☐ Copie Juré
☐ Copie Conseiller
☐ Copie Infothèque

h e g

Haute école de gestion
Genève

Comment intégrer la blockchain à l'assurance pair-à-pair ?

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

<Alessandro BARBIERI

Conseiller au travail de Bachelor :

Naoufel Cheikrouhou, professeur HES

Genève, le 15 juillet 2021

Haute École de Gestion de Genève (HEG-GE)

Filière économie d'entreprise

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science en économie d'entreprise.

L'étudiant a envoyé ce document par email à l'adresse d'analyse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND. http://www.urkund.com/fr/student/392-urkund-faq

L'étudiant atteste avoir réalisé seul-e le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

Remerciements

Je tiens à remercier toutes les personnes qui m'ont accompagné tout au long de mon parcours universitaire au sein de la Haute Ecole de Gestion de Genève.

Je tiens à remercier le Professeur Naoufel CHEIKROUHOU ainsi que son assistante Felicia.SOULIKHAN qui m'ont soutenu et accompagné tout au long de ce travail

J'aimerais également remercier le Professeur Rolf HAURI pour son aide et ses conseils.

Résumé

Dans ce travail, nous allons voir les traits principaux de la blockchain et de l'assurance pair-à-pair. Dans le but de répondre à la problématique suivante : *Comment peut-on intégrer la blockchain avec l'assurance pair-à-pair ?*

La blockchain est considérée comme un grand livre dans lequel toutes les transactions sont stockées et peuvent être vues par toutes les personnes faisant parties du réseau. C'est cette technologie qui a permis la venue du bitcoin. En ce qui concerne l'assurance pair-à-pair, c'est une assurance dans laquelle on enlève l'assureur du processus. Ainsi c'est un ensemble de personnes qui vont se dédommager entre eux en cas de sinistres, permettant une baisse des primes payées par les assurés.

Tout au long de ce travail, nous avons comme objectif l'impact de la blockchain sur la confiance ainsi que la transparence pour les membres de l'assurance pair-à-pair. Vous allez voir que la recommandation répondant à cette problématique étant les smarts-contracts, qui est du code qui va permettre de déployer un contrat qui sera stocké dans la blockchain et où tout le monde pourra avoir accès aux informations de ce contrat.

Table des matières

Liste des tableaux

Liste des figures

1. Introduction

Ces dernières années nous avons pu voir apparaître de nouvelles entreprises qui régissent sous le nom de « fintech ». Un des domaines dans lequel il y a le plus de ces starts up qui se sont créés, sont dans le domaine des assurances. En 2015, 8% des fintechs étaient des assurances, en 2019 nous sommes à près de 50%. Uniquement l'industrie bancaire arrive devant. [1]

Après la banque c'est au tour de l'industrie de l'assurance qui se fait attaquer par les fintechs. De ce fait de nombreuses type d'insurtech sont nés tel que :

- Sites de comparaison
- Courtiers digitaux
- Assurances « cross sellers»
- Assurances pair-à-pair
- Assurances à la demande
- Assurances digitales
- Analyse de Big Data & logiciel d'assurances
- Internet des objets
- Blockchain & smart contracts [2]

Comme on peut le voir il existe de nombreuses catégories différentes dans lesquelles de nouvelles starts up voient le jour. Une des assurances qui semble être la plus intéressante et qui pourrait complètement perturber le marché de l'assurance traditionnel est celui de l'assurance pair-à-pair qui fonctionne comme une mutuel. C'est-à-dire que ce sont les personnes qui font parties du réseau qui vont indemniser la personne lésée par un quelconque accident. A la fin d'une période (annuellement par exemple), s'il reste de l'argent au sein du « pool » créé il sera soit rendu aux différents membres ou bien il sera déduit sur la prime de l'année suivante voire même reverser à des associations

1 ERNST YOUNG, 2019. Global Fintech Adoption Index 2019 [en ligne] . [Consulté le 31 mars 2021]. Disponible à l'adresse : https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf

2 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 31 mars 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

caritatives. Mais cette décision est différente d'une start up à une autre. Il existe une technologie/protocole qui a vu le jour ces dernières années et qui pourrait être combinée avec l'assurance pair-à-pair. Cette technologie est la blockchain. Dans ce travail je tenterais d'analyser quel est l'impact de la blockchain en termes de confiance et de transparence pour les utilisateurs de l'assurance pair-à-pair.

