain. Elles sont beaucoup plus vulnérables et donc sujettes aux attaques. Parmi ces interfaces nous retrouvons par exemple les oracles des contrats intelligents ou encore les plateformes d'échanges. Ces interfaces sont

attaquées pour déclencher des conditions de contrat, voler des clés privées qui y seraient stockées, …

- Qualité du code des contrats intelligents : tous les programmes informatiques sont susceptibles de contenir des erreurs de programmation. Il en est de même pour les contrats intelligents . Il est très important d'accentuer les tests et vérifications avant leur diffusion sur la blockchain. Une fois diffusés, ces contrats ne seront plus modifiables et les erreurs de codage pourraient engendrer de véritables catastrophes *(Ben Taher, 2018)*.

- Attaques du réseau : l'attaque dite des 51%. Elle consiste pour un mineur ou un groupe de mineurs mal intentionnés à prendre le contrôle du réseau. Si une entité contrôle 51% ou plus des nœuds d'un réseau, alors elle détient le contrôle sur celui-ci. Ce faisant, elle peut modifier les données contenues dans le registre et effectuer des doubles dépenses *(IBM, 2022)*. Néanmoins, ce genre d'attaque est pratiquement infaisable et serait extrêmement coûteuse sur les réseaux volumineux.

3.5. La blockchain, une technologie qui pose des questions juridiques

Aujourd'hui, bien qu'il n'existe pas encore de droit spécifique à la technologie blockchain, il n'y a pas non plus de vide juridique *(Fénéron Plisson, 2017)*. A défaut d'un régime légal spécifique, les dispositions du cadre législatif existant sont censées s'appliquer. Cependant, la nature même de la technologie pose une série de questions quant à l'adéquation du cadre existant.

Ces questions dépendent naturellement des applications qui sont faites de la technologie. Ce mémoire traitant d'un sujet financier, nous listons ci-après une série de dispositions réglementaires et vérifions leur compatibilité avec la technologie de la blockchain :

- Les dispositions relatives au Règlement Général de la Protection des Données (RGPD) obligent le responsable du traitement des données à assurer leur sécurité. En cas de piratage ou de vol des données, quel acteur est responsable dans une technologie distribuée ? L'attribution de **la responsabilité** et l'obligation de rendre des comptes

sont compromises dans une technologie distribuée où certaines transactions se font de manière automatique *(Finck, 2019)*. Les DAO (Decentralized Autonomous Organization) permettent parfaitement d'illustrer cette problématique. Selon Blockchain France, 2016, « une DAO est une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans une blockchain ». Son fonctionnement se base sur l'utilisation de contrats intelligents. Ce type d'entreprise est donc totalement automatisée et autonome. Il est ainsi pratiquement impossible de trouver un responsable de l'entreprise.

Plus généralement, le RGDP consacre une série de droits, comme le **droit à l'effacement** des informations tel que prévu à l'article 17, le **droit d'opposition de traitement** prévu à l'article 21 ou encore le **droit de rectification** prévu à l'article 16. Le caractère immuable des données enregistrées dans la blockchain complique clairement la mise en œuvre de ces droits.

Une piste de solution pour le droit à la rectification serait de mettre à jour l'information en l'inscrivant sur un nouveau bloc de la chaine. L'état de la précédente donnée pourrait ainsi être modifié sans modifier l'historique du registre.

Concernant le droit à l'effacement, il est plus complexe de trouver de véritable solution. Il est en effet impossible d'effacer totalement l'information. L'unique solution permettant de s'en rapprocher serait la possibilité de cacher ou de permissionner la lecture de celle-ci au moyen de la cryptographie *(Elkaim,2021)*.

- Les dispositions légales relatives à la **lutte contre le blanchiment d'argent et le financement du terrorisme** (AML) et les dispositions relatives à la **connaissance des activités des clients** (KYC) ne sont pas compatibles avec le caractère anonyme à l'origine de la technologie. Pour lutter contre ces problèmes, la commission des affaires économiques et monétaires du parlement européen (ECON), a proposé d'étendre l'application des lois existantes relatives aux transferts de fonds (Transfer of Funds Regulation, TFR) aux transactions en crypto-actifs. L'objectif est d'arriver à une certaine surveillance, par des services régulés, de la nature des transferts et des détenteurs de fonds en crypto-actifs *(Commission Européenne, 2021)*.

- Le règlement MICA (Markets in Crypto-Assets) transpose les dispositions réglementaires de la finance traditionnelle, tels que MiFID (Markets in Financial Instruments Directive) ou abus de marché (MAR), aux spécificités du marché des crypto-actifs. L'objectif de ce règlement est d'établir un cadre juridique harmonisé permettant de soutenir l'innovation en offrant aux investisseurs un niveau approprié de protection. Cette protection permettrait de garantir une certaine stabilité financière et une concurrence loyale dans ce marché des crypto-actifs *(Schenk & Gineste, 2022).*

Le cadre législatif autour de cette technologie est donc en train de se développer petit à petit. Plusieurs initiatives nationales ou Européennes sont en cours de développement depuis 2016. Ces réglementations ont comme objectif de permettre aux consommateurs de tirer pleinement profit des avantages qu'apporte la technologie blockchain tout en les protégeant au mieux des risques et des attaques. Elles doivent également s'assurer que l'innovation autour de la technologie blockchain ne soit pas prématurément bridée *(Ben Taher, 2018)*.

A titre d'exemple, début 2023, une initiative réglementaire européenne nommée «Régime Pilote DLT» entrera en vigueur (DLT pour Distributed Ledger Technology, en français, technologie des registres distribués). Il permettra aux entreprises voulant développer des produits et des services basés sur la technologie blockchain d'être exemptées des législations financières traditionnelles. Ces exemptions seront octroyées par les autorités nationales sous condition, notamment, de volume d'activités et pour une durée maximale de 6 ans *(Ernotte, 2022)*.

PARTIE II : LA BLOCKCHAIN DANS LE SECTEUR DE L'ASSURANCE

1. Etat des lieux du secteur de l'assurance en Belgique et en Europe

Pour introduire cette deuxième partie du mémoire, nous allons évoquer le poids du secteur de l'assurance dans l'économie belge et européenne.

L'activité du secteur consiste à proposer une couverture d'assurance en contrepartie de l'encaissement d'une prime. Il existe deux catégories de contrats :

- Les contrats d'assurance-vie : l'assurance vie est un produit d'épargne et/ou d'investissement. Elle permet aussi de couvrir le risque de décès. Le versement du capital est lié à un aléa à savoir, la survie ou le décès de la tête assurée.
    - En cas de vie à l'échéance du contrat, l'épargne est versée au bénéficiaire vie (ex : assurance pension).
    - En cas de décès, le capital, épargne ou sous risque, est versé au bénéficiaire décès identifié dans le contrat.
- Les contrats d'assurance non-vie : cette catégorie regroupe toutes les assurances qui ne sont pas directement liées à la vie de l'assuré : les assurances de responsabilité, de dommages et de personnes (ex : habitation, santé, accidents, automobile, …).

En 2020, selon une étude menée par Assuralia, les assureurs belges ont récolté des primes pour un montant total de 28,5 milliards d'euros. La branche vie a généré 15,5 milliards d'euros et la branche non-vie 13 milliards d'euros. Le PIB belge de l'année 2020 s'élève à 457milliards d'euro *(Countryeconomy, 2022)*. En 2020, les primes générées par le secteur de l'assurance représentent donc plus de 6% du PIB belge.

Cette même année, en Europe, les contrats d'assurance non-vie ont produit des primes s'élevant à 592 milliards d'euros. Les contrats d'assurance vie ont généré 668 milliards d'euros. Le montant total des primes engendrées par le secteur assurantiel européen s'élève à 1264 milliards d'euros (Insurance europe, 2022). Le PIB européen de 2020 est d'environ

17.900 milliard d'euros *(Wikipedia, 2021)*. Le secteur de l'assurance représente donc 7% du PIB au niveau européen.

Le tableau ci-dessous reprend les chiffres clefs du secteur de l'assurance en Belgique et en Europe (en ce compris le Royaume-Unis) en 2020.

	Prime 2020 (en milliard d'euros)	
	Belgique	Europe
Total Non-vie	12,9	592
Total vie	15,6	668
Total Non-vie et vie	28,5	1264
PIB	456,7	17.900
Total primes / PIB	6,24%	7,06%

Figure 17 : Chiffres clefs du secteur de l'assurance

Fin 2020 en Belgique, les assureurs vie gèrent des actifs pour un montant de 282 milliards d'euros *(Assuralia, 2021)*. Selon Insurance europe, le secteur de l'assurance est le plus grand investisseur institutionnel en Europe. En 2020, Il représente plus de 10.600 milliards d'euros en actif sous gestion investis dans l'économie.

Pour commercialiser leurs produits, les compagnies d'assurances font appel à différents réseaux de distribution. Les assureurs proposent leurs contrats soit en direct, sans intermédiaire, soit via d'autres canaux de distribution tels que les courtiers, la bancassurance et les agents. L'utilisation de ces canaux peut être différente selon les marchés et s'adapte aux préférences du consommateur.

En Belgique :

Nous devons faire la distinction entre les branches vie et non-vie. En assurance non-vie, nous pouvons constater que même si la part du courtage reste prépondérante, la distribution directe progresse et se place en deuxième position. Ce qui laisse suggérer qu'un système de distribution et de souscription via la technologie blockchain devrait être reçu positivement par les consommateurs.

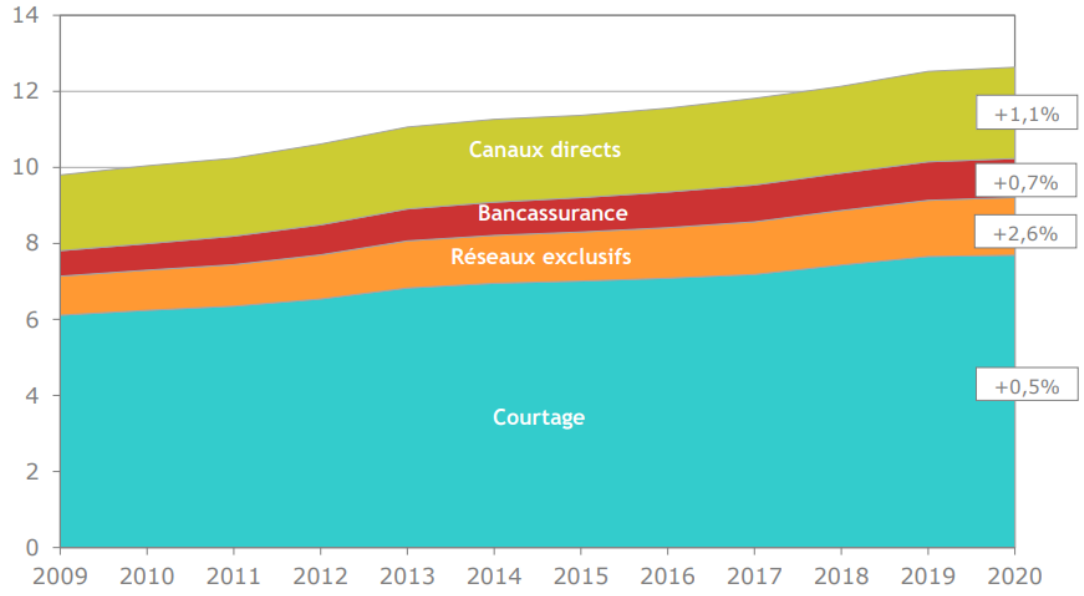


Figure 18 : Evolution des encaissements non-vie belge selon les principaux mode de distribution (en milliards d'euros), Assuralia 2021.

En encaissement vie, seul l'encaissement du courtage progresse. Les réseaux exclusifs et de bancassurance présente un recul significatif, probablement lié à la diminution du nombre d'agences en Belgique. La part du direct reste relativement constante. Cela démontre que les produits proposés en assurance vie nécessitent une approche basée sur le conseil.

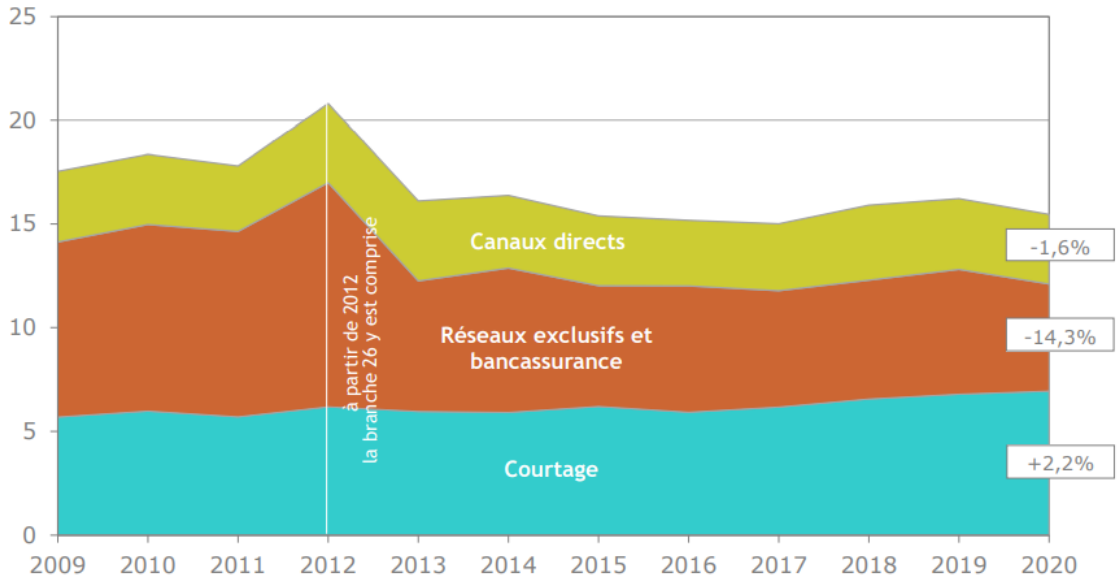


Figure 19 : Evolution des encaissements vie belge selon les principaux mode de distribution (en milliards d'euros), Assuralia 2021.

L'analyse des réseaux de distribution au niveau européen nous appelle à rester prudents dans nos conclusions. En effet, les graphiques ci-dessous qui présentent la part des réseaux de

distribution en vie et non-vie, démontrent une grande diversité dans les approches commerciales. La Belgique qui présente une part significative de sa distribution via le courtage semble être une exception.

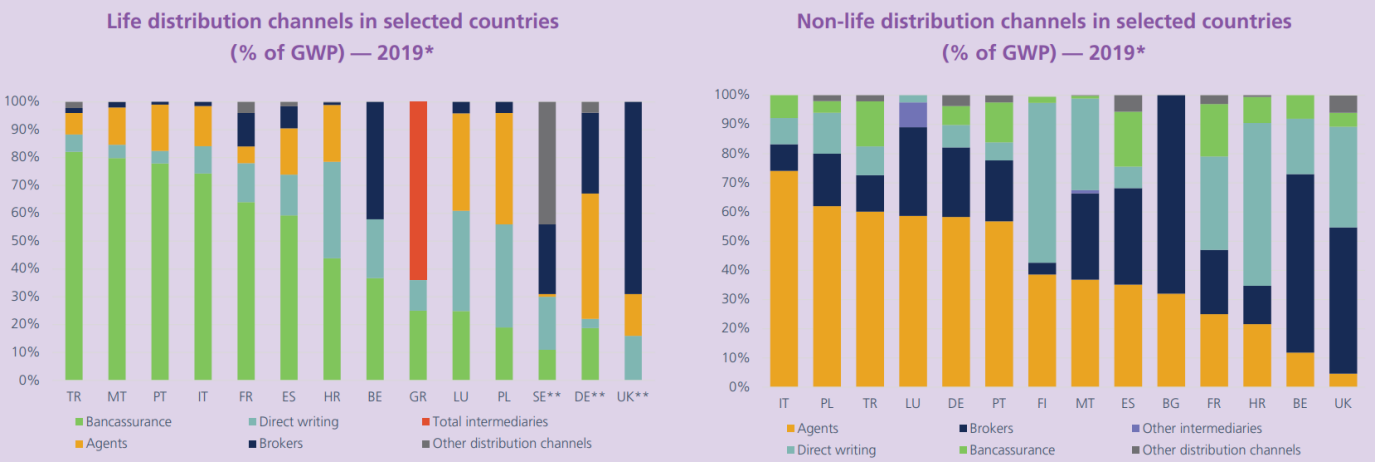


Figure 20 : représentation de la part des réseaux de distribution en vie et non-vie des marchés européens, insurance europe (2022)

2. Quelques domaines d'application de la technologie blockchain appliquée au secteur de l'assurance

Nous avons vu dans la première partie de ce mémoire que la technologie blockchain présente des avantages indéniables. Dans le secteur de l'assurance, cette technologie a le potentiel d'augmenter l'efficacité des processus ainsi que la collaboration entre les acteurs du secteur. Ces améliorations permettent notamment de lutter contre la fraude et la cybercriminalité, défis majeurs du secteur.

En plus de l'amélioration et de l'optimisation des processus fonctionnels existants, la technologie permet d'aborder l'assurance sous un autre angle. Nous pensons par exemple, au développement de l'assurance pair-à-pair[3].

L'objectif de cette section est d'identifier, au moyen des différentes sources académiques existantes, les applications potentielles de la technologie blockchain dans le secteur de l'assurance. Pour ces applications, des exemples de mise en œuvre pratiques seront fournis.

[3] Les assurances pair-à-pair peuvent être définies comme un réseau d'individus, ayant des intérêts communs, qui regroupent leurs primes pour assurer un risque (European Insurance and Occupational Pensions Authority, 2019).

2.1. Réduction des coûts et optimisation de la gestion

Plusieurs utilisations de la technologie blockchain permettent une réduction des coûts.

Via les contrats intelligents, les coûts opérationnels et administratifs peuvent être diminués par une automatisation des tâches et des processus liés à la gestion des sinistres.

La création d'un registre commun permet également la réduction des coûts par un accès simplifié aux données des clients. Cet accès simplifié facilite l'intégration des données dans les plateformes de souscription des contrats. Il permet également de répondre aux obligations légales (AML, KYC).

Finalement, la traçabilité offerte par la technologie diminue les fraudes et améliore la segmentation des risques clients.

Ces réductions de coûts ne sont pas uniquement bénéfiques pour les assureurs. Les primes payées par les clients sont directement impactées par ces économies et sont donc réduites.

2.1.1. Automatisation de la gestion sinistres

Une étude d'IBM rédigée par Shyam Kumar Yerramsetti en 2018 compare la gestion sinistre actuelle avec une gestion sinistre basée sur la technologie blockchain.

Le schéma ci-dessous illustre les difficultés rencontrées dans la gestion sinistre actuelle.

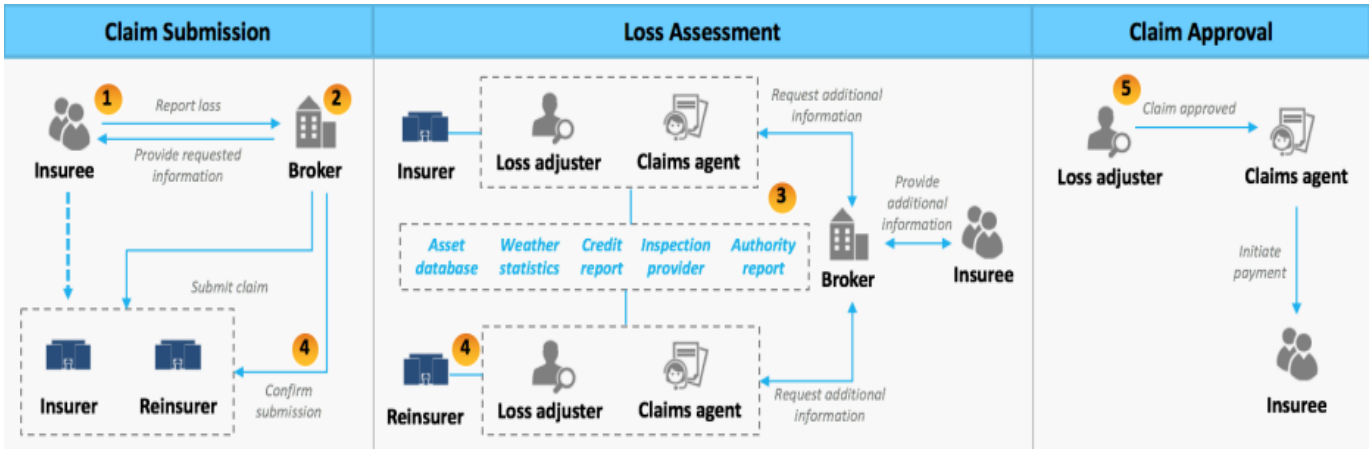


Figure 21 : les Difficultés rencontrées dans la gestion sinistre actuelle, IBM 2018i

1. L'expérience client est insatisfaisante : la procédure d'indemnisation est fastidieuse et demande un travail important pour le client (initier la demande, remplir des questionnaires, garder les preuves de dommages, …).
2. Présence d'intermédiaires : les intermédiaires, les courtiers et les agents augmentent les coûts et ralentissent le processus de règlement.
3. Difficulté d'accès aux données : les données nécessaires sont réparties entre différentes bases de données chez des tiers. Les compagnies doivent alors entrer en contact et demander un accès manuel à ces informations.
4. Manque de collaboration entre les compagnies : cela engendre des pertes et des fraudes potentielles.
5. Manque d'automatisation dans les indemnisations : les experts et les gestionnaires sinistres doivent encore réaliser manuellement de nombreuses tâches.

La technologie blockchain permet via les contrats intelligents d'automatiser les demandes et la gestion des indemnisations. En supprimant les interventions humaines, cette automatisation va réduire le temps nécessaire et les coûts liés à ces processus.

Pour rappel, les contrats intelligents permettent le déclanchement automatique de contrats, d'évènements lorsque des conditions sont remplies. Les conditions d'un produit assurantiel peuvent ainsi être écrites dans un contrat intelligent qui, lorsque les paramètres sont remplis, verse automatiquement les indemnités *(Popovic, et al., 2020)*.

Les compagnies d'assurance pourraient par exemple automatiser leurs assurances auto. En cas de dommage, si le client répare sa voiture dans un atelier de mécanique certifié, les fonds nécessaires au dédommagement des dégâts pourraient être débloqués de manière automatique. Les garagistes certifiés servent ici d'oracle afin de déclencher les contrats présents dans la blockchain.