La structure de la blockchain ainsi que de l'assurance pair-à-pair fonctionne de la même manière, c'est-à-dire en réseau pair-à-pair. D'un côté nous avons des personnes qui s'assurent entre elles en formant un réseau. De l'autre côté nous avons une technologie/protocole qui permet de stocker des informations dans des blocs qui vont être validés par les différents membres du réseau.[3] Il est donc intéressant de se demander comment la blockchain peut-elle agir, étant donné leurs similitudes au niveau des caractéristiques, mais surtout de savoir s'il est réellement possible d'utiliser cette technologie à cette fin.

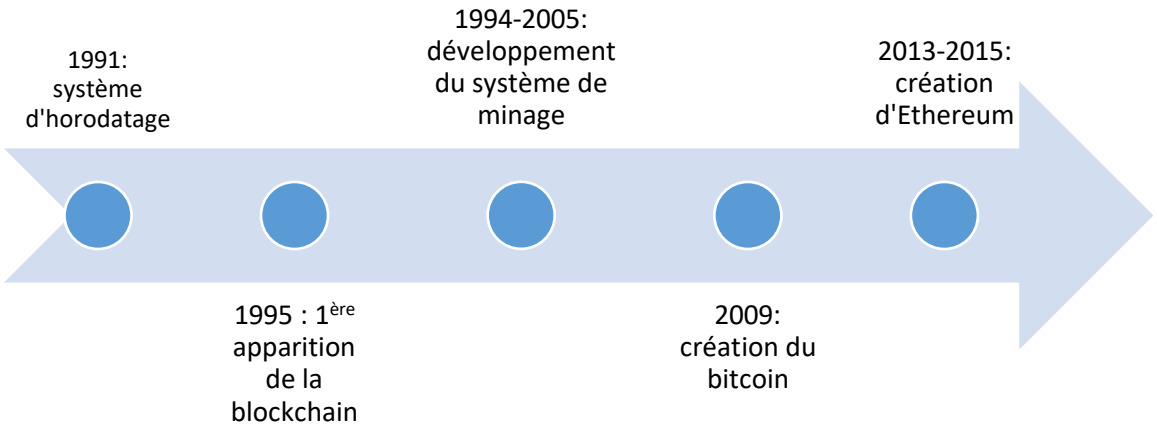
3 BRAUN, Alexander; SCHREIBER, Florian 2017.*The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 31 mars 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

2. La blockchain

2.1 Histoire et définition

Lorsque la blockchain a vu le jour en 1991, ce n'était qu'uniquement un système d'horodatage. C'est tout simplement associer une date à un événement. Pendant près d'une décennie, Nick Szabo, qui est perçu comme l'inventeur du bitcoin, développe cette crypto-monnaie qui est alors inconnue à cette époque, ainsi que le minage qui est un des rouages essentiels au bon fonctionnement de la blockchain et des cryptos-monnaies. Ensuite en 1995, nous avons véritablement la première blockchain de l'histoire apparue dans le New-York Times. A ce jour, elle reste la plus ancienne chaine de bloc au monde. Après le développement du minage ainsi que de la crypto-monnaie, le bitcoin est découvert par le grand public. De 2013-2015, une plateforme est développée par Vitalik BUTERIN, ainsi qu'une crypto-monnaie. Cette plateforme et cette crypto-monnaie se nomme Ethereum. [4]

Tableau 1: Frise chronologique blockchain



MARRAST, 2018, pp. 2

[4] MARRAST Philippe 2018. *Blockchain: Éléments d'explication et de vulgarisation, Pourquoi s'intéresser à la blockchain aujourd'hui ?* [en ligne] Blockchain et Santé : Perspectives d'applications et enjeux juridiques (Séminaire IFERISS), IFERISS, Oct 2018, Toulouse, France. hal-0197350 [consulté le1 mars 2021]. Disponible à l'adresse : https://hal.archives-ouvertes.fr/hal-01973507/document

Pinyaphat TASATANATTAKOOL et Chian TECHAPANUPREEDA définissent la blockchain dans un article nommé « *Blockchain : Challenges and Applications* » de cette manière : « *Blockchain is a form of database storage that is non- centralized, reliable, and difficult to use for fraudulent purposes.* » [5] (*TASATANATTAKOOL & TECHAPANUPREEDA, 2018, PP.1*) La blockchain est tout simplement une chaine de blocs dans lesquels toutes les transactions sont validées et stockées de manière chronologique sous forme de grand livre. Ce grand live est distribué, et il est donc difficile de le corrompre.

Lorsqu'on parle de grand livre, on parle de registre où toutes les transactions vont être inscrites. Ces transactions vont être enregistrées comme dans un journal en comptabilité, avec les notations de débit et de crédit.

Tableau 2: Grand livre

Grand livre				
Date	**Description**	**Débit**	**Crédit**	Solde
11 mars 21	Solde précédant			*300'000*
12 mars 21	Achat de marchandises	100'000		*200'000*
15 mars 21	Achat de machines	50'000		*150'000*
16 mars 21	Vente de marchandises		80'000	*230'000*
17 mars 21	Frais de voyages	10'000		*220'000*
18 mars 21	Ventes de marchandises		30'000	*250'000*

Sapra, Dhaliwal, 2021, pp.3

Lorsqu'une nouvelle transaction va être lancée, elle va directement être inscrite dans le registre du grand livre, sans que quelconque tiers le mette à jour. Quand on parle de transactions, il peut s'agir d'une transaction en crypto-monnaie comme avec du bitcoin, mais également tout simplement des transferts de données d'un appareil à un autre comme c'est le cas dans l'Internet des objets (IoT), ou bien cela peut être également du code brut dans le cadre de l'élaboration d'un smart contract.[6]

5 P. TASATANATTAKOOL and C. TECHAPANUPREEDA,2018. *Blockchain: Challenges and applications,*[en ligne] 2018 International Conference on Information Networking (ICOIN), 2018, pp. 473-475, doi: 10.1109/ICOIN.2018.8343163. [consulté le 1er mars 2021]. Disponible à l'adresse :https://ieeexplore.ieee.org/abstract/document/8343163

6 SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 1er mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

2.2 Structure

2.2.1 Première génération de blockchain

Il faut savoir qu'il existe principalement 2 générations de blockchains. La première est celle qui a été mise en place en 2008 avec le Bitcoin par Satoshi Nakamoto. La structure de cette première version de blockchain est composée d'un entête de bloc (Block Header) ainsi que du corps du bloc (Block Body). Dans l'entête du bloc nous avons :

- La version
- le hash du bloc précédent
- l'horodatage
- le nonce
- le « bit »
- le merkle root

La version est tout simplement, la version du bloc puisque comme tout outil issu de l'informatique, les blocs ont des versions différentes car des mises à jour ont été faites à travers le temps afin d'améliorer le système.

Le hash est un ensemble de caractères qui provient d'une fonction de hachage. Cette fonction, va permettre de convertir des données en une empreinte numérique à travers un algorithme. L'algorithme en question dans la blockchain est le sha-256. Cet algorithme de hachage est une des versions proposées par la NSA depuis 1993 afin d'offrir une solution dans la certification de fichiers pour les autorités qui les distribuent[7]. Cette empreinte sera longue de 256 bits. De ce fait, dans l'entête du bloc, nous aurons le hash du bloc précédant. Dans le bloc N, nous aurons le hash du bloc N-1, dans le bloc N-1 il y aura le hash du bloc N-2. [8]

[7] TBS CERTIFICAT. Tout sur les algorithmes de hachage SHA1, SHA2 et le SHA 256. Tbs-certificat [en ligne].[Consulté le 1er mars 2021].Disponible à l'adresse : https://www.tbs-certificats.com/FAQ/fr/sha256.html