Les objets connectés peuvent également être d'une grande utilité. Nous pouvons imaginer des capteurs dans les toits de maison, dans les voitures, dans des champs de culture, etc. Les informations relevées par ces différents objets connectés seraient stockées dans une blockchain et pourraient ainsi alimenter les paramètres d'un contrat intelligent. En cas

d'accident de voiture ou de sécheresse dans les champs, les assurances seraient déclenchées sans intervention humaine et les indemnisations seraient versées.

Le schéma ci-dessous illustre le fonctionnement d'une gestion sinistre basée sur la technologie blockchain.

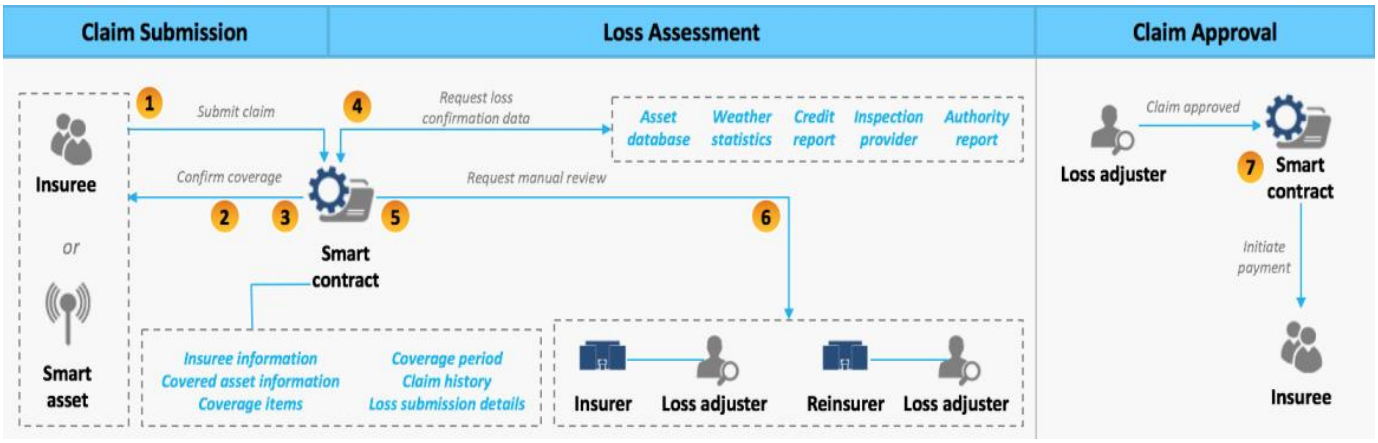


Figure 22 : Une gestion sinistre basée sur la technologie blockchain, IBM 2018

1. Le déclenchement du processus d'indemnisation peut se faire manuellement par le client ou de manière automatique par des objets connectés ou via des oracles dans les contrats intelligents.
2. Les assurés reçoivent automatiquement une confirmation quant à l'intervention ou non du contrat.
3. Les vérifications préalables des réclamations de sinistre peuvent être automatisées dans les contrat intelligents en fonction des critères de l'assureur.
4. Les contrats intelligents vont rechercher automatiquement les données disponibles dans les sources internes et externes afin d'évaluer la demande ou de calculer les pertes.
5. Pour les contrats souscrits via un régime de co-assurance (couverture partagée entre plusieurs assureurs), la répartition du coût peut être gérée par un contrat intelligent.
6. Pour certains cas spécifiques, une validation humaine comme décision finale peut être nécessaire et programmée.
7. Si la demande d'indemnisation est validée, celle-ci s'effectue automatiquement via le contrat intelligent.

A titre d'exemple, nous pouvons citer l'assurance paramétrique mise sur le marché par Axa, Fizzy. Elle prévoit une indemnisation en cas de retard aérien. Une assurance paramétrique est une assurance forfaitaire qui est déclenchée automatiquement lorsque certaines conditions définies en amont sont avérées *(Pengloan, 2020)*.

Après avoir acheté son billet d'avion, le client peut opter pour l'assurance Fizzy. Il y souscrit en rentrant ses informations personnelles et les informations sur son vol dans une application décentralisée[4] (dApp). Le contrat est scellé dès que celui-ci paie la prime. Les données nécessaires au fonctionnement du contrat intelligent Fizzy sont fournies par un oracle connecté aux bases de données des compagnies aériennes. Dans le cas où le vol du client a plus de 45 minutes de retard, le contrat intelligent lui rembourse automatiquement une somme forfaitaire prédéfinie *(AXA, 2017)*.

Ces solutions sont bénéfiques à la fois pour les clients et pour les assureurs. Les clients gagnent un temps précieux sur le temps de traitement des indemnisations. Il leur est également plus facile de comprendre les conditions et les champs d'application des contrats. L'automatisation nécessite en effet une expression claire et précise des conditions du contrat dans le code des contrats intelligents. Il leur est ainsi plus facile de comparer différentes polices d'assurance avant de signer un contrat. De leur côté, les compagnies d'assurance réduisent les interactions humaines et donc leurs coûts *(Kar & Navin, 2020)*.

2.1.2. Identité digitale

La technologie blockchain permet la création par plusieurs acteurs d'un écosystème de registres sécurisés et distribués. Il est ainsi possible de rassembler les différentes informations concernant une entité ou un client au sein d'un registre partagé.

Dans le secteur de l'assurance, un registre rassemblant les informations des clients peut trouver son utilité. Un système de vérification d'identité basé sur la technologie blockchain pourrait réduire la charge de saisie des données clients lors de la souscription des contrats.

[4] Une application décentralisée est une application déployée sur une blockchain. Pour plus d'informations, veuillez consulter le lien suivant : Qu'est-ce qu'une application décentralisée (DApp) ? (blockchainfrance.net).

Pour mettre en place ce système, les clients devraient préalablement se créer une identité digitale. Celle-ci serait vérifiée par des intermédiaires certifiés qui lieraient cette identité à une adresse sur la blockchain. Les clients implémenteraient leur identité digitale et donc la blockchain par des informations personnelles cryptées. Celles-ci pourraient ensuite être partagées au moyen de contrat intelligent avec les assureurs. Ces informations ayant été vérifiées au moins une fois et la blockchain étant une technologie immuable, les assureurs pourraient récupérer ces données sans avoir à refaire toutes les vérifications les concernant.

Dans un scénario plus poussé, des informations supplémentaires pourraient être stockées par des acteurs compétents (examens de santé, fiche de salaire, possession d'actifs, etc.) *(Gatteschi et al., 2018)*.

Cette application de la technologie pourrait également simplifier les obligations légales telles que celles liées aux réglementations « know your customer » ou encore « Anti-Money Laundering». L'obligation de constituer une documentation sur les clients et sur les parties prenantes est en effet un processus coûteux pour les entreprises. Aujourd'hui, par manque de base de données commune, chaque entreprise se voit obliger de constituer ses propres documents pour chaque client. Les informations clients sont centralisées dans les entreprises. Cette centralisation et cette démultiplication des informations les rendent très vulnérables aux cyberattaques. Ces dernières années, le nombre de cyberattaques est en hausse et, avec lui, le vol de millions de données personnelles des clients. Selon le rapport annuel 2021 d'Assuralia, la cybersécurité est un réel défi pour le secteur de l'assurance. L'utilisation de la technologie blockchain permet à ces entreprises de créer un registre de données unique. Les données ne sont plus stockées de manière centralisées et celles-ci sont sécurisées par des processus de cryptage *(PwC, 2017)*. L'intégration d'un client s'en retrouve simplifiée. Lorsque le client souhaite changer d'assureur, il suffira à ce dernier de demander un accès à la documentation déjà présente et vérifiée sur la blockchain *(European Insurance and Occupational Pensions Authority, 2021)*.

Finalement, la mise en place de ce registre permettrait aux clients d'avoir un contrôle accru sur leurs données personnelles et sur les entités à qui celles-ci sont partagées *(Popovic, et al.,*

2020). Les clients bénéficieront donc d'un meilleur service, les erreurs humaines seront diminuées et les coûts seront réduits.

A titre d'exemple, l'entreprise Civic[5] a développé un protocole de **vérification d'identité** personnelle utilisant la technologie blockchain. Pour assurer à ses clients le contrôle de leurs données personnelles, l'entreprise ne les conserve pas directement sur la blockchain. Elle émet et conserve des attestations qui sont en réalité un hash des informations qu'elle a préalablement authentifiées *(Civic, 2017 ; Actualité Informatique, n.d.).*

Le réseau Civic est composé de 3 acteurs interdépendants :

- Les clients privés qui utilisent le protocole pour certifier leurs données d'identité
- Les validateurs de l'entreprise qui authentifient les identités.
- Les entreprises qui ont besoin de vérifier l'identité de leurs clients. Après paiement en cryptomonnaie CVC (Civic), elles pourront accéder au hash généré par Civic. En comparant ce hash au hash qu'elles auront-elles mêmes généré sur base des données reçues de leur client, elles pourront conclure à la validité de ces données sans devoir elles-mêmes s'assurer de leur authenticité.

2.1.3. Evaluation des risques et prévention de la fraude

Selon le Comité européen des assurances, 5 à 10 % du montant total des indemnités versées en assurance sur les marchés européens représenteraient de la fraude à l'assurance. En Belgique, cela signifierait que la fraude s'élève au minimum à 250 millions d'euros par an. Cette fraude engendre une augmentation des primes de 60 à 125 euros par an et par ménage *(Assuralia, n.d.)*.

Les registres proposés par la technologie blockchain peuvent aider les compagnies d'assurance dans cette lutte contre la fraude et dans l'évaluation des risques. La technologie est utilisée pour permettre à plusieurs intermédiaires certifiés d'enregistrer des informations

[5] Smith & Lingham, 2017 : Civic - White Paper (draft)3-4.indd

relatives à une personne *(Gatteschi et al., 2018).* Ces intermédiaires peuvent être des compagnies d'assurances (pour enregistrer les contrats et indemnisations précédents), des médecins (pour fournir les informations sur l'état de santé), des forces de l'ordre (pour informer d'un casier judiciaire), etc. En combinant cette base de données partagée avec des contrats intelligents pouvant lire les informations qui y sont stockées, il est possible de calculer automatiquement le profil de risque d'un individu. Il permettra ensuite de calculer une prime personnalisée basée sur les informations disponibles sur le client, notamment, son état de santé ainsi que ses précédents sinistres enregistrés *(Kar & Navin, 2020)*.

La lecture de cette base de données permet également de repérer certaines tentatives de fraude. Prenons l'exemple d'un client mal intentionné qui aurait souscrit à plusieurs assurances soins de santé dans des compagnies différentes. Celui-ci pourrait alors rentrer plusieurs demandes d'indemnisation sur base de ses factures médicales. Cette pratique est uniquement possible par manque de collaboration entre les acteurs du secteur de l'assurance.

Avec la technologie blockchain, les fraudes communes telles que celle précédemment évoquée ou encore les fraudes liées à une falsification des documents peuvent être évitées. La traçabilité, l'immuabilité et le partage du registre apportés par la technologie permettent aux assureurs de valider l'authenticité des contrats, d'identifier les demandes d'indemnisation double ou multiple, de vérifier l'identité de l'assuré, etc. *(Tarr, 2018).*

Les solutions présentées ci-dessus sont cependant difficilement réalisables aujourd'hui en Europe. Celles-ci nécessitent que chaque individu possède une adresse blockchain unique et qu'un grand nombre d'acteurs (assureurs, forces de l'ordre, médecins, garagistes, …) se coordonnent au sein d'une même solution. L'efficacité des solutions dépend en effet grandement de la qualité et de la quantité d'informations disponibles dans la blockchain.

Plusieurs régulations, notamment concernant les données personnelles et l'utilisation d'objets connectés, posent également problème dans l'application de ces utilisations. Une piste de solution concernant les données personnelles serait de permissionner leur accès. Seuls les acteurs ayant reçu l'autorisation par le client de consulter ses données personnelles y auraient accès.

Finalement, l'architecture la plus adaptée aux applications vues précédemment serait une blockchain consortium. Une blockchain consortium est une blockchain privée gérée par plusieurs acteurs. Ceux-ci déterminent qui peut soumettre des transactions ou accéder aux données *(IBM, n.d.)*. Ces acteurs gestionnaires pourraient être des compagnies d'assurance, des organismes publics, ou autre. Un nombre limité de nœuds de confiance augmenterait la sécurité et la confidentialité des solutions.

Malgré ces difficultés, certains projets existent déjà aujourd'hui.

Cardossier[6] est un dossier numérique basé sur la blockchain. Ce projet est le fruit de la collaboration de plusieurs partenaires dont l'assureur AXA, l'université de Zurich, le concessionnaire AMAG ainsi que le consultant et fournisseur de service informatique AdNovum.

L'objectif du projet est de créer une identité digitale pour chaque voiture. Toutes les informations pertinentes concernant la voiture allant de sa construction jusqu'à sa casse sont enregistrées dans une blockchain. Nous retrouvons par exemple dans ce dossier les changements de propriétaire, les différents entretiens de la voiture, un historique du kilométrage, etc. Un historique transparent et complet de la voiture peut ainsi être créé. Les fraudes comme le trucage du kilométrage moteur en seront grandement diminuées.

Plusieurs avantages évidents découlent de ce projet. Pour les acheteurs de seconde main, le registre et son historique leur permettent de connaitre en détail les informations concernant le produit qu'ils souhaitent acheter. Pour les vendeurs, ils leur permettent de démontrer la qualité d'entretien du produit dans l'optique d'une vente au-dessus du prix de marché. Pour les assureurs, ce dossier leur permet de connaitre l'état du produit à assurer, les précédents sinistres, les précédents assureurs, etc. *(Temperli, 2018 ; Cardossier, 2022)*.

[6] Plus d'informations sur cette entreprise au lien suivant : Managing the lifecycle of a car with blockchain technology. – Cardossier

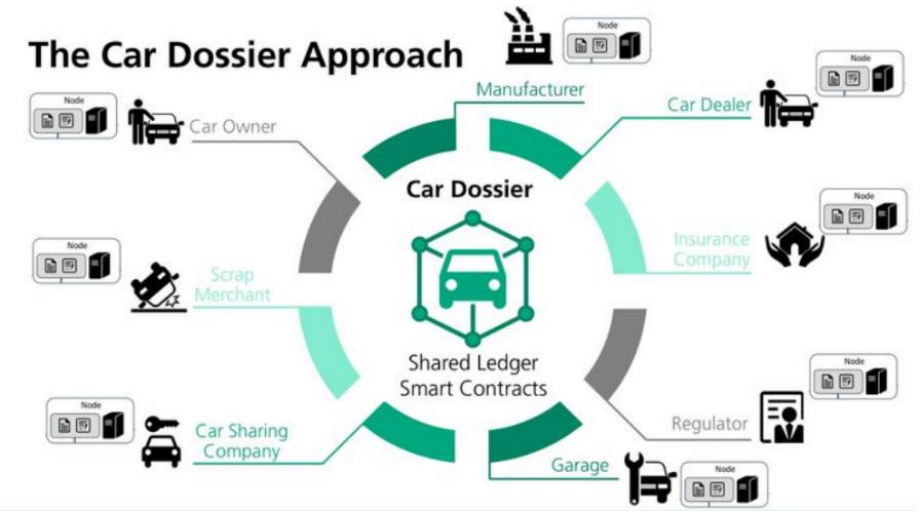


Figure 23 : Cardossier, Temperli 2018

2.1.4. Suppression des dépositaires

Nous avons vu au sein de la partie relative à l'état des lieux du secteur de l'assurance en Belgique et en Europe, que les assureurs y étaient les plus grands investisseurs institutionnels. Pour rappel, les actifs sous gestion de 2022 s'élèvent à 10 600 milliards d'euros.

Comme tout gestionnaire d'actifs, ils doivent se conformer aux règlementations d'application pour la conservation et l'échange des titres.

Pour se faire, ils font appel à un dépositaire. Le dépositaire assume trois fonctions *(ISIFI Conseil, 2022)* :

<u>La conservation</u>

Le rôle principal du dépositaire consiste à assurer le transfert de propriété d'un titre entre l'acheteur et le vendeur. Ce transfert se matérialise par l'échange simultané du titre contre des espèces. Ce processus est appelé le règlement – livraison.

Le dépositaire va également gérer toutes les opérations en relation directe avec la détention du titre. Nous parlons d'opérations sur titres. Sans que la liste ne soit exhaustive, il va gérer le paiement du dividende, les augmentations ou réductions de capital, les OPA, …

Le contrôle

Lorsqu'un gestionnaire d'actifs constitue un fonds (OPCVM, organisme de placements collectifs en valeurs mobilières) et le dépose en conservation auprès d'un dépositaire, ce dernier doit s'assurer que ses caractéristiques soient bien conformes au prospectus qui a été déposé auprès des autorités de marchés (la FSMA en Belgique). Les caractéristiques ont notamment trait à la nature des actifs en portefeuille, à la zone géographique ou au secteur couvert par le fonds, etc…

L'administration du fonds

Le dépositaire va prendre en charge une série de services administratifs pour compte du gestionnaire d'actifs.

Le schéma ci-dessous illustre le positionnement de l'assureur et les fonctions prises en charge par le dépositaire.

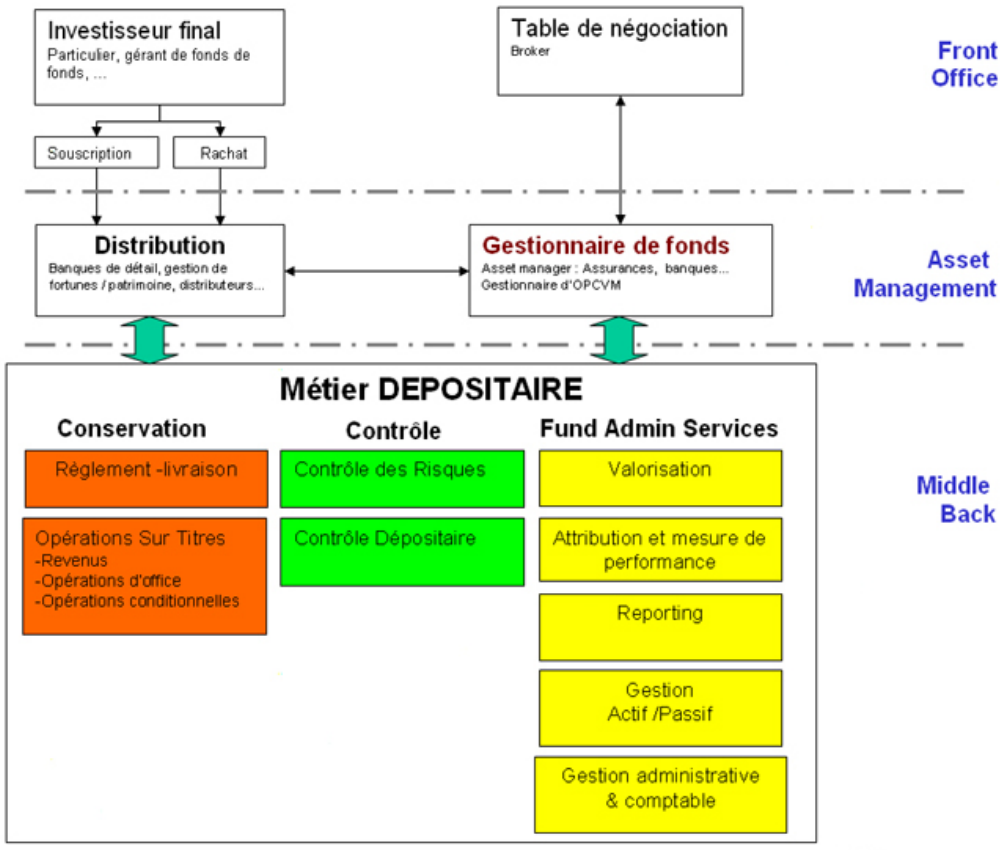


Figure 24 : Processus de règlement-livraison, ISIFI Conseil 2022

Le premier dépositaire est un intervenant local, habituellement une banque. Il va reporter ses opérations à un dépositaire central. La mission de ce dépositaire central est de vérifier en permanence que la somme des quantités détenues par chaque dépositaire local correspond à la totalité des titres émis. Il est donc chargé de la tenue du compte de l'émetteur des titres. Ces titres peuvent être des actions, des obligations ou tout autres titres négociables.

Il existe des dépositaires centraux nationaux qui eux-mêmes reportent à des dépositaires centraux internationaux. Aujourd'hui, il existe trois dépositaires centraux internationaux, Euroclear et Clearstream pour l'Europe et le Depository Trust & Clearing Corporation aux Etats Unis.

Le processus de règlement livraison des titres repose donc sur un gigantesque registre centralisé. La technologie de la blockchain qui est, au contraire, un registre distribué, devrait à terme pouvoir se substituer à ce processus. Les fonctions de conservation et d'administration des dépositaires pourraient ainsi progressivement disparaitre.

Les acteurs de la finance ont déjà intégré cette révolution à venir. Le 27 avril 2021, la BEI (Banque Européenne d'Investissement) a lancé, en collaboration avec Goldman Sachs, Santander et la Société Générale, une émission d'obligations numériques à l'aide de la technologie de la blockchain. L'objectif étant de « déployer la technologie des registres distribués pour l'enregistrement et le règlement des titres obligataires numériques » (*Banque Européenne d'investissement*, *2021).*

Outre l'aspect technique de la solution, l'aspect juridique doit également être pris en compte. La Commission européenne a proposé la création d'un cadre réglementaire transitoire destiné à tester la technologie des registres distribués dans les infrastructures de marchés. Ce cadre réglementaire est appelé « Régime Pilote ». Il devrait prendre effet en 2023 et sera d'application pour trois ans. Il pourra être renouvelé pour une nouvelle période de trois ans avant de donner lieu, si l'expérience est concluante, à un régime définitif (*Rocher, 2022)*.

Nous l'avons vu en introduction, les compagnies d'assurances sont des gestionnaires d'actifs très importants. Les économies qui résulteraient de l'implémentation de la technologie des registres distribués pourraient être significatives.

A titre d'illustration, lorsqu'un assureur vie branche 23 propose la création d'un fonds dédié comme support d'investissement, trois parties interviennent dans la mise en œuvre de la solution : l'assureur, le gestionnaire et la banque dépositaire. Habituellement les frais de fonctionnement de ces trois intervenants s'élèvent à +- 1% de l'encours sous gestion *(Guide-épargne, 2022)*. Les frais relatifs à la banque dépositaire s'élèvent à +- 0.10% *(Assurance Vie Luxembourg, 2022 ; indexa capital, 2021)*. La technologie des registres distribués permettrait ainsi une économie de 10% sur les frais appliqués aujourd'hui.