[8] TABORA Vincent, 2019. A decomposition of the Bitcoin Block Header. Data Driven Investor. [en ligne] 21 novembre 2019 [consulté le 1er mars 2021]. Disponible à l'adresse : https://www.datadriveninvestor.com/2019/11/21/a-decomposition-of-the-bitcoin-block-header/

L'horodatage de chaque bloc est tout simplement le temps en secondes depuis la création du bloc. Le nonce est un numéro d'authentification qui va permettre d'éviter que les informations soient manipulées. Il est souvent rattaché au hash, afin qu'un hash ne puisse être utilisé qu'une seule fois. [9]

Dans un bloc, chaque transaction aura une empreinte qui y sera définie par l'algorithme. Ensuite, toutes ces transactions ne vont former qu'une seule et même empreinte car on va les associer à une seule empreinte, qui sera celle du bloc. Cette empreinte s'appelle le root hash. Et ensuite le bloc suivant, prendra en compte le root hash du bloc précédent pour définir sa propre empreinte numérique.

L'autre des éléments de l'entête du bloc est le bit qui est simplement le niveau de difficulté de minage qui est lié aux nombres de « 0 » qu'il y a dans le nonce, qu'il faut trouver (résultat du calcul) dans le processus de validation des transactions (proof of work) que nous allons traiter plus bas. On parle donc de difficulté de minage car plus il y a de 0, plus il est difficile de trouver le résultat. [10]

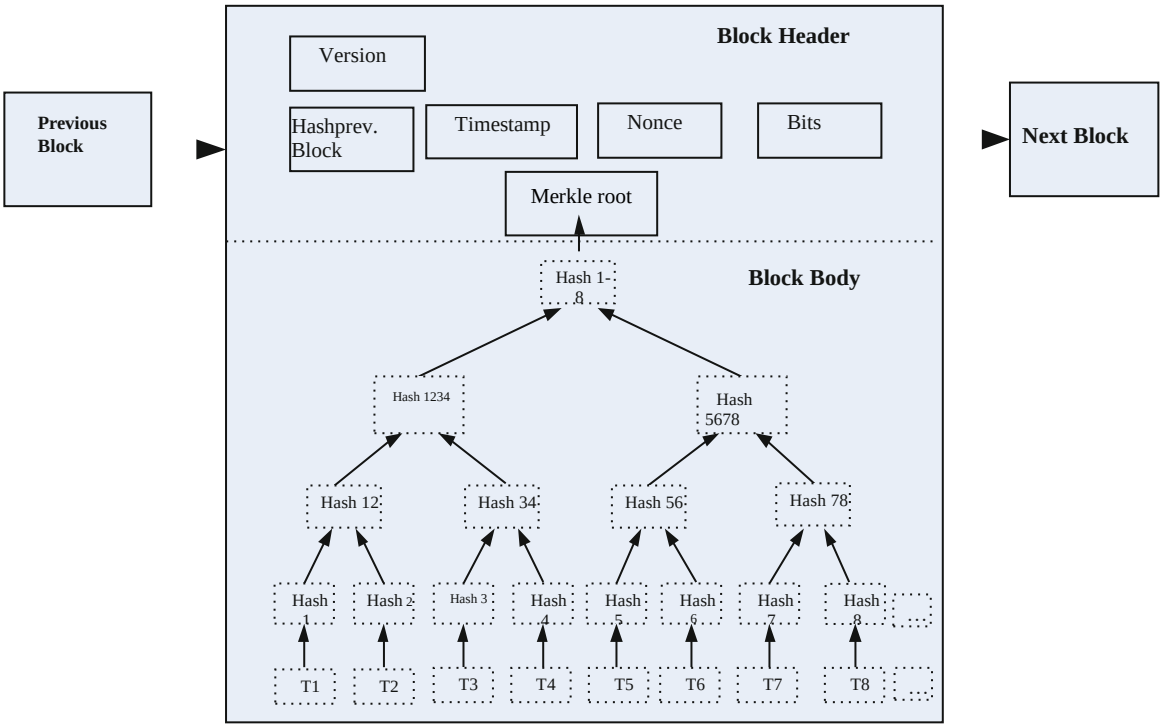
Avant de revenir, sur le dernier point du « block header » nous devons parler du corps du bloc. Comme expliqué plus haut, chaque transaction sera hachée et une empreinte numérique y sera associée. C'est ce qu'on appelle le hash. Ensuite, toutes les deux transactions, il va falloir fusionner leur hash afin de créer un nouveau hash. Ce processus va être effectué à chaque étage de l'arbre jusqu'au moment où il n'y aura plus qu'un seul et même hash qui s'appelle le merkle root. [11]