2.2. Création de nouveaux produits

Le développement de la blockchain et des contrats intelligents permet l'apparition ou la revalorisation de certains produits du monde de l'assurance.
L'amélioration de l'efficacité de certains processus rendus possible par les contrats intelligents permet à certains produits existants telles que l'assurance à l'utilisation ou la micro-assurance de se développer.
La décentralisation et le caractère « trustless » apportés par la technologie permettent également le développement de l'assurance pair-à-pair.

2.2.1. Assurance à l'utilisation - micro-assurance

Les micro-assurances ou les assurances à l'utilisation permettent aux compagnies d'assurance de proposer des produits dont le champ d'application est plus réduit ce qui engendre une prime réduite. Les primes payées par les clients pour ce type de produit étant très faibles, dans un système traditionnel, elles ne sont pas suffisantes pour compenser les coûts administratifs liés au traitement des indemnisations *(Kar & Navin, 2020)*. Ces produits n'étaient donc pas rentables et peu ou pas proposés par les assureurs.

Nous l'avons vu, la blockchain permet de réduire les coûts par une automatisation des processus. Les contrats intelligents vont faciliter la souscription et la gestion des contrats d'assurance. Des assurances plus personnalisables sont donc aujourd'hui envisageables. Grâce à la technologie, il est par exemple possible d'offrir des assurances que le client peut activer ou désactiver à tout moment. Dans le cas d'un Airbnb, le client pourrait activer son assurance uniquement lorsque celui-ci est loué.

L'ajout d'objets connectés peut augmenter les possibilités offertes par la technologie dans le domaine de la micro-assurance. Par exemple, en récupérant les données GPS d'une voiture, il est possible d'offrir des assurances pour lesquels les clients payeraient uniquement dans certaines régions ou uniquement lorsque la voiture est utilisée et donc en mouvement *(Gatteschi et al., 2018).*

La technologie ouvre la porte à un nouveau segment de marché, le marché « à la demande ». Elle permettra à certaines compagnies d'obtenir un avantage concurrentiel en proposant une multitude de nouveaux produits plus modulables.

Un cas pratique de ces assurances à l'utilisation est l'assurance auto proposé par Cuvva[7]. Elle permet à ses utilisateurs d'obtenir une couverture complète à court terme (d'1 heure à 28 jours) pour n'importe quel véhicule au Royaume-Unis. Imaginons que nous voulions emprunter le van d'un ami pour une aventure de quelques jours, ou, que nous partions en vacances en groupe dans une seule voiture, l'application Cuvva permet d'assurer un véhicule autre que le sien lorsque nous le conduisons. La voiture de notre ami sera dès lors couverte et ce dernier ne verra pas sa statistique sinistre impactée lors d'un accident occasionné par un tier.

Pour souscrire à l'assurance il suffit d'avoir un téléphone et de pouvoir télécharger l'application. La souscription se fait en 3 étapes *(Cuvva, n.d.; Huckstep, n.d.)*:

- Enregistrement : le client fournit son nom, adresse, date de naissance, une photo de son permis de conduire ainsi qu'un selfie.
- Devis: le client fournit le numéro de registre du véhicule et la valeur approximative de celui-ci.
- Lancement : la couverture commence lorsque le client choisit une durée de couverture. Il fournit une photo du véhicule (+plaque) pour prouver qu'il est en possession de celui-ci et autorise le payement de la prime.

[7] Plus d'informations sur cette entreprise au lien suivant :The Cuvva story: a better kind of insurance

Dans cette application, la technologie blockchain est utilisée pour stocker toutes les preuves, données fournies par le client et pour automatiser les processus de souscription à la police auto.

2.2.2. Assurance pair à pair

A l'origine, les assurances reposent sur une logique collectiviste. Un ensemble d'individus se protègent mutuellement contre de potentiels risques individuels *(Jérusalmy, 2018)*. Les assurances pair-à-pair peuvent être définies comme un réseau d'individus, ayant des intérêts communs, qui regroupent leurs primes pour assurer un risque *(European Insurance and Occupational Pensions Authority, 2019)*.

Aujourd'hui les compagnies d'assurances jouent le rôle d'intermédiaire pour cet ensemble d'individus. Nous avons vu que la technologie permettait de supprimer les intermédiaires. La technologie favorise la collaboration entre les individus sans que ceux-ci aient besoin de se faire confiance mutuellement. Des assurances dites pair-à-pair, sans intermédiaire, pourraient voir le jour.

Grâce aux contrats intelligents, il est possible de créer des entreprises, des organisations autonomes sur une blockchain. Ces entreprises sont appelées DAO (Decentralised Autonomous Organisation). Tout comme une entreprise traditionnelle est composée d'un ensemble de processus, les DAOs ont leurs processus automatisés et codés dans une blockchain au travers d'un contrat intelligent. Ces entreprises autonomes et décentralisées représentent le cadre idéal pour la création d'assurances pair-à-pair. Les règles de gouvernance des contrats d'assurances y seraient codées *(European Insurance and Occupational Pensions Authority, 2021)*.

Teambrella prétend être le premier cas concret d'assurance pair-à-pair basé sur la blockchain (via le réseau bitcoin). L'entreprise propose d'assurer la franchise d'assurance dommages (moto, auto, habitation).

Pour couvrir le montant des franchises, la communauté constitue un pot commun alimenté par les primes des membres du groupe. Les individus constituant un groupe peuvent être des

connaissances, qui se font confiance, mais également, grâce à la blockchain, des inconnus. L'historique sinistres des autres assurés peut être partagé de manière sécurisée et non falsifiable.

En cas de sinistre, les participants votent pour déterminer si le groupe accepte de prendre en charge la franchise d'un des membres.

Si, à la fin de la période, les sinistres ont été peu nombreux, la cagnotte restante est redistribuée aux individus l'ayant constituée *(Paperno et al., 2016; Hugh terry, 2017; Olivier Jérusalmy, 2018)*.

2.3. Réassurance

La réassurance est l'assurance des sociétés d'assurances *(Wikipédia, 2022)*. Au travers de la réassurance, un assureur se garantit lui-même contre le risque d'avoir à payer à ses assurés un sinistre trop important ou des sinistres en trop grand nombre *(CNRTL, 2012).*

Pour minimiser et répartir les risques, ces contrats de réassurance peuvent être partagés entre plusieurs acteurs. La prise en charge des sinistres peut par exemple être répartie en plusieurs couches, chacune prise en charge par un réassureur différent. Un réassureur A prendrait en charge les sinistres allant de 100 000 à 1M €, un réassureur B prendrait en charge ceux allant de 1M à 2M€ et ainsi de suite. Les primes payées à ces réassureurs seraient évidemment proportionnelles aux risques couverts.

Un courtier en réassurance intervient habituellement dans la mise en place de ces contrats. Il assure une bonne gestion des contrats entre les assureurs et leurs réassureurs. En cas de sinistres, il doit déterminer quel réassureur paiera les dommages et examiner si ces sinistres sont couverts par les termes du contrat *(Sayegh, 2018)*.

Tout comme pour les assurances classiques, les atouts de la technologie blockchain peuvent être appliqués à la gestion de la relation entre assureurs et réassureurs.

La gestion traditionnelle de la souscription des contrats et la gestion de l'indemnisation des sinistres par les réassureurs est lente. Le délai est principalement dû au nombre de parties intervenantes et à un manque d'automatisation. Nous avons déjà vu comment, via les contrats intelligents, la blockchain permet d'automatiser ces différents processus. Cette automatisation peut être appliquée dans le cadre des réassurances dites « traités » ou « obligatoires » qui ont des conditions d'application précises. Une automatisation des indemnisations trouverait notamment son utilité dans des situations de crise telles que des catastrophes naturelles, période dans lesquels des fonds doivent être débloqués très rapidement.

L'utilisation des registres décentralisés peut également faciliter le partage d'informations entre les assureurs et les réassureurs. Ces registres permettent d'avoir une trace immuable et horodatée de toutes les informations (sinistres, indemnisations, primes perçue, etc.). Les assureurs peuvent entrer les données via un contrat intelligent dans le registre. L'accès aux informations nécessaires contenues dans le registre peut ensuite être accordé en temps réel via ce contrat intelligent aux réassureurs, aux courtiers, aux régulateurs, etc. Les données comprises dans le registre peuvent être extraites de la blockchain pour des modélisations, des contrôles ou des audits automatisés.

L'automatisation des contrats et la traçabilité du registre pourraient permettre de réduire ou de supprimer le rôle du courtier qui agit comme un intermédiaire.

Finalement, l'une des principales forces de la technologie blockchain est sa capacité à favoriser la collaboration entre les acteurs. Elle permet via l'automatisation des processus et par la décentralisation des registres de faciliter la mise en place d'écosystèmes et d'entreprises communes.

Le consortium B3i[8] en est l'exemple parfait. B3i est une entreprise formée par plus de 21 grands assureurs (AXA, Aegon, Allianz, Achmea, Generali, …) et réassureurs mondiaux (Swiss Re, Africa Re, Deutsche Rück, Munich Re, …). L'entreprise a deux missions principales :

1. Créer le secteur de l'assurance de demain
2. Révolutionner la gestion de la réassurance

Pour réaliser ces objectifs, l'entreprise développe une infrastructure de réseau et une plateforme utilisant la blockchain. Ces outils vont permettre une automatisation des protocoles. Ceux-ci minimiseront voire supprimeront les besoins de gestion des produits et services assurantiels. Les dirigeants de B3i pensent que les nouvelles technologies peuvent faciliter et accélérer l'accès des clients à l'assurance. Ils pensent également que la collaboration est indispensable. Ensemble, ils pourront optimiser et automatiser les processus à l'échelle du marché. Ils généreront des économies de temps et de coûts significatives qui ne pourraient pas être réalisées par des acteurs individuels. Ils prévoient un gain de productivité pouvant atteindre les 30% *(B3i, 2022)*.

Depuis sa création en 2016, l'entreprise met en œuvre des outils et des expérimentations en lien avec la technologie blockchain.

L'outil principal crée par B3i est une plateforme, nommée Fluidity, basée sur la technologie Corda Distributed Legder (blockchain Corda). Elle regroupe assureurs, courtiers et réassureurs en leur fournissant une infrastructure de réseau (les nœuds peuvent être gérés par les clients de la plateforme) et un système de gestion de contrats intelligents.

Ce produit de B3i permet une automatisation de certains processus de (ré)assurance et une optimisation de la négociation des risques. Les acteurs de la plateforme se partagent le contrôle d'un registre dans lequel les données sont non seulement échangées mais aussi notariées et certifiées. Les informations du registre sont accessibles aux différents acteurs en

[8] Plus d'informations sur cette entreprise au lien suivant : Insolvency | Insurance Industry | B3i

gardant à l'esprit que cet accès est restreint et que seules les informations pertinentes pour l'acteur sont visibles pour lui.

Au travers de cette plateforme et du registre, les assureurs peuvent demander un devis de (ré)assurance en fournissant de manière cryptée des informations telles que la franchise, le taux, etc. Une fois un accord trouvé, le contrat est stocké dans un contrat intelligent. Lors d'un sinistre, le contrat calculera et effectuera les paiements aux parties affectées en fonction de son analyse des données des différentes parties *(B3i, n.d ; Cryptonaute, 2019)*.

Une fois la plateforme fonctionnelle, B3i a voulu tester ses capacités. La première application de la plateforme concerne une gestion des contrats de réassurance en cas de catastrophe naturelle, « Property Catastrophe Excess of Loss Reinsurance (Cat Xol) ». Le produit s'appelle B3i Cat Xol et permet aux acteurs du secteur de l'(ré)assurance d'interagir, de négocier et de placer des risques concernant les catastrophes naturelles de manière plus sûre et plus efficace.

Récemment, la plateforme s'est vue attribuée un nouveau défi. Six consortiums de (ré)assureurs nucléaires Européen (France, Allemagne, Espagne, Suisse, Royaume-Uni et les pays nordiques) ont engagé l'entreprise B3i dans l'objectif de développer une solution pour la gestion des contrats de réassurance. Les risques et les montants à assurer étant très élevés, une répartition de ceux-ci est nécessaire. Cela implique donc l'intervention de nombreux acteurs. La plateforme sera utilisée dans l'objectif de simplifier et gérer les accords entre ces multiples parties. Selon B3i, leur solution diminuerait les efforts administratifs et augmenterait la certitude contractuelle ainsi que la surveillance du portefeuille. De plus, le partage des données permettrait une amélioration de l'analyse des risques et des performances en matière d'audit et de conformité *(B3i, 2022).*

3. Proof of Concept

Au travers des précédentes parties de ce mémoire, nous avons vu de manière théorique les avantages et les cas d'utilisation de la blockchain. Cette partie-ci du mémoire sera consacrée à un approfondissement plus pratique des différentes notions qui composent la technologie blockchain. Pour se faire, nous analyserons un PoC (proof of concept) que j'ai réalisé avec l'aide d'un ingénieur d'intégration, Guillaume Braibant. Le projet, nommé Insurme, consiste à mettre en œuvre une application de souscription d'un contrat RC familial en ayant recours à la technologie de la blockchain.

3.1. Objectif du PoC

Un Proof of Concept (preuve de concept en français) ; est une réalisation dont l'objectif est de montrer la faisabilité d'une innovation *(Wikipédia, 2022)*. Dans notre cas, l'objectif du PoC est de démontrer que les différentes notions et avantages dont nous avons parlés tout au long de ce mémoire peuvent être appliqués de manière concrète. Nous verrons comment, au travers de contrats intelligents, il est possible de stocker des données sur une blockchain et d'automatiser une souscription de contrat.

3.2. Les difficultés rencontrées dans la souscription traditionnelle d'un contrat d'assurance

Les clients rencontrent les difficultés suivantes :

- Le processus de demande d'offres est répétitif et fastidieux : sauf s'ils s'adressent à un intermédiaire indépendant, les clients vont devoir remplir plusieurs questionnaires similaires auprès de compagnies différentes.
- La maitrise des données personnelles est insuffisante : une fois leurs données transmises, les clients n'ont plus un accès direct pour les modifier ou les effacer.
- La traçabilité des échanges est insuffisante : il n'existe pas de système qui permette de conserver l'historique des échanges et les contrats qui en résultent.

Les compagnies d'assurances rencontrent les difficultés suivantes :

- Manque d'automatisation : plusieurs tâches dans la souscription des contrats d'assurance sont encore réalisées manuellement.
- Manque d'accès aux données clients : certaines données telles que les données d'identité ou l'historique sinistres des clients sont compliquées à obtenir et à vérifier.

3.3. Insurme : une nouvelle façon de souscrire à un contrat d'assurance

3.3.1. Les acteurs de l'application

Les acteurs principaux de l'application sont les utilisateurs (clients) et les assureurs. Leurs rôles et leurs actions principales au sein de l'application sont repris dans le schéma ci-dessous.

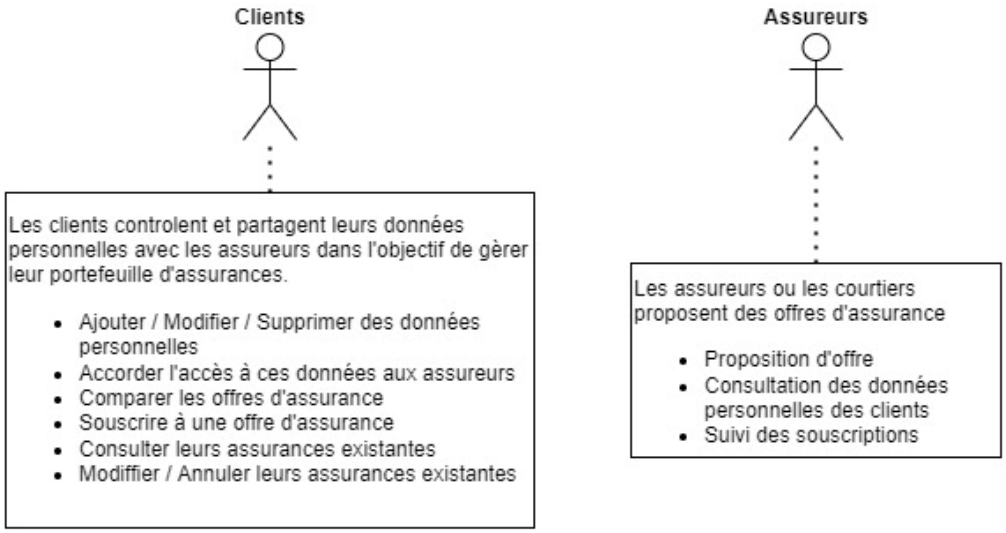


Figure 25 : Les acteurs de l'application

3.3.2. Fonctionnement de l'application

Dans un premier temps, l'application permet à ses utilisateurs de stocker leurs données personnelles dans une blockchain permissionnée. Elle permet également aux compagnies d'assurance de présenter la gamme des produits disponibles aux clients présents sur l'application.

Dans un deuxième temps, les utilisateurs vont pouvoir demander différentes offres d'assurance aux assureurs présents sur Insurme. Pour recevoir des offres adaptées à leur profil, les clients vont partager aux compagnies de leur choix les informations nécessaires les

concernant. Pour assurer aux utilisateurs un contrôle de leurs données personnelles, une gestion simple et sécurisée de celles-ci est intégrée dans l'application. Elle est composée d'un mécanisme d'autorisation d'accès aux données pour une activité et un délai précis.

Finalement, les clients vont pouvoir comparer les offres reçues et choisir celle qui leur convient. Ils vont alors signer le contrat et le faire parvenir à la compagnie d'assurances. Une fois un contrat conclu, tous les accès aux données accordés durant la phase de recherche d'offres sont automatiquement retirés aux autres compagnies d'assurance.

Le schéma ci-dessous illustre les interactions des utilisateurs et des assureurs avec les contrats intelligents formant l'application.

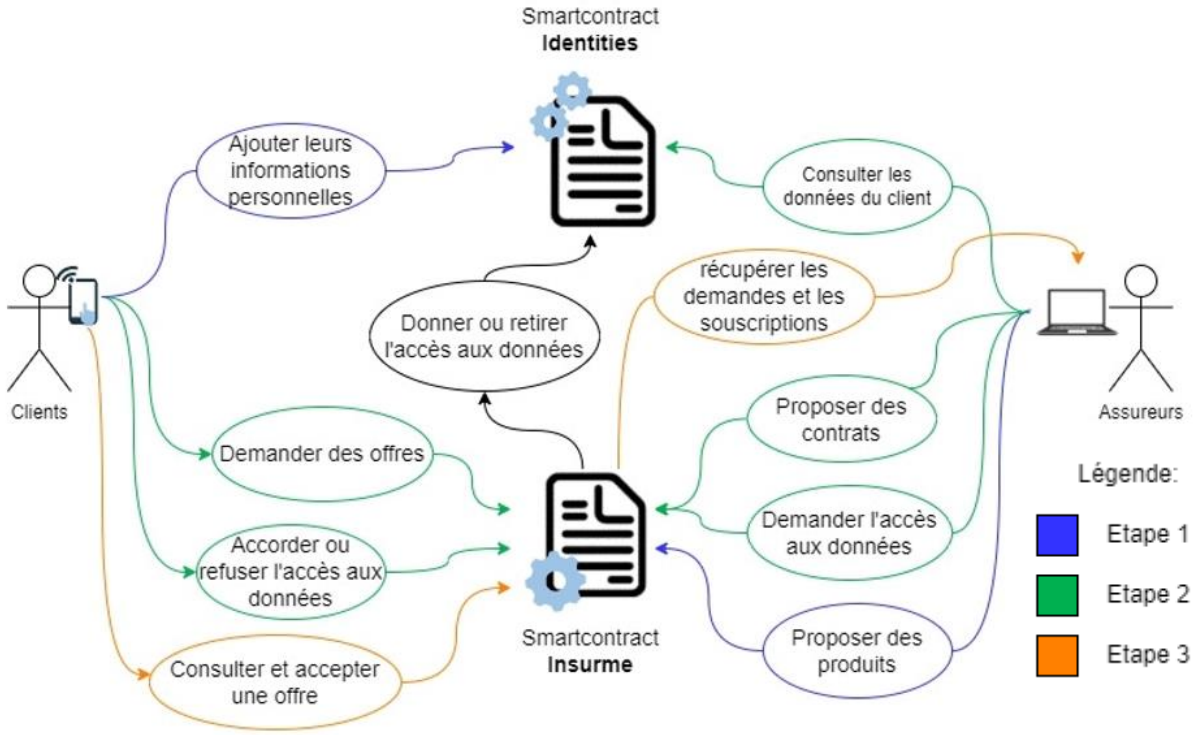


Figure 26 : Interactions avec les contrats intelligents

Le schéma nous montre que les contrats intelligents, ou « smart contracts », peuvent également interagir entre eux. L'application Insurme est composée de deux contrats intelligents. Le premier, nommé Identities, est responsable du stockage et du partage des données personnelles. Le deuxième, nommé Insurme, est le contrat intelligent principal de l'application. Il est chargé de gérer les processus de souscription du contrat d'assurance.

Les fonctionnalités liées à la gestion de l'identité peuvent être intéressantes dans le cadre d'autres applications. Il a donc été choisi de les mettre dans un contrat intelligent spécifique qui pourra être utilisé à la fois par celui chargé de gérer le processus de souscription mais également par d'autres contrats intelligents (réutilisabilité - extensibilité).

L'objectif de ce mémoire n'est pas de faire un compte rendu complet de la mise en œuvre et du fonctionnement de l'application. Pour le lecteur intéressé, nous développons en annexe les points suivants :

En annexe 1, nous détaillons la méthodologie utilisée pour la création de l'application.

En annexe 2 et 3, nous identifions et détaillons les fonctionnalités disponibles pour chaque acteur de l'application.

3.3.3. Démonstration

Commençons par identifier les éléments indispensables à la conception de notre proof-of-concept basé sur la technologie blockchain.

Pour développer l'application il nous a fallu :

- Une technologie blockchain : nous avons choisi d'utiliser la technologie Ethereum.
- Un réseau blockchain : nous avons choisi de créer une blockchain privée en raison du besoin de confidentialité des données personnelles. A cet effet, nous avons utilisé l'outil préexistant Settlemint.
- Un langage de programmation : nous avons utilisé Solidity.