9 BIT2ME ACADEMY. Bit2me Academy [en ligne]. [consulté le 10 mars 2021] Disponible à l'adresse : https://academy.bit2me.com/fr/qu%27est-ce-que-le-nonce/

10 TABORA Vincent, 2019. A decomposition of the Bitcoin Block Header. Data Driven Investor. [en ligne] 21 novembre 2019 [consulté le 1er mars 2021]. Disponible à l'adresse : https://www.datadriveninvestor.com/2019/11/21/a-decomposition-of-the-bitcoin-block-header/

11 BAI Chong, 2019.*State-of-the-Art and Future Trends of Blockchain Based on DAG Structure.*[en ligne] In: Duan Z., Liu S., Tian C., Nagoya F. (eds) Structured Object-Oriented Formal Language and Method. SOFL+MSVL 2018. Lecture Notes in Computer Science, vol 11392. Springer, Cham.[consulté le 10 mars 2021] https://doi.org/10.1007/978-3-030-13651-2_11

Figure 1: Structure de la blockchain



Bai, 2019

Comme on peut le voir dans l'image ci-dessus, nous avons n transactions (T) qui seront hachées au premier niveau de l'arbre. Et ensuite ces transactions vont être fusionnées, pour former un nouveau hash au deuxième niveau, ainsi de suite jusqu'au merkle root. Ce merkle root est donc le dernier composant de l'entête du bloc.[12]

12 BAI Chong, 2019.*State-of-the-Art and Future Trends of Blockchain Based on DAG Structure.*[en ligne] In: Duan Z., Liu S., Tian C., Nagoya F. (eds) Structured Object-Oriented Formal Language and Method. SOFL+MSVL 2018. Lecture Notes in Computer Science, vol 11392. Springer, Cham.[consulté le 12 mars 2021] https://doi.org/10.1007/978-3-030-13651-2_11

2.2.2 Deuxième génération de blockchain

La première génération de blockchain était faite uniquement pour des crypto-monnaies. Aucune autre utilisation de la blockchain pouvait être faite jusqu'à la plateforme Ethereum qui a vu le jour en 2014, qui est le début de la 2ème génération de blockchain. Cette plateforme offre une possibilité de créer différentes applications décentralisées. Le point central de cette nouvelle blockchain sont les « smart contracts ».

Nous l'avons vu plus haut, les données qui sont stockées peuvent être des transactions de crypto-monnaies ou bien même d'autres données comme par exemple du code.

Sur Ethereum, nous sommes donc dans cette configuration. Il existe deux types de comptes, les comptes ordinaire et les comptes de contrat. Dans les comptes ordinaires, nous avons de l'ether. Les ethers sont des jetons digitaux qui sont utilisés pour faire des transactions avec Ethereum et également la crypto-monnaie d'Ethereum.

Les transactions en ether peuvent être faites à travers ces comptes. Dans le deuxième type de compte, il n'y pas seulement des ethers mais également des smart contracts où nous avons une adresse spécifique qui correspond à chaque compte. En revanche, le contrat intelligent pourra seulement être appelé par un contrat ordinaire, mais en aucun cas le compte « smart contract » peut être appelé par lui-même. Ces contrats intelligents permettent notamment aux développeurs de créer des applications décentralisées.