Pour simplifier l'utilisation de notre application, il nous a fallu :

- Un portefeuille : nous avons choisi d'utiliser le portefeuille Metamask pour gérer le stockage des clefs publiques et privées. Il servira de compte pour les utilisateurs et facilitera leurs interactions avec l'application et la blockchain.
- Une interface web, user friendly, pour l'application : nous avons choisi la plateforme low code OutSystems pour nous aider dans cette tâche.

Les explications relatives à la technologie et aux outils utilisés ainsi que le fonctionnement de l'application par la visualisation des différents écrans se trouvent en annexe 4.

La démonstration permet d'illustrer le flux de souscription d'un contrat de RC familiale en ayant recours à la technologie blockchain. Plus spécifiquement, nous y découvrons :

- le fonctionnement pratique d'une blockchain : la démonstration met en lumière au travers d'exemples concrets les concepts théoriques liés à l'utilisation d'une blockchain. Nous y retrouvons des échanges de donnés, la signature de transactions au moyen d'une clef privée, la validation d'une offre, etc.
- le fonctionnement d'un contrat intelligent et la façon dont nous pouvons interagir avec ceux-ci.
- le fonctionnement des registres distribués proposés par la technologie blockchain : la blockchain utilisée dans l'application Insurme enregistre toutes les transactions entre les utilisateurs et/ou les contrats intelligents.
  En résumé, les transactions générées par le processus de souscription et inscrites de manière indélébile dans la blockchain comportent :
    - Les données personnelles du client et le produit pour lequel il souhaite recevoir une offre
    - Les demandes d'accès aux données clients soumises par les assureurs
    - Les approbations du client aux différentes demandes d'accès des assureurs
    - Les offres soumises par les assureurs
    - L'acceptation d'une offre par l'utilisateur

Pour une présentation plus dynamique de la démonstration, nous invitons le lecteur intéressé à visualiser la vidéo YouTube suivante : https://youtu.be/81GKXAdiQ0s

3.3.4. Avantages de l'utilisation de l'application

L'application présente plusieurs avantages. Elle permet :

- Une gestion simple et un partage efficace des données personnelles des clients via un contrat intelligent.
- Une souscription automatique des contrats d'assurance.
- Une simplification de l'expérience client dans la recherche et la souscription de contrat d'assurance.
- La création d'un historique assurantiel des clients dans la blockchain.
- Une traçabilité des contrats et des transactions.

Les objectifs évoqués en introduction de cette partie ont été remplis. Cependant, il est utile de préciser que nous sommes restés au stade expérimental du fonctionnement de l'application.

Elle n'a pas fait l'objet d'une phase de testing visant à identifier ses lacunes. Nous renvoyons le lecteur au point 3 de la partie 1 qui identifie les faiblesses et les points d'attention de la technologie blockchain.

Nous n'avons pas non plus réalisé d'analyse coût/bénéfice qui permettrait de valider la mise en production de cette approche.

Nous nous sommes limités à démontrer que la technologie pouvait être mise en œuvre pour souscrire un contrat d'assurance.

4. Enquête

Les avantages et cas d'utilisation théorique de la blockchain ont été traités. La faisabilité de certains d'entre eux a été démontrée au travers du PoC. Maintenant, confrontons ces résultats avec l'avis des acteurs du secteurs de l'assurance impliqués dans cette nouvelle technologie :

Les témoignages (repris en annexe 6) confirment l'intérêt du secteur pour la technologie blockchain et ses avantages :

- Patrick Sergysels, directeur data chez AG Insurance, valide l'intérêt pour l'assureur d'avoir accès à une base de données distribuée qui regrouperait l'ensemble des données d'identification des clients. Elle faciliterait le processus KYC et « l'onboarding » des clients.
- Patricia Boydens, consultante innovation chez Assuralia et Datassur, souligne l'intérêt de la technologie dans la désintermédiation et la création de registres immuables. Elle précise cependant que le potentiel de la technologie est limité par la mentalité européenne et les régulations de protection du consommateur qui en résulte.
- Koen Vingerhoets, blockchain évangéliste et business architecte chez Fujitsu, considère que la technologie n'a pas encore pu démontrer son potentiel dans ce secteur. Il est cependant certain que les avantages relatifs à la réduction des coûts et à la traçabilité des données et/ou des objets sont des atouts clefs pour le secteur. De même, il pense que le concept de l'assurance à « l'utilisation », rendue possible par cette technologie, pourrait révolutionner le secteur. Elle modifierait la perception que le client a du produit d'assurance. Au lieu de le considérer comme un coût à faible utilité, le lien direct instauré entre l'utilisation du produit et l'activation de la couverture, permet de la valoriser.
- Tobias Ambühl, directeur technologique d'AXA Suisse (CTO), estime que la technologie blockchain est incontournable. Les grands acteurs du secteur ne peuvent plus lui tourner le dos. Il met en évidence deux grands domaines dans lesquels le secteur de l'assurance pourrait utiliser la technologie : le domaine du risque, par exemple avec la tokenisation et le domaine de la confiance. Dans ce deuxième domaine, la technologie

pourrait aider les clients à retrouver l'autorité sur leurs identités et leur données numériques.

Cependant, malgré le potentiel de la technologie pour le secteur de l'assurance, nous sommes forcés de constater que celle-ci n'a pas encore réussi à percer. En Belgique, aucune compagnie d'assurances ne l'utilise de manière concrète. En Europe, les tentatives d'applications ou de développements liés à la technologie ne sont également pas de francs succès commerciaux.

Le retard dans l'utilisation de la technologie blockchain dans le secteur assurantiel belge et européen est, selon nos interlocuteurs, dû à plusieurs raisons.

Premièrement, la jeunesse de la technologie pourrait avoir sa part de responsabilité. Une nouvelle technologie suit souvent un cycle d'évolution. Le « Hype Cycle » de Gartner identifie plusieurs phases dans ce cycle : la naissance du concept, l'euphorie quant à son potentiel, la prise de conscience de ses limites, la désillusion, puis la concrétisation de projets rentables.

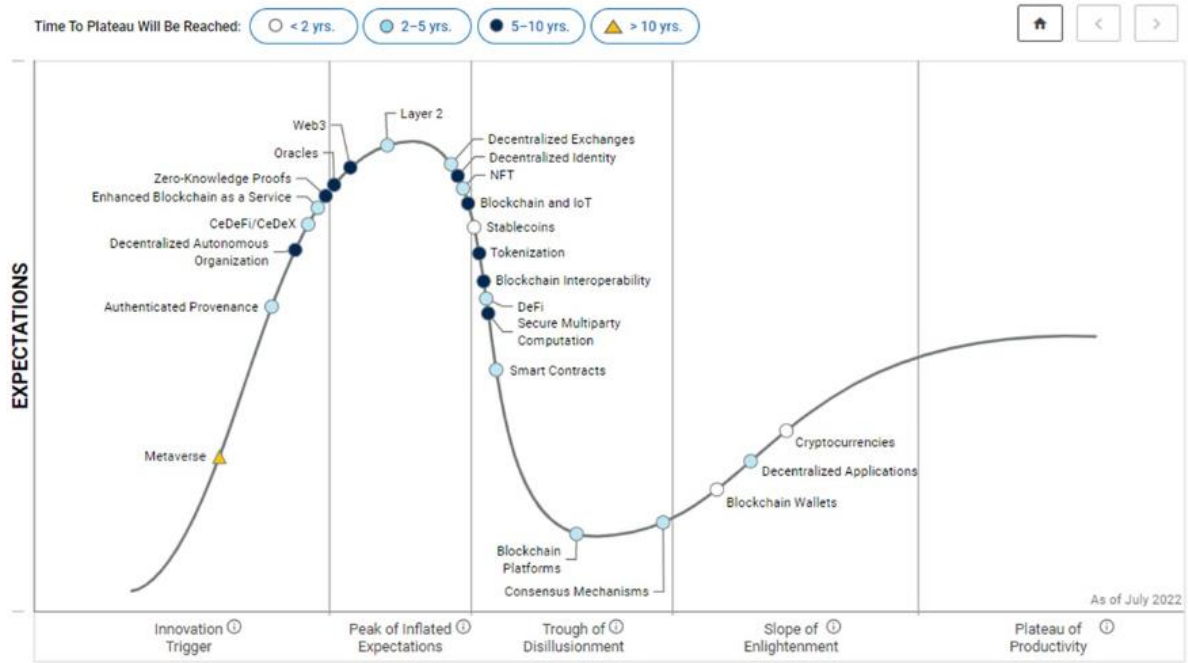


Figure 27 : Hype Cycle de la blockchain et du Web 3, Gartner 2022

La majorité des applications sont aujourd'hui dans les phases II et III du cycle. Nous pouvons donc conclure que la technologie manque encore de maturité pour que son potentiel soit complètement exploité et rentabilisé.

Les expériences personnelles de nos interlocuteurs nous confirment les résultats obtenus via le Hype Cycle.

Dans les années 2015 à 2017, Koen Vingerhoets et Patrick Serysels ont tous deux participé aux premiers pas de la technologie dans le secteur de l'assurance belge. A l'époque, la technologie blockchain était considérée comme d'une d'importance stratégique par les compagnies d'assurances. La technologie était dans une phase d'innovation, d'euphorie. Les entreprises se sont ainsi lancées dans la création de projets en voulant absolument utiliser LA nouvelle technologie. Cependant, nous l'avons vu au travers du mémoire, la technologie n'est pas parfaite, ni adaptée à tous les projets. La plupart de ces projets pilotes se sont ainsi soldés par des échecs et le secteur est entré dans une phase de désillusion vis-à-vis de celle-ci.

Aujourd'hui, la technologie continue d'évoluer. Les avantages et désavantages de celle-ci deviennent de plus en plus clairs pour les acteurs du secteur. Néanmoins, les interlocuteurs pensent que la technologie doit encore maturer avant d'arriver à une phase de prospérité dans laquelle des utilisations plus adaptées à ses avantages peuvent être trouvées. Dans cette dernière phase, la technologie développera ainsi son intérêt et sa valeur ajoutée.

Deuxièmement, les mentalités européennes concernant les nouvelles technologies sont conservatrices en comparaison de celles des pays développés d'Asie ou d'Amérique.

Les régulations européennes, notamment celles relatives à la protection des consommateurs, sont plus avancées. Ces lois protectrices et cette réticence des acteurs européens limitent l'innovation et le potentiel de la technologie sur nos marchés.

Finalement, nous constatons des disparités très importantes en matière de distribution au sein de l'Europe. Le marché de l'assurance en Belgique reste très traditionnel. Nous avons vu dans la partie « état des lieux du secteur de l'assurance en Belgique et en Europe » que la distribution en Belgique passe principalement par le courtage. Les applications B2C qui

seraient mises en œuvre via la technologie blockchain s'apparente bien évidemment à de la vente directe. La part du direct en Belgique étant minoritaire, il est assez logique que les principaux acteurs belges de l'assurance n'y accordent pour l'instant que peu ou pas de moyens. A l'inverse, dans certains pays étrangers tel que la Suisse, où le direct est prépondérant, des projets concrets tels que Car Dossier mis en œuvre par Axa ont vu le jour.

Patrick Sergysels nous souligne également l'existence d'outils traditionnels mais néanmoins fonctionnels sur le marché belge de l'assurance. Il cite par exemple, le réseau Portima qui organise les échanges d'informations entre les compagnies d'assurances et le secteur du courtage. Ces outils, proposés par des entreprises privées, réduisent l'intérêt du secteur pour les avantages issus de la technologie blockchain.

CONCLUSION

L'objectif de ce mémoire était de déterminer si la technologie de la blockchain est suffisamment mature pour envisager des applications concrètes à court terme dans le secteur de l'assurance belge et/ou européen.

Pour pouvoir réaliser cette analyse, nous avons défini les concepts clés de cette technologie, ses atouts et ses faiblesses.

Nous avons ensuite cartographié le secteur de l'assurance belge et européen. Il s'agit d'un acteur économique prépondérant au vu du volume de primes encaissées et de l'actif sous gestion. Nous avons vu que les canaux de distribution n'étaient pas uniformes d'un pays à l'autre, la part de la vente directe ou par intermédiaires (agents et courtiers) variant significativement. En Belgique, la commercialisation de produits d'assurance via le courtage reste majoritaire.

Le cœur du mémoire s'emploie à identifier, notamment via des exemples concrets, les applications existantes ou possibles de la technologie dans le secteur de l'assurance.

Nous y avons vu comment l'utilisation d'un registre distribué et de contrats intelligents, permettent de réduire les coûts et d'optimiser la gestion. Via l'analyse des flux de gestion d'un dossier sinistre, nous avons démontré les gains potentiels de productivité.

La gestion des données est devenue un enjeu majeur de notre société. La blockchain permet la création d'une base de données sécurisée et infalsifiable. Les clients pourraient l'alimenter, autoriser des organismes tiers (mutualités, assureurs, prestataires de santé, services publics, …) à l'alimenter, et, en partager l'accès avec les partenaires de leur choix (assureurs, intermédiaires, …). Chaque individu disposerait ainsi de son identité digitale. Il s'agirait d'une avancée significative pour le secteur de l'assurance. Les applications seraient très nombreuses. Nous pensons, en particulier, aux processus KYC et AML. Plus généralement,

elle permettrait de réduire la fraude à l'assurance mais également d'automatiser tout ou une partie du processus de souscription des contrats.

Cette automatisation facilite l'apparition ou la revalorisation de certains produits d'assurance. Nous pensons à l'assurance à l'utilisation et à l'assurance pair-à-pair.

En guise de démonstration, nous avons créé une application d'appel d'offres et de souscription d'un contrat de responsabilité civile familiale en ayant recours à la technologie Ethereum. Nous y illustrons le fonctionnement pratique d'une blockchain, d'un contrat intelligent et la façon dont l'historique des transactions est sauvegardé.

Les entretiens réalisés avec des acteurs de terrain confirment l'intérêt du secteur pour la technologie. Néanmoins, malgré ce potentiel, aucun projet rentable n'a actuellement vu le jour en Europe. Nous expliquons ce constat par un manque de maturité de la technologie, par une réglementation protectrice du consommateur qui limite l'innovation et, par le fait que le marché européen reste très conservateur et présente un haut taux de pénétration.

L'une des principales forces de la technologie blockchain est sa capacité à favoriser la collaboration entre les acteurs. Elle permet via l'automatisation des processus et par la décentralisation des registres de faciliter la mise en place d'écosystèmes et d'entreprises communes. Nous pensons dès lors que les premiers succès d'intégration de la technologie blockchain dans le secteur de l'assurance en Europe concerneront des applications B2B au même titre que ce que nous constatons aujourd'hui dans le secteur de la finance. Le consortium B3i qui, pour rappel, rassemble de grands assureurs et réassureurs internationaux pourrait en être l'incubateur.

En ce qui concerne les applications B2C, elles verront probablement le jour lorsque la technologie aura été expérimentée en B2B et aura atteint un stade de maturité et d'acceptation plus large. Il n'est pas exclu que les premières applications soient développées aux Etats-Unis ou en Asie, régions actuellement plus propices aux développements technologiques.

Il serait dès lors particulièrement intéressant d'élargir le champs d'investigation en s'intéressant aux applications de la blockchain dans les marchés de l'assurance non européens mais cela sort du cadre actuel de ce mémoire.

ANNEXES

1. Méthodologie utilisée pour la création du PoC

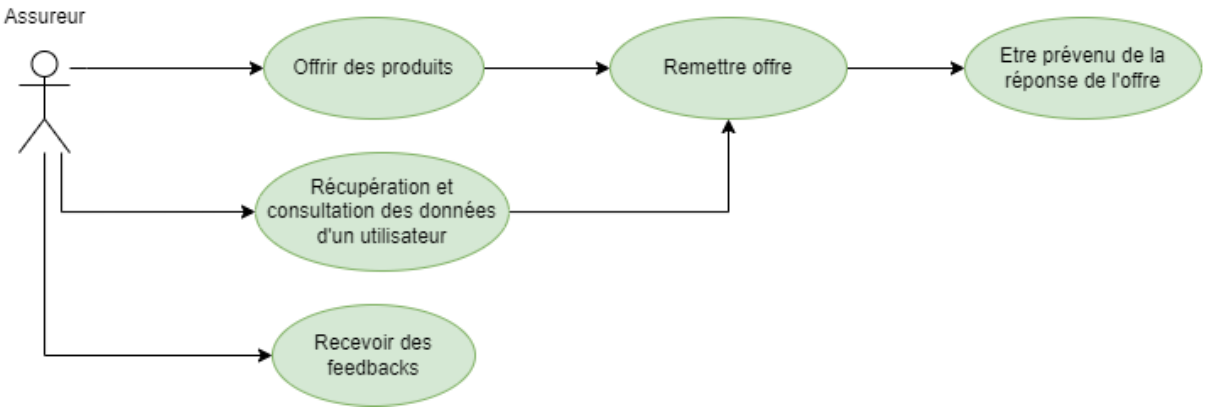
La méthode d'analyse et d'élaboration qui a été utilisée lors de la création de l'application, est divisée en plusieurs catégories : les principes de l'application, les personnas, les fonctionnalités, les exigences et finalement les tâches. Cette méthode vise à progressivement raffiner et mettre en lumière les différents aspects et composants de l'application à développer.

- Principes : les principes définissent les grandes lignes de l'application, ses objectifs, son but. Ils servent à baliser les discussions, analyses et travaux futurs.
- Personnas : un personna désigne une entité qui interagit avec l'application. Un même utilisateur peut incarner différents personnas selon ses motivations ou selon certaines conditions. Par exemple, dans le cadre d'une application d'assurance P2P basée sur la blokchain, un même utilisateur peut être à la fois un assureur et un assuré (client).
- Fonctionnalités / User stories : les fonctionnalités décrivent les interactions possibles des personnas avec l'application. Les fonctionnalités de Insurme peuvent être retrouvées à l'annexe 2.
- Exigences fonctionnelles et non-fonctionnelles :
    - Fonctionnelles : les exigences fonctionnelles sont des exigences par rapport aux fonctionnalités fournies par l'application. Elles détaillent les fonctionnalités en donnant plus de précision sur son fonctionnement et sur les informations que le développeur aura besoin pour créer l'application. Par exemple, il est important de savoir quelles informations doivent figurer au sein d'un contrat, quels types de données les contrats ont besoin lors de la souscription, quels sont les produits à afficher sur les interfaces, …
    - Non-fonctionnelles : les exigences non-fonctionnelles sont des exigences par rapport au fonctionnement technique de l'application et de ses composants. Elles peuvent être des exigences relatives à la disponibilité de l'application, à sa performance, son design général, …
- Tâches : chaque tâche définit une action concrète à réaliser dans le cadre de l'élaboration de l'application. Ces tâches sont balisées en termes de complexité et/ou

de temps, ont un objectif, une description ainsi qu'une indication sur la manière de valider l'accomplissement de la tâche. Elles sont réparties via un cahier de charges entre les membres de l'équipe de création du PoC en fonction des compétences spécifiques de chacun.

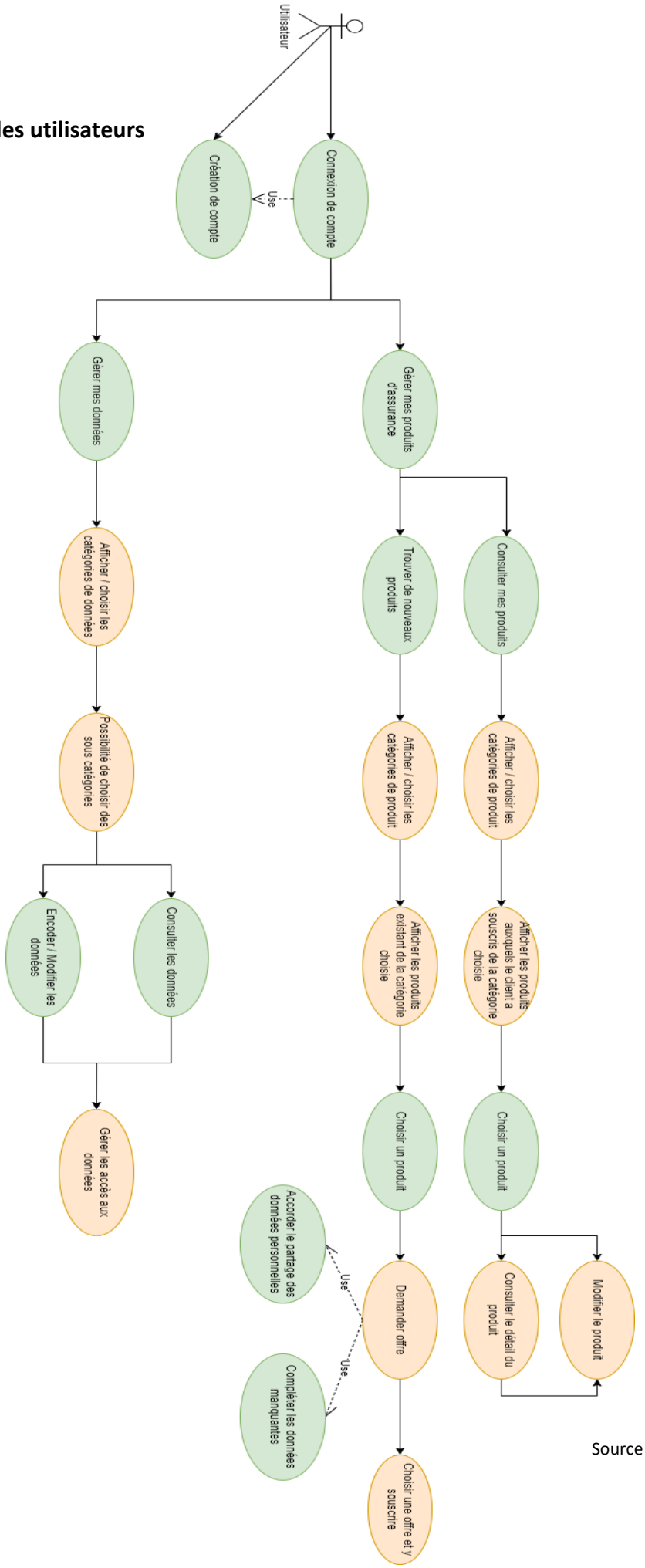
2. Fonctionnalités de l'application

2.1. Fonctionnalités des assureurs



Source : Draw.io

2.2. Fonctionnalités des utilisateurs

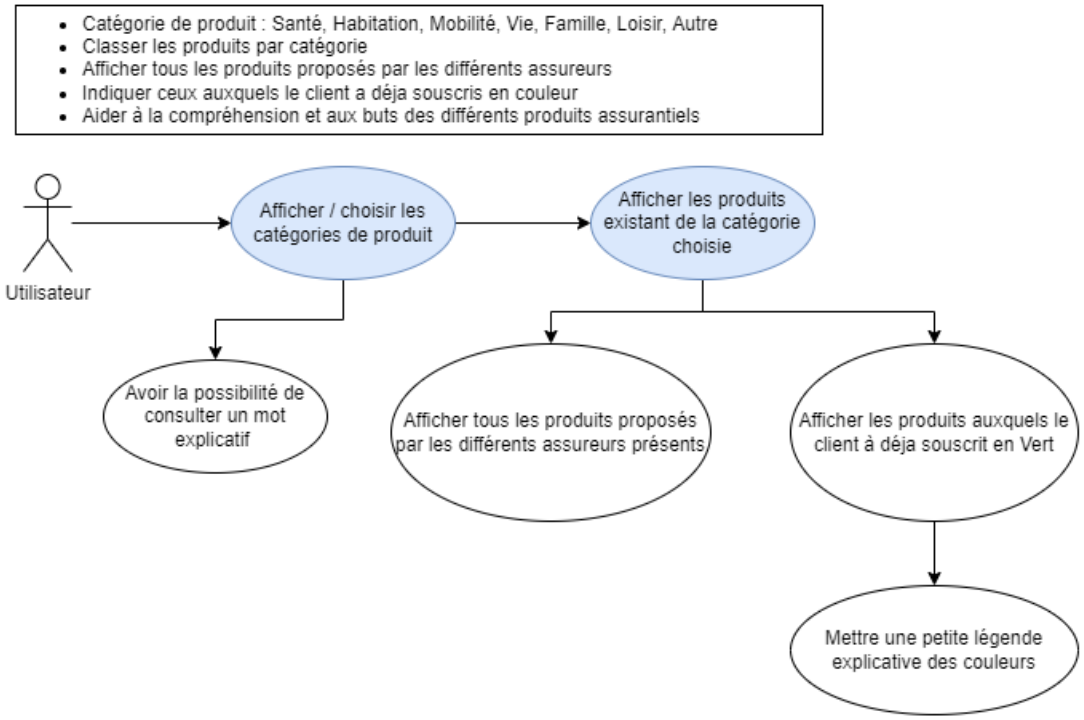


Source : Draw.io

Les fonctionnalités représentées dans les deux schémas ci-dessus en vert ne nécessitent pas plus de détails et d'exigences quant à leur fonctionnement. Cependant, celles représentées en orange ont une explication et des exigences que vous pouvez retrouver ci-dessous.

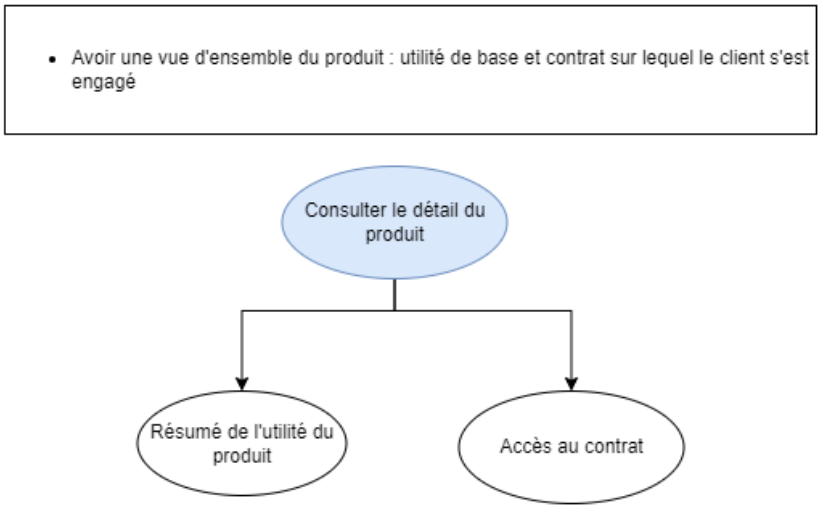
3. Fonctionnement et exigences des fonctionnalités

3.1. Catégorie de produit



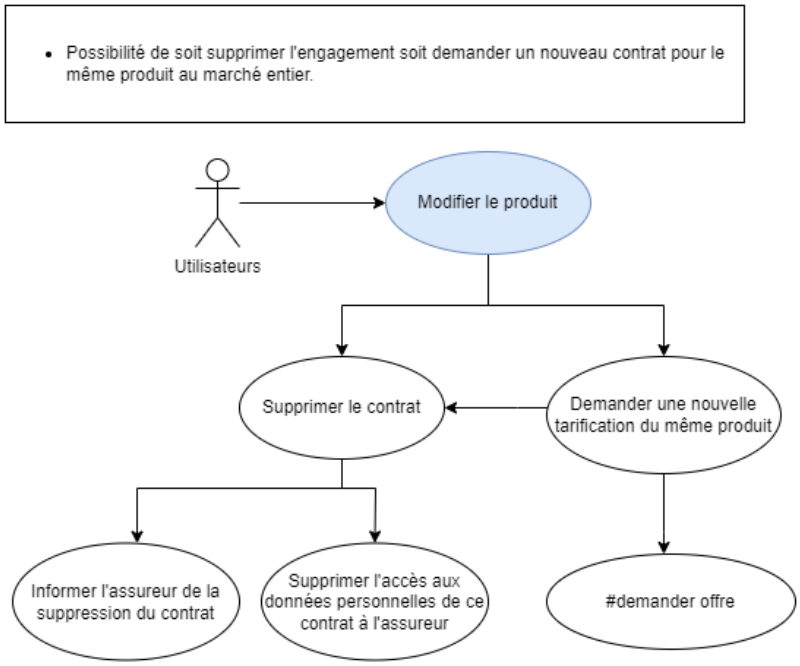
Source : Draw.io

3.2. Consulter le détail d'un produit



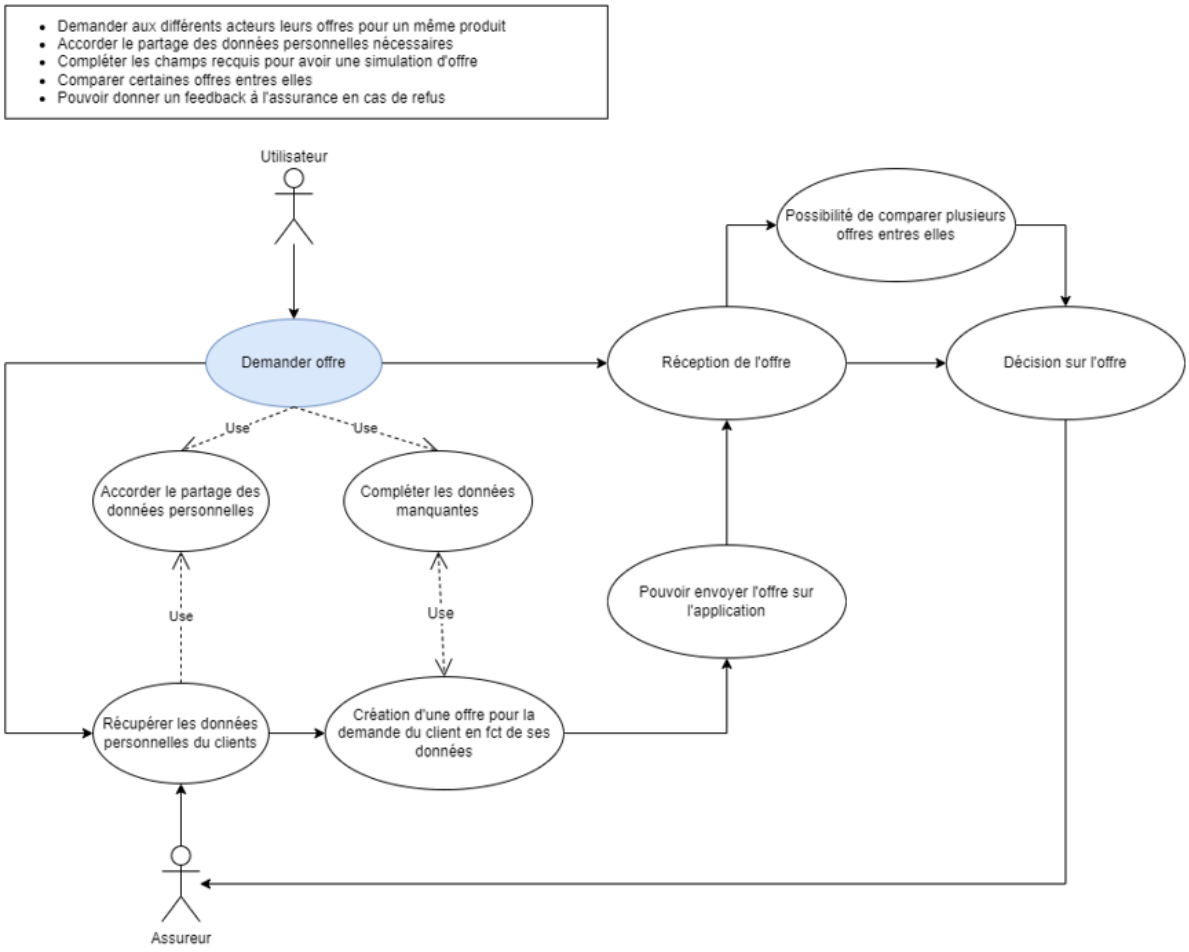
Source : Draw.io

3.3. Modifier le produit

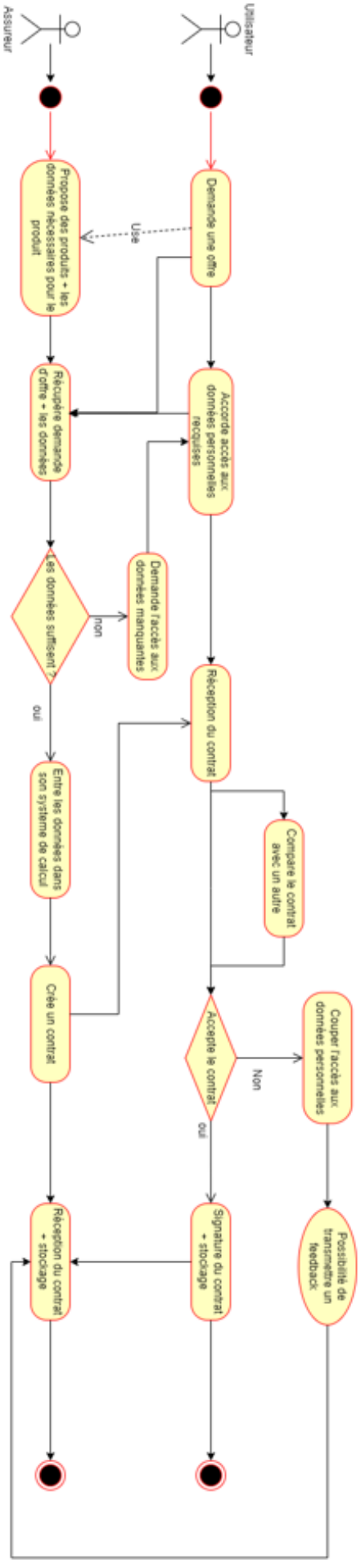


Source : Draw.io

3.4. Demander une offre



Source : Draw.io



Source : Draw.io

3.5. Catégories de données

Source : Draw.io

4. Démonstration

4.1. Ethereum

Afin de mieux comprendre la démonstration du proof-of-concept, certaines notions de la blockchain Ethereum et de ses contrats intelligents doivent être brièvement introduits.

Nous avons en effet choisi la technologie blockchain Ethereum comme support pour notre PoC. La raison de ce choix est simple : l'écosystème Ethereum est celui qui dispose des outils et de la communauté les plus fournis et les plus matures.
Le terme Ethereum peut désigner deux choses : le réseau principal de la blockchain publique du nom « Ethereum » et la technologie basée sur l'Ethereum Virtuel Machine permettant la mise en oeuvre d'une blockchain. C'est cette deuxième notion qui nous sera utile dans la création de l'application.

L'Ethereum Virtual Machine (EVM) est un ensemble de spécifications qui définissent les règles de fonctionnement pour une blockchain. Elle définit également les opérations de base utilisables par les contrats intelligents. L'Ethereum Virtual Machine peut être vue comme un mode d'emploi pour créer un programme capable de mettre en œuvre une blockchain *(Ethereum, 2022)*.

4.2. Contrats intelligents dans la blockchain Ethereum

Au sein de la blockchain Ethereum, un contrat intelligent est un code informatique compilé et stocké dans la blockchain. Ce code est exécuté par l'Ethereum Virtual Machine lorsqu'une transaction spéciale destinée au contrat intelligent est émise par un utilisateur de la blockchain. Un contrat intelligent peut être vu comme une application qui vit au sein d'une

blockchain. Cette application peut par exemple retenir et gérer des données ou exécuter des processus.

Le contrat intelligent est ajouté à la blockchain au moyen d'une transaction spéciale qui n'a pas de destinataire et dont les données correspondent au code compilé du contrat intelligent. Chaque contrat intelligent créé au sein de la blockchain Ethereum possède un identifiant (adresse) du même format que l'identifiant des utilisateurs de la blockchain.

Vu que leur code est stocké au sein de la blockchain, les contrats intelligents ont les propriétés suivantes :

- Leur code est infalsifiable et ne peut être modifié.
- Leur code est disponible pour tous les acteurs du réseau qui disposent d'une copie de la blockchain et chacun peut l'utiliser.
- Chacun est capable de vérifier et reproduire le traitement qu'un contrat intelligent a fait d'une transaction.

4.3. Outils utilisés pour réaliser l'application

Pour faciliter la création de notre application, nous nous sommes basés sur une série d'outils préexistants.

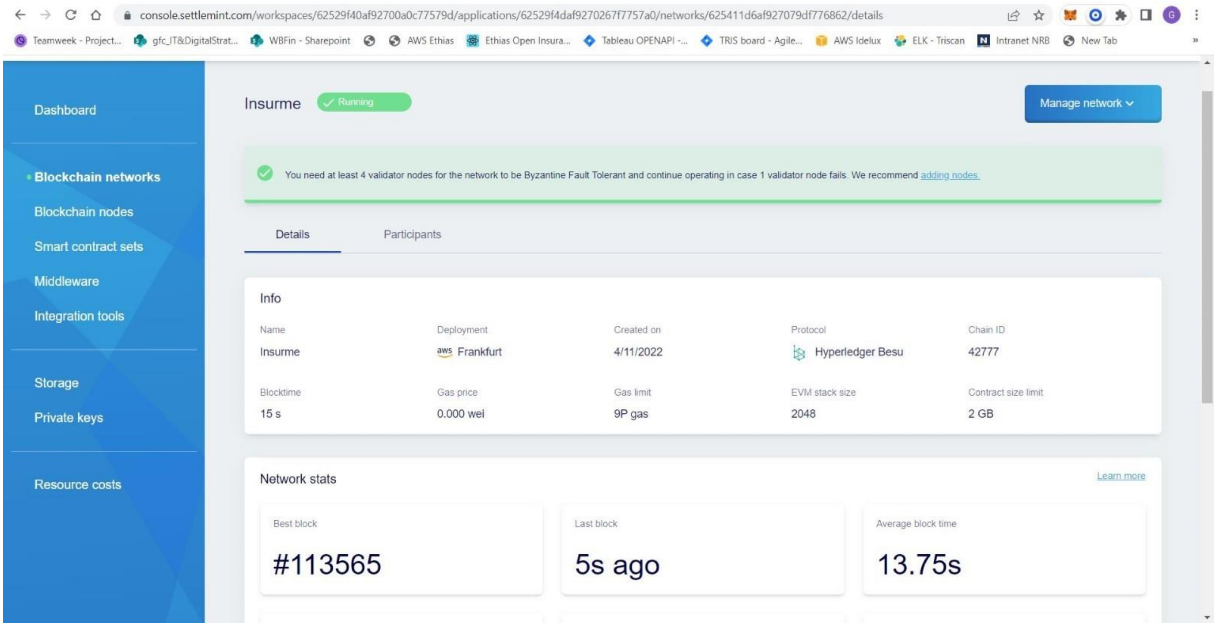
Le premier outil utilisé est un outil développé par Settlemint[9]. Settlemint est une société belge fondée en 2016. Elle prose une plateforme low-code pour gérer et développer des applications basées sur une blockchain.

La plateforme permet de mettre en œuvre notre réseau au travers de différentes technologies Blockchain. Elle provisionne, configure et gère automatiquement les nœuds connectés à la blockchain. D'autres fonctionnalités permettant notamment de faciliter le développement et le déploiement de contrats intelligents sont proposées par la plateforme.

Dans le cas d'Insurme, la plateforme a été adoptée pour créer une blockchain privée basée sur la technologie Ethereum et pour gérer les nœuds de celle-ci.

[9] Van Niekerk & van der Veer, 2016: SettleMint | High-performance low-code blockchain development platform

La photo ci-dessous illustre les détails de notre blockchain privée gérée par Settlemint. Nous pouvons par exemple apercevoir le nom de la blockchain, la date de création de celle-ci, le protocole utilisé (Ethereum entreprise), le temps entre chaque création de bloc, etc.



Source : Settlemint

Le deuxième outil utilisé lors de la création de notre application est Metamask[10]. Metamask est un portefeuille développé par la société Consensys, société New-Yorkaise fondée en 2014.

Avant d'expliquer ce qu'est un portefeuille, quelques rappels sur la technologie blockchain :

- Tout utilisateur peut avoir une ou plusieurs paires de clés privées/publiques
- La clé privée sert à signer les transactions et à prouver son identité.
- La clé publique est connue de tous et identifie un utilisateur au sein d'une blockchain.
- La clé publique est utilisée pour vérifier les signatures créées par un utilisateur.
- La perte d'une clé privée signifie qu'il n'est plus possible d'interagir avec son compte et donc de transférer les biens qui lui sont liés.

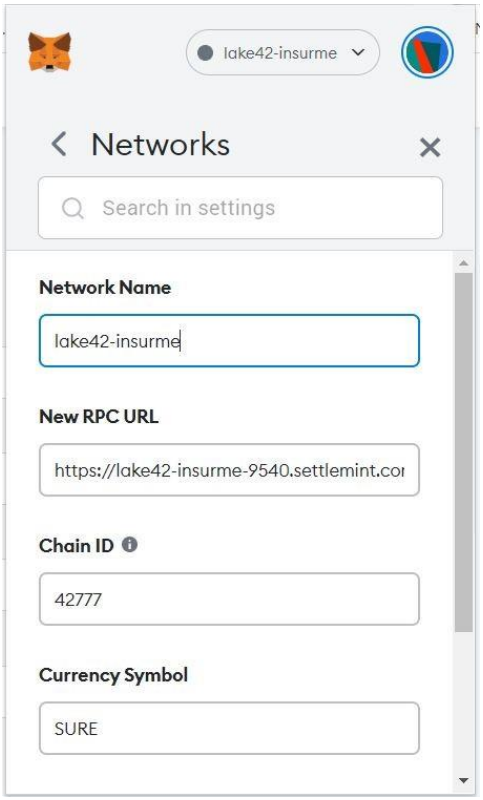
Toutes ces nouveautés ne sont pas faciles à prendre en main. Le rôle du portefeuille est de les simplifier.

Il permet de conserver de manière sécurisée les paires de clés publiques/privées des utilisateurs. Il peut également faciliter les interactions entre les utilisateurs, la blockchain et les applications.

[10] Metamask, 2016 : The crypto wallet for Defi, Web3 Dapps and NFTs | MetaMask

Par exemple, l'application WEB peut dialoguer avec le portefeuille de l'utilisateur pour encoder une transaction et la soumettre pour signature à l'utilisateur. L'utilisateur pourra alors choisir ou non de signer la transaction. Le portefeuille se chargera d'effectuer la signature au moyen de la clé privée qu'il contient.

Dans le cadre d'Insurme, Metamask a été choisi car il s'agit du portefeuille le plus mature, sécurisé et simple d'utilisation.

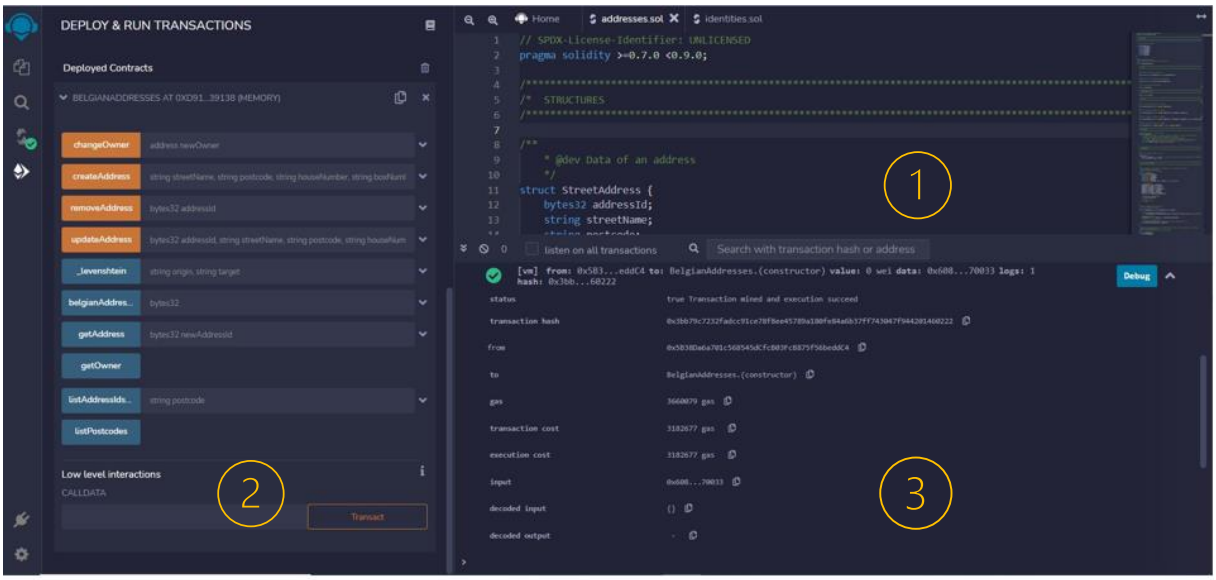


Source : Metamask

Le troisième outil employé s'appelle Remix. C'est un environnement de développement préconfiguré pour les contrats intelligents Ethereum. Il ne nécessite pas d'installation et s'utilise via un browser WEB : https://remix.ethereum.org

Dans le cadre d'Insurme, Remix a été utilisé pour développer, déployer et interagir avec les contrats intelligents de l'application.