Tout comme dans la première génération, le protocole de consensus de la seconde génération est également la preuve du travail jusqu'à la version 2.0 de la plateforme. L'algorithme de la preuve du travail est appelé « Ethash » et est un peu différent de celle du Bitcoin. [13]

Afin de mieux illustrer la différence entre les différents types et d'expliciter de meilleure manière les différents types de transactions, nous allons voir à présent des exemples de transactions que j'ai fait dans le cadre d'un cours à la Haute Ecole de Gestion de Genève, sur Ethereum à travers Remix Solidity qui est une plateforme qui nous permet de développer les applications dans la blockchain d'Ethereum.

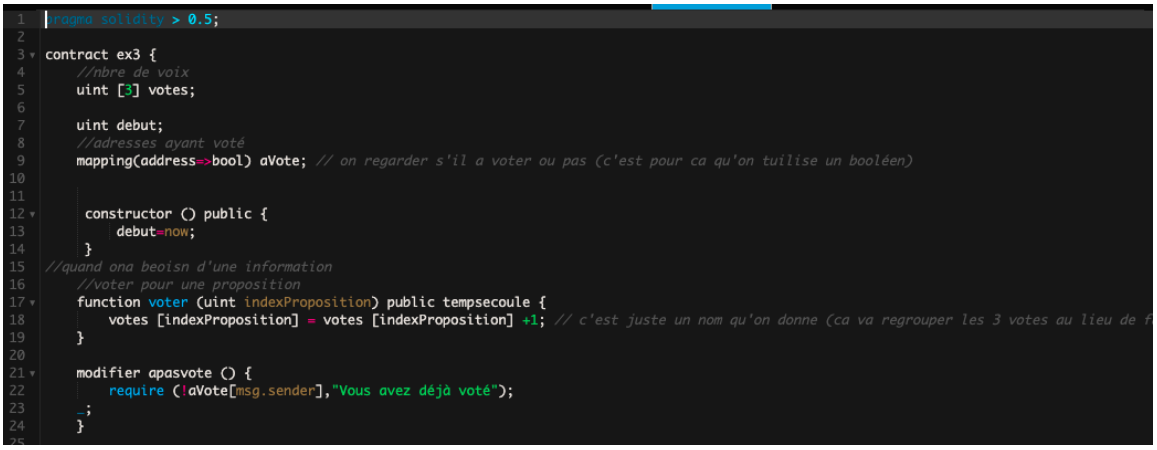
13 BAI Chong, 2019.*State-of-the-Art and Future Trends of Blockchain Based on DAG Structure.*[en ligne] In: Duan Z., Liu S., Tian C., Nagoya F. (eds) Structured Object-Oriented Formal Language and Method. SOFL+MSVL 2018. Lecture Notes in Computer Science, vol 11392. Springer, Cham.[consulté le 16 mars 2021] https://doi.org/10.1007/978-3-030-13651-2_11

Figure 2: exemple de transaction (votation)

```
pragma solidity >0.5;

contract ex4{

    address payable createur;
    uint debut;

    constructor () public payable {
       createur = msg.sender;
       debut=now;
    }

    modifier uniquement_proprio () {
        require (createur == msg.sender, "uniquement le proporietaire peut retirer");
        _;
    }
    modifier tempsecoule () { //c'est ce qu'on veut--> dans ce cas on veut donc qu'on retire après 5 minutes (30 secondes)
        require (now-debut>30, "Vous pouvvez retirer seulement 5 minutes après la création du contrat");
        _;
    }
    function verser (uint montant) public payable {
    }
    function retirer () public payable uniquement_proprio  tempsecoule {
        createur.transfer(address(this).balance);
    }
}
    modifier tempsecoule () {
        require (now-debut<30,"le vote est fini "); // require c'est ce qu'on veut
        _;
    }


    modifier tempsecoule2 () {
        require (now-debut>=30,"le vote n'est pas encore fini "); // require c'est ce qu'on veut
        _;
    }
    function voirlesvotes () public view returns (uint [3] memory){
    return (votes);
    }

    //pour connaitre la proposition gagnante
    function meilleurinitiative () public view tempsecoule2 returns (uint)  {
    //ne fonctionne que s'il y a gagnant
        if (votes [0]>votes [1] && votes [0]>votes [2]) return 0;
        if (votes [1]>votes [0] && votes [1]>votes [2]) return 1;
        if (votes [2]>votes [0] && votes [2]>votes [1] ) return 2;
    }