La photo ci-dessous illustre les différentes sections proposées par Remix : une partie dans laquelle le développeur code (1), une partie console (2) servant à utiliser les fonctionnalités codées dans les contrats intelligents et une partie servant d'affichage pour les résultats des opérations introduites dans la console (3).

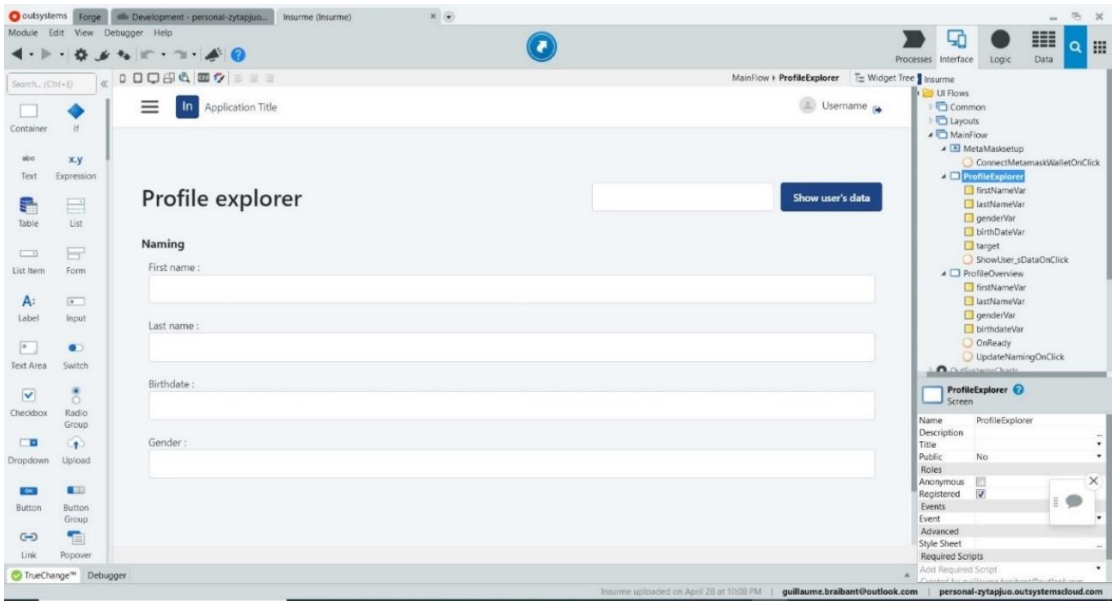


Source : Remix

Le dernier outil dont nous nous sommes servis pour le design et l'interface utilisateur de l'application est OutSystems[11]. La société a été fondée en 2001 et son siège social se situe à Londres. Elle propose une plateforme low code du même nom pour développer des application WEB et Mobile.

Dans le cas d'Insurme, la plateforme a été adoptée pour réaliser un portail WEB simple qui permet aux utilisateurs d'encoder leurs données dans l'application mais aussi consulter les données d'autres utilisateurs s'ils en ont les accès.

L'interface se présente comme suit :



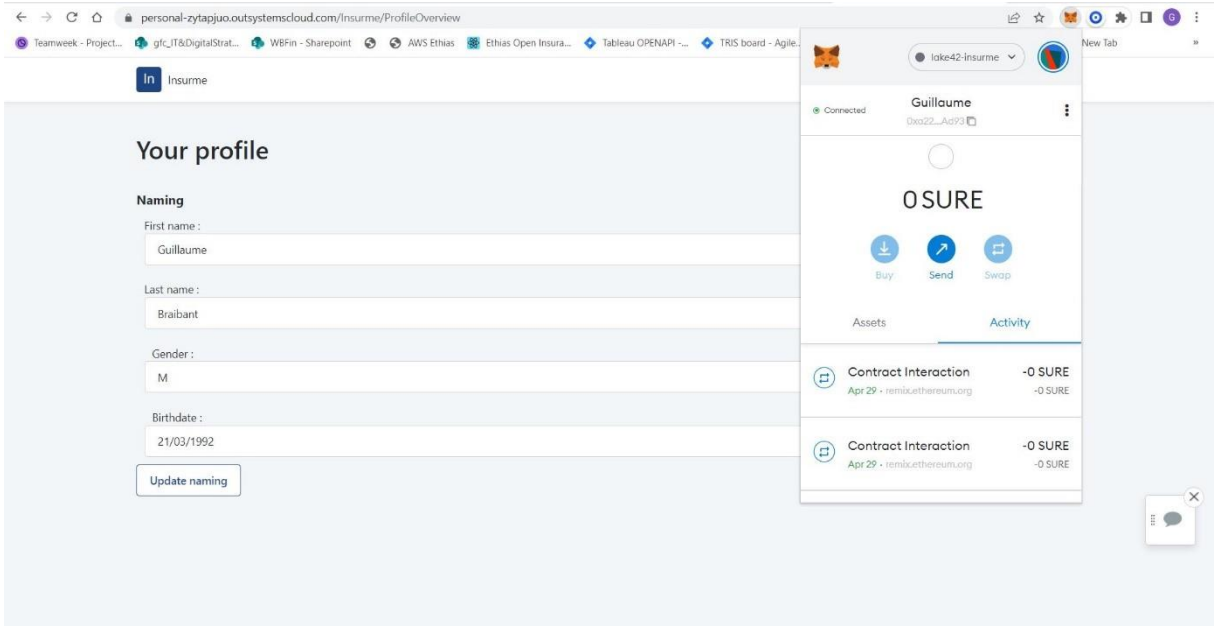
Source : OutSystems

[11] OutSystems, 2001 : Low Code High-Performance Software Development | OutSystems

4.4. Composants de l'application Insurme

L'application Insurme est composée des éléments suivants :

- Contrat intelligent « Identities » : il fournit et gère les fonctionnalités liées à la définition et au partage de données personnelles au sein de la blockchain.
- Contrat intelligent « Insurme » : il fournit et gère les fonctionnalités permettant à des utilisateurs de demander et de souscrire à de nouveaux produits d'assurance. Il offre également des fonctionnalités aux assureurs leur permettant de demander l'accès à des données personnelles. Il propose également la signature des contrats d'assurance.
- Portail WEB : il s'agit de l'application web Insurme. Elle permet de:
    - Configurer le portefeuille de l'utilisateur pour interagir avec les contrats intelligents d'Insurme. Il lui servira de compte dans l'application.
    - Consulter et encoder ses données au sein du contrat intelligent Identities.
    - Consulter les données d'un autre utilisateur via le contrat intelligent Identities (si autorisé).



Source : OutSystems

4.5. Démonstration du flux de souscription

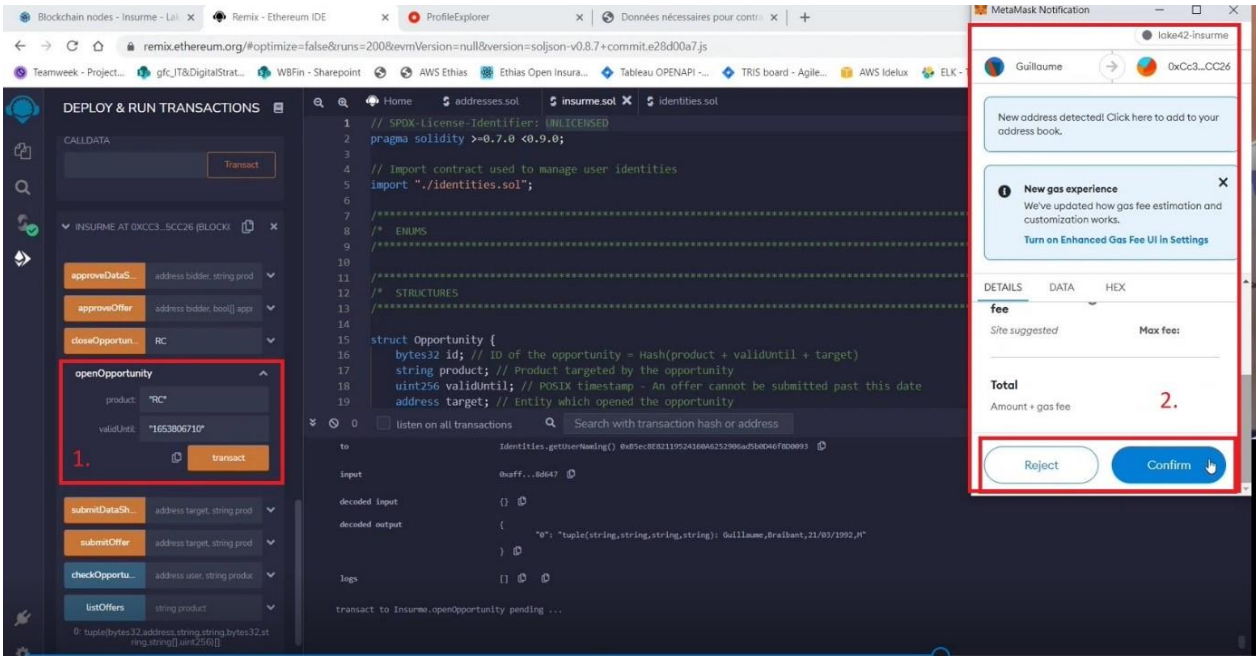
L'application web, plus user friendly, n'ayant pas été réalisée pour toutes les fonctions présentes dans Insurme, le flux d'une souscription à un contrat RC familiale sera principalement démontré au travers de l'outil Remix. Le fonctionnement de l'application n'en

est pas impacté, seul le design et la facilité d'utilisation ne seront pas présents dans l'outil Remix.

Remix est capable de comprendre le code d'un contrat intelligent et de générer une console qui permet d'interagir de manière simple avec des contrats intelligents tout en pouvant inspecter les données échangées avec la blockchain et les contrats intelligents.

4.5.1. Création d'une opportunité par l'utilisateur

Le flux de souscription commence par l'ouverture d'une opportunité par un utilisateur. Par une opportunité, l'utilisateur demande aux assureurs de lui proposer des produits dans la catégorie qu'il désire.



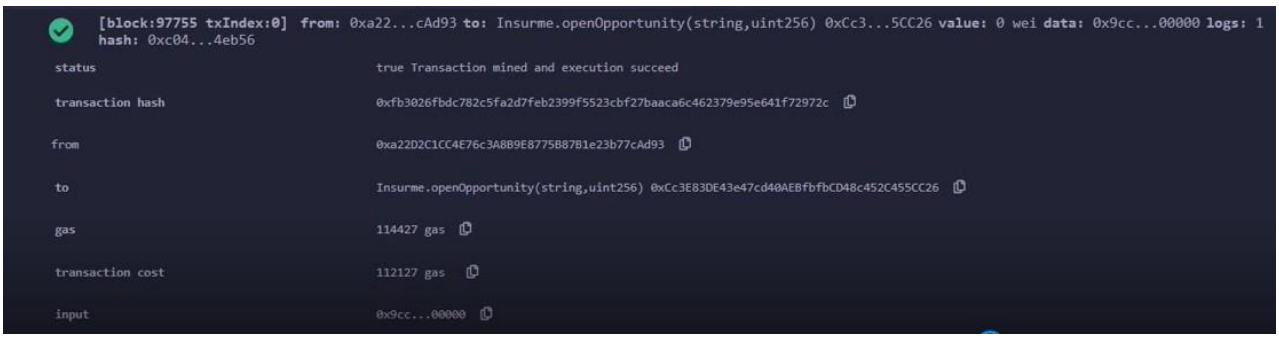
Source : Remix

Le cadre 1 montre une partie de la console générée automatiquement par Remix pour interagir avec le contrat intelligent Insurme.

Nous pouvons y apercevoir le nom de la fonctionnalité, les champs de données nécessaires à la transaction ainsi qu'un bouton « transact » qui permet de soumettre la transaction à signature.

Le cadre 2 montre le wallet qui affiche la transaction soumise par Remix à signature. Par un clic sur «Confirm», l'utilisateur signe et envoie la transaction à la blockchain (au réseau pour confirmation).

Lorsque la transaction est confirmée, une information est affichée par Remix avec les détails de la transaction :



Source : Remix

Il est possible d'y distinguer :

- Le statut de la transaction
- Le hash de la transaction
- L'expéditeur de la transaction (l'adresse de l'utilisateur)
- Le destinataire de la transaction (l'adresse du contrat intelligent Insurme)
- Les données incluses avec la transaction

Suite à la confirmation d'une transaction, des événements peuvent être déclenchés automatiquement. Ici, la validation de la demande d'offre engendre l'événement nommé «opportunityCreated». Celui-ci sert à notifier les assureurs qu'une nouvelle opportunité est disponible. L'événement reprend les données pertinentes dans la demande :

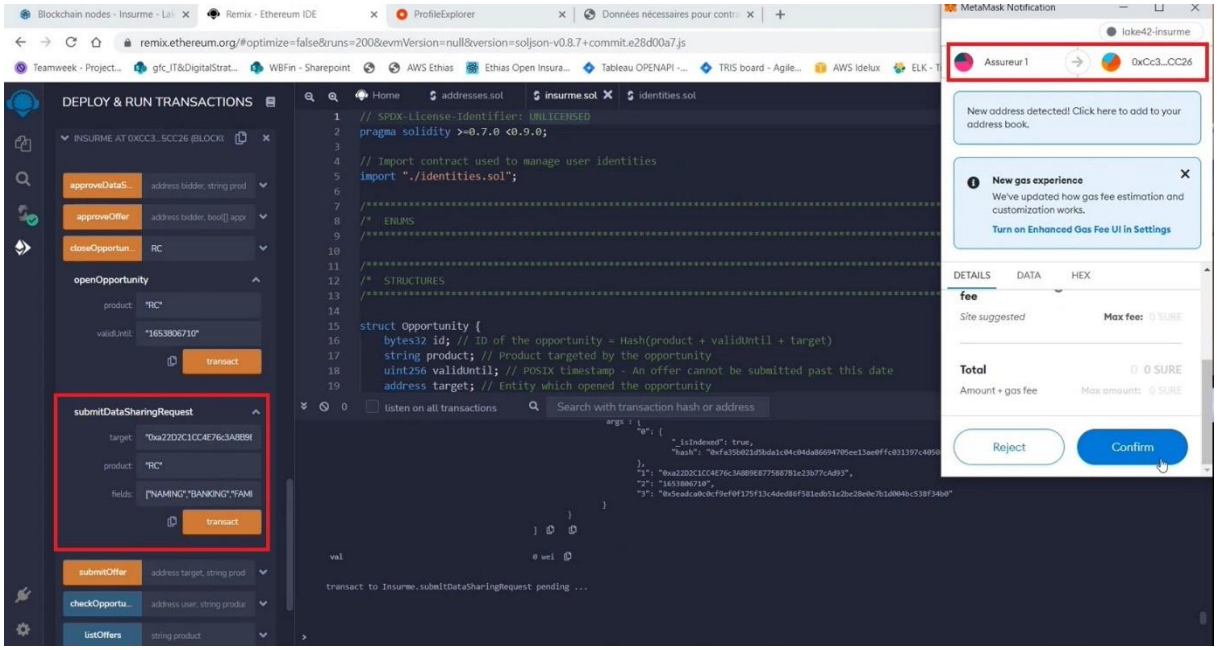
- l'utilisateur qui a créé l'opportunité
- le type de produit d'assurance demandé.

Source : Remix

4.5.2. Demande d'accès aux informations personnelles du client

Un assureur qui voudrait répondre à la demande du client peut demander des informations à l'utilisateur en vue d'établir un contrat.

Passons maintenant dans la peau d'un hypothétique assureur. La fonctionnalité «SubmitDataSharingRequest » permet à l'assureur de demander cet accès aux données. Dans cette fonction, l'assureur doit encoder l'identifiant de l'utilisateur, le produit d'assurance pour lequel il souhaite faire une offre ainsi que les données que l'assureur demande (ici : la signalétique, l'adresse et les informations bancaires).



Source : Remix

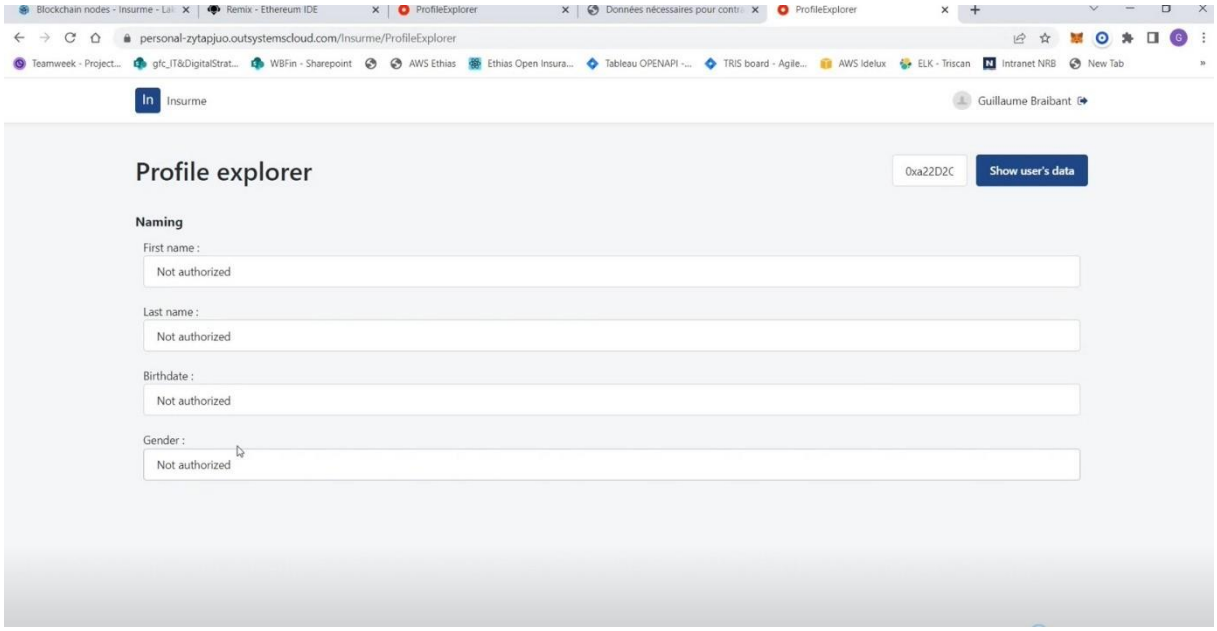
L'assureur peut ensuite signer la transaction «demande» au moyen de son portefeuille et faire exécuter celle-ci.

A nouveau, des données techniques seront imprimées par Remix à propos de la transaction. Par soucis de brièveté, elles ne seront pas à nouveau détaillées. Il est cependant important de noter qu'un nouvel événement sera généré afin de prévenir l'utilisateur qu'une demande d'accès aux données a été soumise. L'utilisateur pourra choisir de l'approuver ou non.

4.5.3. Approbation de la demande d'accès

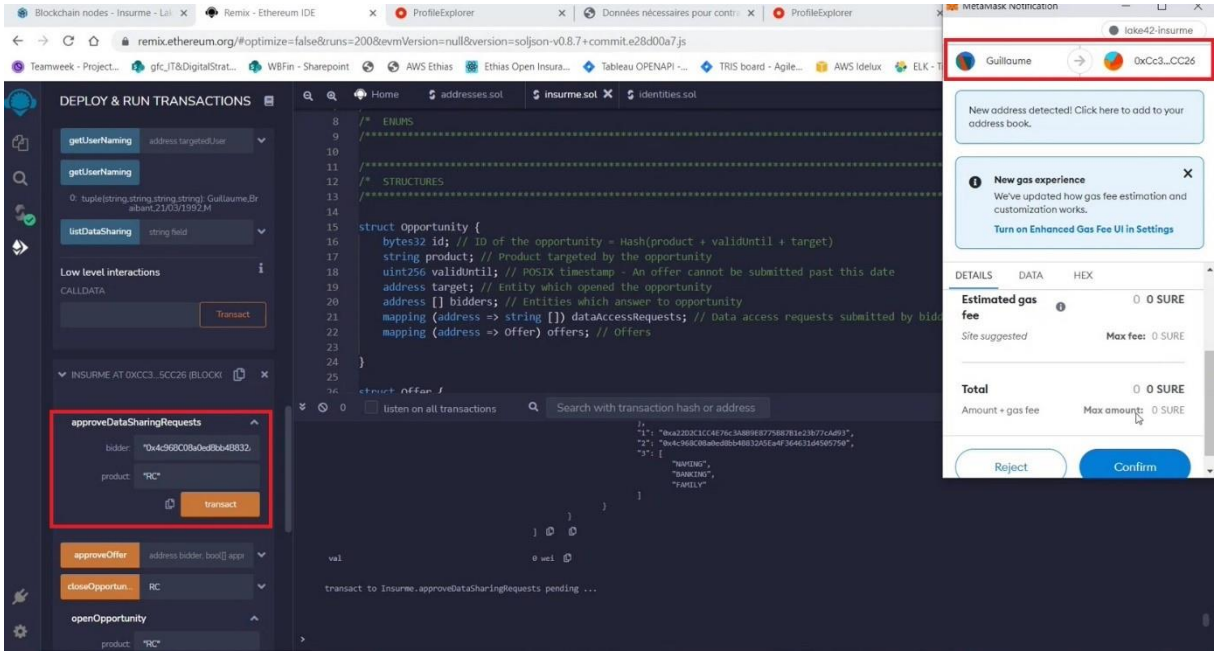
Dans le cadre de l'application, un portail web a été créé pour permettre de consulter facilement les données d'un utilisateur d'Insurme.

L'écran de l'application web suivant montre ce qu'il se passe lorsque l'assureur tente de consulter les données de l'utilisateur (identifié via son adresse) dans l'application sans son autorisation :



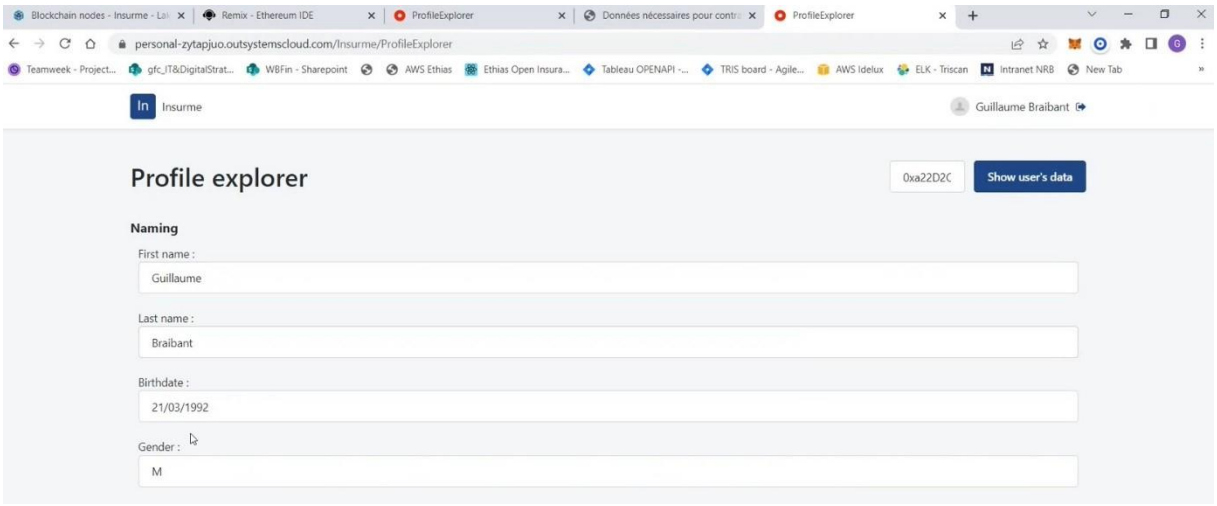
Source : OutSystems

Si l'utilisateur décide d'approuver la demande d'accès de l'assureur, il utilise la fonctionnalité «approveDataSharingRequest» du contrat intelligent. Il donne ainsi à l'assureur le droit de regard sur ses données personnelles nécessaires dans le cadre de sa demande d'assurance RC.



Source : Remix

L'assureur est prévenu de l'acceptation de sa demande. Il peut alors consulter les données de l'utilisateur via le portail WEB :



Source : OutSystems

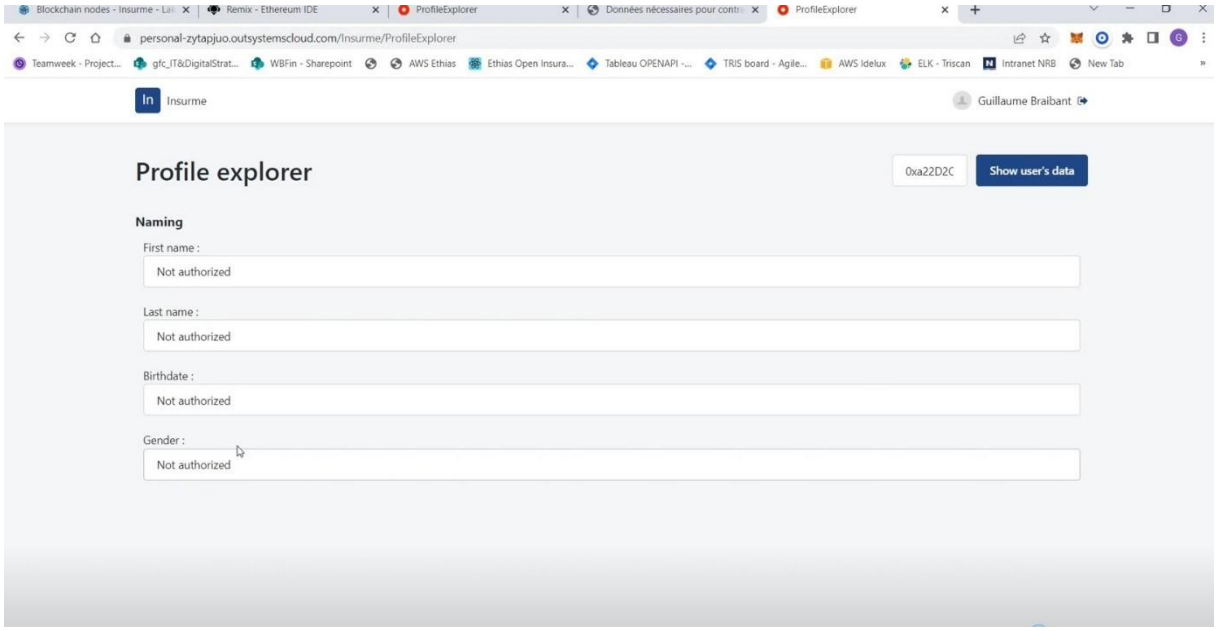
4.5.4. Soumission d'une offre et souscription au contrat

La suite du processus de souscription se fait comme suit :

- L'assureur utilise la fonctionnalité «submitOffer» du contrat intelligent Insurme pour soumettre une offre à l'utilisateur. La transaction, envoyée à l'utilisateur via la blockchain, contient les détails de l'offre. Un événement est généré pour prévenir l'utilisateur qu'une offre a été soumise pour approbation. Un assureur ne peut pas retirer son offre mais il peut en soumettre une autre qui invalidera l'offre précédente.

- Si une offre le satisfait, l'utilisateur peut l'accepter au moyen de la fonctionnalité «approveOffer». La transaction contient l'identifiant de l'offre approuvée et sera stockée sur la blockchain. Lorsqu'un utilisateur approuve une offre, le contrat intelligent clôture automatiquement l'opportunité (demande d'offres) et retire tous les accès fournis par l'utilisateur à ses données. Un événement est généré pour prévenir les assureurs de :
    - De la fin de l'opportunité
    - De l'acceptation de l'offre
    - Du retrait des accès aux données

Si l'assureur tente à nouveau de consulter les données de l'utilisateur après la clôture de l'opportunité, l'opération échouera :



Source : OutSystems

Pour finir, l'intérêt du processus est qu'à chaque transaction (demandes, messages, autorisations, contrats, …), les informations de celles-ci sont durablement inscrites dans la blockchain. Aucune des parties ne peut ainsi nier avoir signé la transaction. En effet, eux seuls sont capables d'émettre une signature valide sur une transaction les concernant.

En résumé, les transactions générées par le processus et inscrites de manière indélébile dans la blockchain comportent :

- Les données de la demande de l'utilisateur (produit demandé)
- Les demandes d'accès aux données-clients soumises par les assureurs
- Les approbations du client aux différentes demandes d'accès des assureurs
- Les offres des assureurs
- L'acceptation d'une des offres par l'utilisateur

5. Outils d'évaluation de compatibilité entre un projet et la technologie blockchain

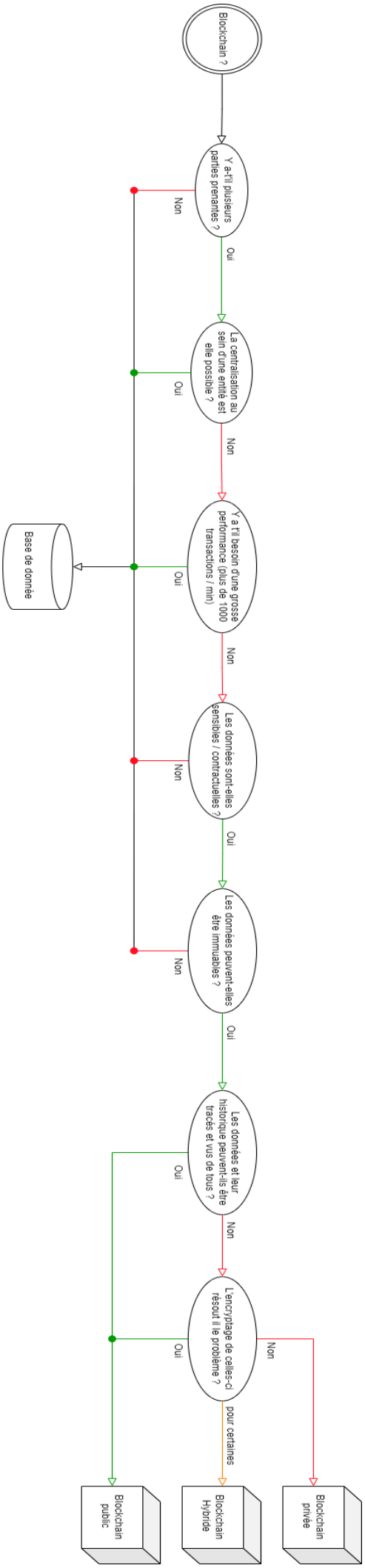
5.1. Questionnaire - Avez-vous besoin de la technologie blockchain ?

- ✓ Votre business ou votre chaine de valeur implique plusieurs parties prenantes? ☐
- ✓ Y a-t-il un intérêt d'historiser certaines transactions ou de tracer l'évolution de certains actifs? ☐
- ✓ Les produits sont-ils sujets à des processus répétitifs qui pourraient être automatisés ? ☐
- ✓ La sécurisation des données au travers d'un registre immuable est-elle intéressante ? ☐
- ✓ La centralisation des données est-elle un frein pour votre activité ? ☐

Si vous avez répondu oui à une seule de ces questions, la technologie blockchain peut avoir un intérêt pour votre entreprise.

Source : PowerPoint

5.2. Arbre de décision



Source : Draw.io

6. Interviews

Vous retrouverez ci-dessous le résumé de chacune de nos interviews réalisées via Microsoft Teams.

6.1. Interview de Patrick Sergysels (AG insurance), 18 juillet 2022

6.1.1. Présentation

Patrick Sergysels est le directeur informatique et data des AG insurance, compagnie dans laquelle il travaille depuis 1998. A la base, il a une formation d'ingénieur civil chimiste. Il a occupé différents postes en lien avec l'informatique et la blockchain. En 2010, il était responsable de l'innovation. De 2015 à 2017, il devient un des premiers membres du consortium B3i. En 2018, il participe à l'initiative belge B-Hive qui est un projet KYC entre les assureurs et les banques belges.

6.1.2. Avez-vous déjà eu recours à la technologie blockchain au sein de votre entreprise ?

A l'exception de nos expériences au travers d'Ageas dans B3i et de nos expériences personnelles dans B-hive, pas vraiment.

Nous prenons parfois part à certains PoC locaux mais sans grands investissements de notre part.

6.1.3. Avez-vous toujours des projets de mise en œuvre liés à la technologie ?

Non, malheureusement la technologie est au frigo. Sans compter nos petites participations aux PoCs, nous n'avons plus de projets actifs.

6.1.4. Quelles sont les applications / avantages de la technologie qui vous paraissent les plus pertinentes dans le secteur de l'assurance ?

- La digitalisation et l'automatisation des différents processus sont des avantages certains.

- La désintermédiation peut également être intéressante.

- Le principal avantage et celui qui serait le plus intéressant pour les AG est la création de l'identité digitale. Le KYC est difficile dans notre entreprise car nous ne vendons pas en direct. Le onboarding des clients s'en retrouve donc laborieux.

6.1.5. Connaissez-vous des applications concrètes de la technologie dans le secteur de l'assurance en Belgique ?

En Belgique non, il existe plusieurs pocs mais aucun d'eux n'est vraiment en production que je sache.

6.1.6. Quel est votre avis sur le futur de cette technologie dans le secteur de l'assurance en belgique / Europe ?

Je pense que la technologie va maturer. Beaucoup de technologies passent par une phase d'engouement (2015-2017) puis une phase de déception dans laquelle les premiers projets sont des échecs. Les utilisateurs de celle-ci se rendent compte des désavantages de la technologie, qu'elle n'est pas aussi parfaite qu'ils le pensaient. Après cette phase, dans laquelle les premiers pilotes ne sont pas une réussite, pas rentables, une phase de prospérité peut commencer. La technologie est plus mature et des utilisations plus adaptées à ses avantages peuvent être trouvées. Dans cette dernière phase, la technologie développe son intérêt et sa valeur ajoutée. Selon lui, nous ne sommes pas encore dans cette phase de prospérité. Aujourd'hui, la technologie n'est pas assez mature. Les coûts liés aux projets sont encore trop élevés. Par exemple, dans le projet B3i, les coûts des développeurs blockchain sont impressionnant, il faut compter entre 200 000 et 300 000€ par an pour un développeur. Le prix de certaines plateformes d'hébergement tel que « Hyperléger » est également onéreux. C'est d'ailleurs une des raisons pour laquelle B3i est sous la plateforme Corda. Une autre raison est que celle-ci propose plus de sécurité sur la confidentialité.

6.2. Interview de Patricia Boydens (Assuralia), 21 juin 2022

6.2.1. Présentation

Je suis consultante en innovation. Pour le moment, je suis en mission chez Datassur et Assuralia.

6.2.2. Avez-vous déjà eu recours à la technologie blockchain au sein de votre entreprise ?

Non, les entreprises dans lesquelles je travaille n'ont pas encore tenté l'expérience de la blockchain, en tout cas aucune application n'a concrètement été développée. J'ai fait une présentation d'informations sur la technologie et ses applications début de l'année 2022 chez Assuralia.

6.2.3. Quelles sont les applications / avantages de la technologie qui vous paraissent les plus pertinentes dans le secteur de l'assurance ?

-Les contrats intelligents sont un plus dans le secteur. Ils permettent l'automatisation. Cette automatisation permet de réduire les coûts et d'augmenter la vitesse des processus.

-La désintermédiation peut être très intéressante dans le secteur.

-La tokenisation pourrait également être intéressante dans le secteur pour certains produits tel que ceux de la branche 23. Les assureurs pourraient se passer des banques dépositaires et ainsi faire des économies.

6.2.4. Connaissez-vous des applications concrètes de la technologie dans le secteur de l'assurance en Belgique ?

En Belgique non. J'ai entendu parler de B3i en Europe. J'ai également entendu parler d'une certaine initiative du nom de « Schadevrije jaren » aux Pays-bas.

6.2.5. Quel est votre avis sur le futur de cette technologie dans le secteur de l'assurance en belgique / Europe ?

Selon moi, les régulations et les mentalités Européennes sont encore bloquantes aujourd'hui. Celles-ci freinent énormément le potentiel de la technologie. Pour prendre l'exemple de l'Asie, ils ont une manière totalement différente de gérer les données de la nôtre. Ils ont des bases de données beaucoup plus poussées et complètes. Ils ont énormément d'informations sur chaque individu. Avec cette mentalité différente et des régulations moins protectrices, la technologie blockchain peut plus facilement dévoiler son potentiel. Il est beaucoup plus facile d'imaginer des produits personnalisés en fonction des préférences des individus. Il est également plus facile d'automatiser des contrats ou des assurances paramétriques par exemple.

Selon moi, les régulations Européennes vont devoir s'adapter et changer à l'avenir de façon à mieux correspondre au monde de demain. La gestion actuelle des données ne pourra pas restée inchangée.

6.3. Interview de Koen Vingerhoets (Fujitsu), 25 juillet 2022

6.3.1. Présentation

Je suis titulaire d'une maîtrise en droit. Après mes études, j'ai commencé dans l'informatique : je programmais, je configurais des pare-feux, je m'occupais de l'architecture des bases de données, de la conception des applications, de l'helpdesk, de tout.

Ensuite, j'ai été avocat pendant une courte période. Par après, en 2008, je suis passé au secteur financier. Dans celui-ci, j'ai travaillé pendant plus de dix ans chez Delta Lloyd Life, KBC et Belfius. J'étais dans l'assurance chez Delta Lloyd Life et chez KBC.

Après 2020, je suis passé chez Deloitte Tax Illegal.

Depuis quelques mois, je travaille chez Fujitsu dans le centre de blockchain d'entreprise. Donc, ce que je fais essentiellement ou ce que je peux faire, c'est combiner des connaissances informatiques, des connaissances juridiques et des connaissances commerciales. Je ne suis pas un expert dans ces domaines, mais je peux parler avec des experts de ces différents domaines en les comprenant. Je peux ensuite faire le lien entre les différents domaines et avoir une vue générale. Je suis un peu comme une fonction de pont entre tout ce qui est lié à la blockchain. Mon titre chez Fujitsu peut être "évangéliste blockchain" ou "architecte d'entreprise. Je ne pense pas qu'il y ait d'expert blockchain, quelqu'un qui puisse tout couvrir. La blockchain aujourd'hui, c'est toute une industrie, ce n'est plus seulement le livre blanc du Bitcoin.

6.3.2. Avez-vous déjà eu recours à la technologie blockchain au sein de vos entreprises ?

J'ai déjà participé à beaucoup de projets liés à la technologie. En 2015, quand j'étais chez KBC, nous avons commencé à travailler sur la blockchain d'un point de vue stratégique. La blockchain était considérée comme d'importance stratégique et notre mission était de trouver des cas d'utilisation au sein du groupe KBC.

En 2016, nous avons exploré les cas d'utilisation. A l'époque tout était possible, tout était OK. Le mot d'ordre était : faisons d'abord quelque chose et ensuite voyons si ça a du sens. Nous avons donc testé quelques projets : concernant l'assurance auto et l'authentification des documents authentiques. Le secteur de l'assurance belge a collaboré dans l'objectif d'essayer de réaliser un projet blockchain basé sur une carte verte numérique (projet B-hive). L'idée était

bonne, mais elle a malheureusement été tuée par le gouvernement. Notre argument principal était les coûts, chaque année ces cartes vertes coûtaient 4 millions d'euros aux compagnies d'assurance. Nous sommes donc allés voir le gouvernement pour lui expliquer ce que nous voulons faire. Cependant, en Belgique, la plaque d'immatriculation est couverte par le GDPR car elle est liée à une personne et non à une voiture. Cette donnée était bloquante pour notre projet. Nous ne pouvions pas stocker sur une blockchain publique les plaques qui étaient considérées comme données personnelles. Nous voulions donc délier les plaques des individus.

Pour réduire les coûts, le gouvernement a alors autorisé l'impression des cartes vertes par les particuliers. Aujourd'hui, vous pouvez obtenir une carte verte numériquement et vous pouvez l'imprimer sur du papier blanc. Alors que le gouvernement pensait nous aider, il a en fait tué notre business case. Nous ne pouvions plus aller jusqu'au bout, nous ne pouvions plus expliquer à notre direction que nous avions besoin de quelque chose de numérique si tous les coûts disparaissaient d'un coup. Ils ont réduit les coûts et n'ont pas vu qu'il y avait un cas d'utilisation au-delà des frontières belges, une valeur ajoutée. Si vous heurtez quelqu'un de, disons, la Pologne, ce serait bien de savoir qu'il est réellement assuré. Il est facile de copier une carte verte. Il serait bien que si vous scannez la plaque d'immatriculation polonaise, vous obteniez également une simple mention "c'est bon, ces gars-là sont assurés".

Aujourd'hui, chez Fujitsu, je ne suis pas vraiment autorisé à parler de mon expérience personnelle, mais nous discutons avec deux grands groupes d'assureurs à propos d'un projet blockchain. Je ne peux malheureusement pas en dire plus. Fujitsu est une société de services et une société de services informatiques, donc nous recevons des questions des compagnies d'assurance pour les aider à développer leurs solutions blockchain.

6.3.3. Avez-vous toujours des projets de mise en œuvre liés à la technologie ?

Oui, bien sûr, nous en avons beaucoup chez Fujitsu mais ils ne sont pas liés à l'assurance. C'est l'une des raisons pour lesquelles j'ai changé pour Fujitsu. Ils travaillent globalement et ils ont des projets en production. Leurs projets mènent à des résultats.

6.3.4. Quelles sont les applications / avantages de la technologie qui vous paraissent les plus pertinentes dans le secteur de l'assurance ?

-La réduction des coûts, les gains d'efficacité, l'amélioration des choses de manière générale.

-La traçabilité.

-Amélioration de la traçabilité, suivi des données

-Assurance par utilisation

6.3.5. Connaissez-vous des applications concrètes de la technologie dans le secteur de l'assurance en Belgique ?

Claimshare de KPMG, c'est à peu près la seule que je connaisse, et je ne sais pas qui l'utilise. Je ne sais pas si ça marche vraiment ou pas.

6.3.6. Quel est votre avis sur le futur de cette technologie dans le secteur de l'assurance en belgique / Europe ?

Je pense que le secteur de l'assurance en Belgique se penche sur d'autres défis aujourd'hui, par exemple augmenter le nombre de contacts avec les clients. Je pense qu'il n'y a pas assez de collaboration pour obtenir des solutions qui pourraient aider l'ensemble du secteur. Le secteur bancaire s'en sort un peu mieux à ce niveau-là, ils collaborent plus. La technologie a beaucoup de potentiel mais le système actuel marche tel qu'il est. Les compagnies d'assurance sont largement rentables.

Le secteur doit également faire face à de nombreuses régulations.

6.4. Interview de Tobias Ambühl (Axa Suisse), 28 juillet 2022

Interview traduite de l'anglais vers le français

6.4.1. Présentation

Je suis directeur technologique et des plateformes digitales pour AXA Suisse. Je m'occupe des équipes de robotiques, d'intelligence artificielle, des ingénieurs en innovation, des managers de projets, de l'équipe cloud, etc. Nous allons sûrement encore grandir dans un futur proche.

6.4.2. Avez-vous déjà eu recours à la technologie blockchain au sein de vos entreprises ?

Oui, plusieurs projets ont déjà eu lieu chez AXA Suisse, il est facile d'en retrouver certains sur le net. Depuis que je suis rentré en fonction, début de cette année, nous nous sommes pas encore lancés dans de vrais projets concernant la technologie. Pendant une courte période, nous avons accepté le bitcoin comme moyen de paiement pour certains produits. Mais, aujourd'hui, cela a été mis en attente. Les questions ESG sont très importantes aujourd'hui et un groupe aussi grand qu'AXA ne pouvait pas se permettre d'accepter le Bitcoin par peur de scandale écologique.

6.4.3. Avez-vous toujours des projets de mise en œuvre liés à la technologie ?

Oui, nous avons commencé à expérimenter certains cas d'utilisation autour de la tokenisation et des identités décentralisées. Nous nous efforçons de trouver des cas d'utilisation dans lesquels la technologie pourrait démontrer son utilité. Nous essayons de laisser de côté tout ce qui concerne la finance, la DEFI (finance décentralisée) qui est déjà largement traité. Nous nous intéressons plus à des projets liés aux aspects WEB3 de la technologie. Dans cette idée, nous voulons aider les clients à être maitre de leurs données. Nous développons une application pour aider les consommateurs à rester en possession de leurs données lors de la recherche d'appartement. Par exemple, ici à Zurich, lorsque nous cherchons un nouveau lieu de vie, il n'est pas rare d'envoyer nos fiches de salaire, nos données sensibles à plus de 20-30

propriétaires. Selon moi, cela n'est plus possible aujourd'hui et la technologie blockchain pourrait aider dans ce type de cas d'utilisation.