```

Comme expliqué plus haut, nous pouvons avoir des transactions en crypto-monnaie et les autres types de données. Dans le premier exemple nous sommes dans une configuration de votations. Dans cette situation, nous voulons autoriser certaines personnes de voter et de savoir quelle votation a reçu le plus de voix. Les informations qui sont enregistrées sont une matrice dans laquelle on associe un vote par adresse, l'horodatage et ensuite de savoir quelle votation a reçu le plus de votes.

Figure 3: exemple de transactions (versement d'ether)



```
pragma solidity > 0.5;

contract ex3 {
    //nbre de voix
    uint [3] votes;

    uint debut;
    //adresses ayant voté
    mapping(address=>bool) aVote; // on regarder s'il a voter ou pas (c'est pour ca qu'on tuilise un booléen)


     constructor () public {
         debut=now;
     }
//quand ona beoisn d'une information
    //voter pour une proposition
    function voter (uint indexProposition) public tempsecoule {
        votes [indexProposition] = votes [indexProposition] +1; // c'est juste un nom qu'on donne (ca va regrouper les 3 votes au lieu de f
    }

    modifier apasvote () {
        require (!aVote[msg.sender],"Vous avez déjà voté");
    _;
    }
```

Dans la deuxième image, nous sommes dans une configuration avec des crypto-monnaies. Nous voulons permettre aux personnes de pouvoir verser de l'argent et d'en retirer. Les principales informations stockées dans la blockchain sont donc le montant à verser, le montant à retirer et également les adresses des différents comptes dans lesquels l'argent va voyager.

Ethereum est un outil en open source, c'est-à-dire que tout le monde peut en avoir accès librement et sans coûts ajoutés afin de créer des contrats intelligent.

Avec Ethereum, chaque nœud a une machine virtuelle qui est appelé Ethereum Virtual Machine (EVM) dans laquelle le code va être exécuté, la validation des transactions va être faite et elle permet aussi de calculer les frais de transactions.[14]

14 CHANUT Guillaume,2019. Qu'est ce que la machine virtuelle Ethereum ?. *Cryptoast* [en ligne]. 25 avril 2019. 12 janvier 2020 [consulté le 20 mars 2021] : Disponible à l'adresse : https://cryptoast.fr/quest-ce-que-la-machine-virtuelle-ethereum/

Une des différences avec le Bitcoin, les utilisateurs devront payer des frais de transactions qui sont connus sous le nom de « gas ». Ils doivent donc payer un certain montant de gas afin de pouvoir exécuter leurs contrats ou bien leurs transactions. Le gas est définit comme suit :

$$Gas = \ prix\ du\ gas * limite\ de\ gas$$

Le prix du gas est le prix par unité et la limite du gas est la quantité de gas. Ce qui nous fait donc le total de gas. Les deux éléments de l'équation sont définis par les utilisateurs. A chaque fois qu'une transaction va être faites, il va falloir une certaine quantité de gas afin qu'elle soit exécutée. Si le montant de gas offert est supérieur au gas minimum requis afin d'exécuter la transaction, l'excès de gas sera renvoyé dans le compte du mineur. Dans le cas contraire où la quantité de gas offerte est inférieure à celle requise, la transaction sera annulée et le gas qui a été utilisé sera tout de même versé au mineur pour l'effort fourni, malgré le fait que la transaction n'a pas été exécutée. En revanche le montant de la transaction en ether sera rendu à l'utilisateur. Les mineurs vont valider les transactions dans lesquelles on leur offre le plus de gas. Afin que la transaction soit validée le plus rapidement possible, certains mineurs offrent une quantité de gas plus importante que ce qui est requis pour attirer les mineurs à valider leurs transactions. [15]