6.4.4. Quelles sont les applications / avantages de la technologie qui vous paraissent les plus pertinentes dans le secteur de l'assurance ?

Je pense qu'il y a deux grands domaines dans lesquels le secteur des assurances pourrait utiliser la DLT :

- *dans le domaine du risque : par exemple, la tokenisation du risque,*
- *dans le domaine de la confiance : aider les clients à retrouver l'autorité sur leurs identités et leurs données numériques. Aujourd'hui, nous sommes trop dépendant des grands acteurs du web tels que Google, Méta, Amazone. Ils détiennent pratiquement tous les pouvoirs sur internet en contrôlant les données. Ils peuvent décider de vos accès à certains sites, ils savent ce que vous consommez, ce que vous faites, ils détiennent vos mots de passe, etc.*

6.4.5. Quel est votre avis sur le futur de cette technologie dans le secteur de l'assurance en belgique / Europe ?

Il y a quelques mois, notre groupe CEO, Thomas Buberl, a annoncé qu'il était convaincu du potentiel de la technologie Blockchain. Tourner le dos à cette technologie n'est plus une option. Je suis convaincu de l'utilité de la blockchain dans les deux avantages mentionnés dans la questions précédente.

BIBLIOGRAPHIE

Actualité Informatique. (s.d.). *Civic Cryptomonnaie CVC - Définition*. Récupéré sur Actualité Informatique: https://actualiteinformatique.fr/cryptomonnaie/definition-cryptomonnaie-civic#:~:text=Civic%20est%20un%20protocole%20de,mieux%20g%C3%A9rer%20les%20identit%C3%A9s%20num%C3%A9riques.

Assuralia. (2021, Octobre 28). *Chiffres clés et principaux résultats de l'assurance belge en 2020*. Récupéré sur Assuralia: https://www.assuralia.be/fr/home/47-etudes-et-chiffres/etudes-d-assuralia/237-les-principaux-chiffres-du-marche-belge-de-l-assurance-en-2020

Assuralia. (2021). *Rapport annuel 2021.* Récupéré sur Assuralia: https://www.assuralia.be/rapportannuel2021/index.html?utm_source=assuralia.be&utm_medium=website&utm_campaign=site

Assuralia. (s.d.). *Lutte contre la fraude.* Récupéré sur Assuralia: https://www.assuralia.be/fr/infos-secteur/fonctionnement-de-l-assurance/377-lutte-contre-la-fraude

Assurance Vie Luxembourg. (2022, Février 21). *Rôle du dépositaire au Luxembourg*. Récupéré sur Assurance Vie Luxembourg: https://www.assurancevieluxembourg.fr/role-du-depositaire-au-luxembourg-assurance-vie-luxembourg/

AXA. (2017, Septembre 13). *AXA goes blockchain with fizzy*. Récupéré sur AXA: https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy

B3i. (2022). *NUCLEAR POOLS*. Récupéré sur B3i: https://b3i.tech/pools/

B3i. (s.d.). *Fluidity*. Récupéré sur B3i: https://b3i.tech/fluidity/

B3i. (s.d.). *Whitepaper B3i*. Récupéré sur B3i: https://inbound.b3i.tech/hubfs/Legally%20Binding%20-%20A%20Step%20Forward%20-%20Whitepaper%20-%20B3i.pdf

Banque Européenne d'investissement. (2021, Avril 28). *La BEI émet sa toute première obligation numérique sur une chaine de blocs publique*. Récupéré sur Banque Européenne d'investissement: https://www.eib.org/fr/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain#:~:text=Le%2027%20avril%202021%2C%20la%20BEI%20a%20lanc%C3%A9%2C,l%E2%80%99enregistrement%20et%20le%20r%C3%A8glement%20des%20t

Bercy infos. (2022, Avril 12). *Qu'est-ce que la blockchain ?* Récupéré sur Ministère des finances et de l'économie: https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application#:~:text=Une%20blockchain%20est%20un%20registre,par%20un%20protocole%20informatique%20tr%C3%A8s

Berné, R. (2020, Novembre 8). *Blockchain : avantages et inconvénients.* Récupéré sur Cryptoast: https://cryptoast.fr/blockchain-avantages-inconvenients/

Binance Academy. (2022, Mars 30). *Avantages et inconvénients de la Blockchain.* Récupéré sur Binance Academy: https://academy.binance.com/fr/articles/positives-and-negatives-of-blockchain

Binance Academy. (2022, Mars 22). *Qu'est-ce que le minage de cryptomonnaie ?* Récupéré sur Binance Academy: https://academy.binance.com/fr/articles/what-is-cryptocurrency-mining

Bit2me Academy. (2021). *Les transactions Bitcoin, comment fonctionnent-elles?* Récupéré sur Bit2me Academy: https://academy.bit2me.com/fr/transactions-Bitcoin/

Blockchain France. (2016, Mai 12). *Qu'est-ce q'une DAO?* Récupéré sur Blockchain France: https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/

Buterin, V. (2014). *Ethereum Whitepaper.* Récupéré sur Ethereum: https://ethereum.org/en/whitepaper/?fbclid=IwAR34Fw59xIPDTWG2pXOit_ojdyPQOJwtyShEPHyu3VDL7IVTx-kYqxUtyjM

Buterin, V. (2017, Février 06). *The Meaning of Decentralization*. Récupéré sur Medium: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274#.57gocynsr

Cardossier. (2022). *Managing the life cycle of a car with blockchain technology*. Récupéré sur Cardossier: https://cardossier.ch/

Chainlink. (2021, Septembre 14). *What Is a Smart Contract?* Récupéré sur Chainlink: https://chain.link/education/smart-contracts?utm_medium=paid-search&utm_source=google-adwords&utm_campaign=defi-oracle&utm_content=educational-page&gclid=EAIaIQobChMI4-LR5rjw9wIVEQOLCh1X0QUyEAAYASAAEgKBgPD_BwE

Civic. (2017). *Whitepaper*. Récupéré sur Civic: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

CNRTL. (2012). *Réassurance*. Récupéré sur Centre National de Ressource Textuelles et Lexicales: https://www.cnrtl.fr/definition/r%C3%A9assurance

coinmarketcap. (s.d.). *Cryptocurrency Prices by Market Cap.* Consulté le Juillet 31, 2022, sur coinmarketcap: https://coinmarketcap.com/

Commission Européenne. (2021, Juillet 20). *Regulation of the European parliament and the council on information accompanying transfers of funds and certain crypto-assets.* Récupéré sur European Commission: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0422

Countryeconomy. (s.d.). *Belgique - PIB - Produit intérieur brut*. Consulté le Juillet 31, 2022, sur Countryeconomy: https://fr.countryeconomy.com/gouvernement/pib/belgique

Cryptonaute. (2019, Aout 2). *B3i dévoile un premier produit conçu sur la plateforme blockchain Corda*. Récupéré sur Cryptonaute: https://cryptonaute.fr/b3i-annonce-premier-produit-blockchain-corda/

Cuvva. (s.d.). *Temporary car insurance*. Récupéré sur Cuvva: https://www.cuvva.com/car-insurance/temporary

de La Raudière, L., & Mis, J.-M. (2018). *Rapport de la mission d'information commune : la blockchain (chaîne de blocs) et ses usages.* Assemblée Nationale. Récupéré sur Ministère de l'économie des finances et de la relance.

Deloitte. (2017). *Blockchain Risk Management.* Récupéré sur Deloitte: https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html

Deloitte. (2018). *Evolution of blockchain technology.* Récupéré sur Deloitte: https://www2.deloitte.com/tr/en/pages/financial-services/articles/evolution-of-blockchain-technology.html

Deloitte. (2021). *Deloitte's 2021 Global Blockchain Survey.* Récupéré sur Deloitte: https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf

Double dépense. (2020, Juin 02). Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Double_d%C3%A9pense

Elkaim, J. (2021, Juillet 19). *Blockchain et données à caractère personnel : les contraintes d'une cohabitation numérique*. Récupéré sur Village de la justice: https://www.village-justice.com/articles/blockchain-donnees-caractere-personnel-les-contraintes-une-cohabitation,39703.html

epatrimoine. (s.d.). *Qu'est ce que l'assurance-vie?* Récupéré sur epatrimoine: https://epatrimoine.fr/definition-assurance-vie

Ethereum. (2022, Juin 17). *ETHEREUM DEVELOPMENT DOCUMENTATION.* Récupéré sur Ethereum: https://ethereum.org/en/developers/docs/

European Insurance and Occupational Pensions Authority. (2019, Mars 19). *Report on best practises on licencing requirements, peer-to-peer insurance and the principle of proportionality in an insurtech context*. Récupéré sur EIOPA: https://www.eiopa.europa.eu/document-library/report/report-best-practises-licencing-requirements-peer-peer-insurance-and_en

European Insurance and Occupational Pensions Authority. (2021). *Discussion paper on blockchain and smart contracts in insurance.* Récupéré sur EIOPA : https://www.eiopa.europa.eu/sites/default/files/publications/consultations/eiopa-discussion-paper-on-blockchain-29-04-2021.pdf

eurostat. (2021, Décembre 20). *Which EU countries had the highest GDP in 2020?* Récupéré sur eurostat: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211220-1

Fausse, S. N.-F. (s.d.). *Bitcoin : un système de paiement électronique pair-à-pair.* Récupéré sur BitcoinFr: https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf

Fénéron Plisson, C. (2017). *La blockchain, un bouleversement économique, juridique voire sociétal.* Récupéré sur Cairn: https://www.cairn.info/revue-i2d-information-donnees-et-documents-2017-3-page-20.htm

Finck, D. M. (2019, Juillet). *Blockchain and the general data protection regulation*. Récupéré sur European Parliamentary Research Service: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018, Avril). *To Blockchain or Not to Blockchain: That is the question.* Récupéré sur IEEE Comptuter Society: https://ieeexplore.ieee.org/document/8338007

Georgiadis, E. (2019, Avril). *How many transactions per second can bitcoin really handle ?* Récupéré sur ePrint: https://eprint.iacr.org/2019/416.pdf

Geroni, D. (2021, Aout 16). *Everything You Need To Know About Tokenization.* Récupéré sur 101 Blockchains: https://101blockchains.com/tokenization-blockchain/

GUEGAN, D. (2017). *Blockchain Publique versus Blockchain Privée : Enjeux et Limites.* Récupéré sur Université Paris 1 Panthéon –Sorbonne: https://halshs.archives-ouvertes.fr/halshs-01673321/file/17053.pdf

Guide-épargne. (2022). *Comparer les assurances investissement de la branche 23*. Récupéré sur Guide-épargne: https://www.guide-epargne.be/epargner/branche-23.html?referrer=https%3A%2F%2Fwww.google.be%2F

Huckstep, R. (2015). *Cuvva launches an InsurTech app for short term, instant car insurance*. Récupéré sur Daily Fintech: https://dailyfintech.com/2015/12/17/cuvva-launches-an-insurtech-app-for-short-term-instant-car-insurance/

IBM. (2022). *Basic blockchain security*. Récupéré sur IBM: https://www.ibm.com/topics/blockchain-security

IBM. (s.d.). *Avantages de la blockchain.* Récupéré sur IBM: https://www.ibm.com/fr-fr/topics/benefits-of-blockchain#:~:text=La%20blockchain%20accro%C3%AEt%20la%20confiance,en%20introduisant%20une%20efficacit%C3%A9%20nouvelle.

IBM. (s.d.). *Qu'est ce que la technologie de blockchain.* Récupéré sur IBM: https://www.ibm.com/fr-fr/topics/what-is-blockchain

indexa capital. (2021, Fevrier 05). *Quels sont les frais facturés par la banque dépositaire pour ses services de garde et de courtage ?* Récupéré sur indexa capital: https://support.indexacapital.com/fr/bel/commissions-banque-depositaire-et-courtage

Iredale, G. (2020, Novembre 03). *History Of Blockchain Technology: A Detailed Guide*. Récupéré sur 101 Blockchains: https://101blockchains.com/history-of-blockchain-timeline/

Iredale, G. (2020, Avril 17). *Top Disadvantages Of Blockchain Technology*. Récupéré sur 101 Blockchains: https://101blockchains.com/disadvantages-of-blockchain/

ISIFI Conseil. (2022). *LEs services aux investisseurs des dépositaires.* Récupéré sur Fimarkets: https://www.fimarkets.com/pages/services_investisseurs_depositaire.php

Jérusalmy, O. (2018, Mars). *La technologie blockchain : support d'innovation en matière d'assurance*. Récupéré sur Financité: https://www.financite.be/sites/default/files/references/files/la_technologie_blockchain_support_dinnovation_en_matiere_dassurance_.pdf

Jiachi, C., Xin, X., David, L., & John, G. (2020, Mai). *Why do Smart Contracts Self-Destruct? Investigating the Selfdestruct function on ethereum.* Récupéré sur ResearchGate: https://www.researchgate.net/publication/341478354_Why_Do_Smart_Contracts_Self-Destruct_Investigating_the_Selfdestruct_Function_on_Ethereum

Julija, G., & Andrejs, R. (2018, Novembre). *The Advantages and Disadvantages of the Blockchain Technology.* Récupéré sur ResearchGate:

https://www.researchgate.net/publication/330028734_The_Advantages_and_Disadvantages_of_the_Blockchain_Technology

Kar, A., & Navin, L. (2020, Novembre 16). *Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature.* Récupéré sur Elsevier: https://reader.elsevier.com/reader/sd/pii/S073658532030191X?token=A4265372066BDD9009E5103D40F5D7ADAAB708E57A2A73AAEBC64178675C4CEF739FD8D6EBA70D02D316F9623E6BD781&originRegion=eu-west-1&originCreation=20220619122126

König, L., Unger, S., Kieseberg, P., & Tjoa, S. (2020). *The Risks of the Blockchain.* Récupéré sur jisis: https://isyou.info/jisis/vol10/no3/jisis-2020-vol10-no3-06.pdf

Lars, L. (2020, Août 10). *Blockchain publique et blockchain privée : quelles différences ?* Récupéré sur Cryptoast: https://cryptoast.fr/differences-blockchain-publique-blockchain-privee/

Lars, L. (2020, Février 1). *La crypto-monnaie peut-elle se démocratiser de manière décentralisée ?* Récupéré sur Cryptoast: https://cryptoast.fr/bitcoin-democratisation-decentralisation/

Lars, L. (2020, Août 22). *Qu'est-ce qu'un bloc dans la technologie blockchain ?* Récupéré sur Cryptoast: https://cryptoast.fr/bloc-blockchain-crypto-explication/#:~:text=Un%20bloc%2C%20ou%20block%20en,ou%20contenir%20des%20donn%C3%A9es%20arbitraires.

L'histoire de la Blockchain. (2018, Décembre 06). Récupéré sur Binance Academy: https://academy.binance.com/fr/articles/history-of-blockchain

M.Antonopoulos, A. (2017). *Mastering Bitcoin.* O'Reilly.

Maire, V. (2022, Mai 24). *BNP Paribas utilise désormais la blockchain de JP Morgan pour ses opérations financières.* Récupéré sur Cryptoast: https://cryptoast.fr/bnp-paribas-utilise-blockchain-jp-morgan-operations-financieres/

Manuel, S. (2011, Mars 03). *Analyse et conception de fonctions de hachage.* Récupéré sur HAL open science: https://pastel.archives-ouvertes.fr/pastel-00573346/document

Melchior, E. (2018). *Réflexions juridiques autour de la blockchain : analyse sous l'angle du droit des contrats.* Récupéré sur Revue du droit des technologies de l'information: http://www.crid.be/pdf/public/8457.pdf

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Récupéré sur Bitcoin: https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies.* Princeton University Press.

NS Insurance. (2019, Aout 01). *B3i releases property catastrophe excess of loss product Cat XoL v1.0*. Récupéré sur NS Insurance: https://www.nsinsurance.com/news/b3i-releases-property-catastrophe-excess-of-loss-product-cat-xol-v1-0/

Oberhaus, D. (2018, Septembre 03). *La plus vieille blockchain du monde se cache dans le New York Times depuis 1995*. Récupéré sur Vice: https://www.vice.com/fr/article/j5nzx4/la-plus-vieille-blockchain-du-monde-se-cache-dans-le-new-york-times-depuis-1995

Online tools. (2017). *Sha 256*. Récupéré sur online tools: https://emn178.github.io/online-tools/sha256.html

Paperno, A., Kravchuk, V., & Porubaev, E. (2016). *Whitepaper Teambrella : a Peer-to-Peer Coverage System*. Récupéré sur Teambrella: https://neironix.io/documents/whitepaper/5742/whitepaper.pdf

PAVEL, I. (2019, Novembre). Réalités industrielles. *série des annales des mines*, pp. 98-104.

Pengloan, A. (2020, janvier 26). *C'est quoi l'assurance paramétrique ? Définition et cas d'usage*. Récupéré sur Eficiens: https://www.eficiens.com/assurance-parametrique-definition/

Poelstra, A. (2015, Mars 22). *On Stake and Consensus.* Récupéré sur Pos: https://download.wpsoftware.net/bitcoin/pos.pdf

Popovic, D., Avis, C., Byrne, M., Cheung, C., Donovan, M., Flynn, Y., . . . Shah, J. (2020). *Understanding blockchain for insurance use cases.* Récupéré sur Cambridge University Press: https://www.cambridge.org/core/journals/british-actuarial-journal/article/understanding-blockchain-for-insurance-use-cases/3F0FBE7A633CE3EAC2CEA0DD98A63286

PwC. (2017, Janvier 20). *Blockchain, a catalyst for new approches in insurance.* Récupéré sur PwC: https://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-a-catalyst.html

PWC. (2018, Aout 28). *PwC study shows four out of five executives surveyed (84%) report blockchain initiatives underway.* Récupéré sur PWC: https://www.pwc.com/sk/en/current-press-releases/pwc-blockchain-initiatives-underway.html

Qu'est-ce que la blockchain ? (2022, mai). Récupéré sur Ministère de l'économie et des finances: https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application#:~:text=Une%20blockchain%20est%20un%20registre,par%20un%20protocole%20informatique%20tr%C3%A8s

Rocher, A. (2022, Mai 13). *Régime pilote : une réglementation expérimentale au service de l'innovation*. Récupéré sur Société Générale: https://www.securities-services.societegenerale.com/fr/insights/views/news/regime-pilote/

Sayegh, K. (2018, Octobre). *Blockchain Application in Insurance and Reinsurance*. Récupéré sur researchgate: https://www.researchgate.net/publication/327987901_Blockchain_Application_in_Insurance_and_Reinsurance

Schenk, L., & Gineste, P. (2022, Mai 07). *Réglementation Européenne des cryptommonaies : Mica, frein à l'innovation ou cadre approprié?* Récupéré sur Journal du coin: https://journalducoin.com/analyses/reglementation-europe-cryptomonnaies-mica-frein-cadre-adapte/

Sheldon, R. (2021, Aout 09). *A timeline and history of blockchain technology*. Récupéré sur Techtarget: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

Supernova. (2018). *Blockchain.* Récupéré sur Wikiwai: http://www.wikiwai.com/informatique-technologie/gestion_des_donnees/blockchain/2018/supernova/premiers-pas-sur-la-blockchain-un-guide-pour-debuter/#Resume_de_la_publication

Taher, I. B. (2018, Janvier 22). *blockchain et assurance entre ambition et réalité : les risques et le cadre réglementaire*. Récupéré sur Wavestone: https://www.insurancespeaker-

wavestone.com/2018/01/blockchain-assurance-entre-ambition-realite-risques-cadre-reglementaire/

Tarr, J.-A. (2018). *Distributed ledger technology, blockchain and insurance: opportunities, risks and challenges.* Récupéré sur Queensland University of Technology: https://eprints.qut.edu.au/122862/2/122862.pdf

Temperli, D. (2018, Octobre 13). *En quoi la blockchain est-elle si intéressante pour les assurances*. Récupéré sur AXA: https://www.axa.ch/fr/blog/entreprises/gruendung-innovation/blockchain-assurances-suisse.html

Terry, H. (2017). *Teambrella – Bitcoin enabled P2P insurance*. Récupéré sur The digital Insurer: https://www.the-digital-insurer.com/dia/teambrella-bitcoin-enabled-p2p-insurance/

Vergne, J. (2020). *Decentralized vs. Distributed Organization: Blockchain, Machine Learning and the Future of the Digital Platform.* Récupéré sur Sage: https://journals.sagepub.com/doi/pdf/10.1177/2631787720977052

Wikipedia. (2022, Juillet 17). *Economy of the European Union*. Récupéré sur Wikipedia: https://en.wikipedia.org/wiki/Economy_of_the_European_Union#:~:text=The%20European%20Union's%20GDP%20was,6%20of%20the%20global%20economy.&text=447%2C706%2C209%20(EU27%2C%201%20January%202020,est.)&text=(2016%20est.)

Wikipedia. (2022, Février). *Extensibilité.* Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Extensibilit%C3%A9

Wikipédia. (2022, Juillet 05). *Preuve de concept*. Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Preuve_de_concept

Wikipédia. (2022, juin 16). *Réassurance*. Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/R%C3%A9assurance

Yerramsetti, S. K. (2018). *Blockchain: Emerging Use Cases for Insurance*. Récupéré sur IBM Global Business Services: https://www.the-digital-insurer.com/wp-content/uploads/2019/02/1409-Blockchain-Emerging-Use-Cases-for-Insurance.pdf

Résumé

Ces dernières années, la blockchain est entrée dans le langage courant. Pourtant, souvent associée aux cryptomonnaies, elle souffre d'un déficit d'image. La complexité de la technologie en est notamment la cause. Un des objets de ce mémoire est de vulgariser les concepts qui sous-tendent le fonctionnement de cette technologie novatrice. Une analyse de ses avantages et de ses inconvénients est réalisée. Après avoir assimilé les bases de la blockchain, ses applications dans le secteur de l'assurance européen ont été étudiées. En particulier, l'utilisation de la technologie des registres distribués permet la réduction des coûts, l'optimalisation de la gestion et la création de nouveaux produits. Pour démontrer le fonctionnement de la blockchain et illustrer ses atouts, une application de souscription d'un contrat de responsabilité civile familiale a été développée. Enfin, des acteurs du secteur de l'assurance ont dressé un état des lieux de l'utilisation actuelle de la technologie en Belgique et en Europe.

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
Louvain School of Management
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve
Boulevard Emile Devreux 6, 6000 Charleroi, Belgique
Chaussée de Binche 151, 7000 Mons, Belgique
www.uclouvain.be/lsm