15 BAI Chong, 2019.*State-of-the-Art and Future Trends of Blockchain Based on DAG Structure.*[en ligne] In: Duan Z., Liu S., Tian C., Nagoya F. (eds) Structured Object-Oriented Formal Language and Method. SOFL+MSVL 2018. Lecture Notes in Computer Science, vol 11392. Springer, Cham.[consulté le 18 mars 2021] https://doi.org/10.1007/978-3-030-13651-2_11

2.3 Les transactions

Lorsqu'une transaction va être faite, il y a plusieurs étapes à devoir passer. A travers ces différentes étapes, il y aura différentes validations qui devront être faites par les utilisateurs. Dans le monde de la blockchain, ces utilisateurs sont appelés les « nœuds ». Les nœuds sont les différents ordinateurs qui sont dans le réseau. Il existe donc 3 catégories de nœuds :

- simple node (nœud simple)
- full node (nœud complet)
- miner node (nœud mineur)

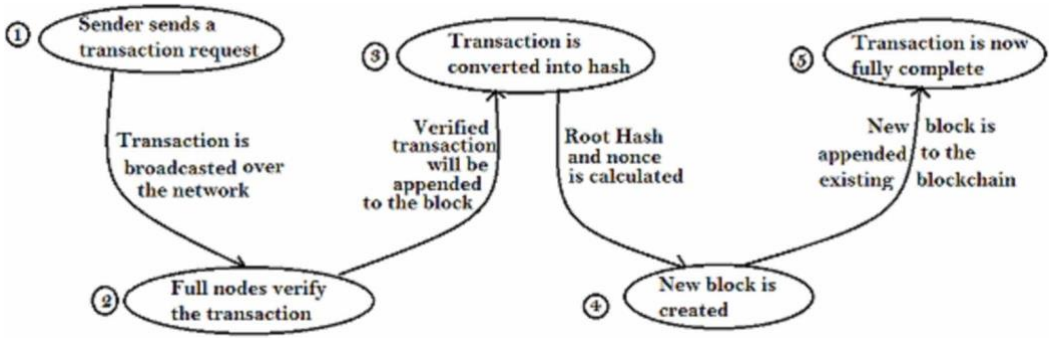
Le nœud simple est l'utilisateur qui a le moins de pouvoirs parmi ces nœuds. Il peut uniquement recevoir des transactions. Il ne peut ni stocker ni valider les transactions dans le réseau. En soit, il n'a seulement que des droits basiques dans la blockchain
Le nœud complet est important pour la sécurité de la blockchain, contrairement au nœud simple, il peut vérifier les transactions ainsi que les propager à travers le réseau. Il va également devoir identifier les transactions malveillantes et directement les arrêter afin qu'elles ne se propagent pas et qu'elles n'affectent pas tout le réseau. En revanche, il ne pourra pas miner le bloc, c'est-à-dire le valider.
Le 3ème utilisateur est celui qui a le plus de pouvoirs, et par conséquent le plus de responsabilités. Il se rapproche énormément du nœud complet mais comme son nom l'indique, il peut valider des blocs et en créer de nouveau.
Lorsqu'on parle de blockchain, on entend souvent parler de validation car pour qu'une transaction soit rajoutée dans le réseau décentralisé il faut que le nœud complet puisse valider la transaction et ensuite que le nœud mineur la rajoute dans le bloc. Pour se faire, il existe plusieurs manières de vérifier ces transactions. C'est ce qu'on appelle le protocole de consensus. Un des plus connus et le premier de ces protocoles est le Proof of Work (PoW) dit preuve de travail en français. 90% de la capitalisation de crypto-monnaies, utilise ce protocole. Lorsqu'on veut valider une transaction il faut trouver quelle est la valeur du nonce à travers une équation.[16]

16 SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 18 mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

Il existe plusieurs étapes pour valider une transaction. Tout d'abord l'émetteur de la transaction va devoir signer avec son empreinte numérique afin de pouvoir effectuer une demande de transaction. Cette demande sera ainsi transmise auprès des nœuds du réseau pair-à-pair. Une vérification sera faite afin de savoir si le donneur d'ordre a le droit d'effectuer cette action. Cette vérification sera faite par le nœud complet. Dès que la transaction aura été vérifiée elle sera rajoutée au bloc avec la transaction précédente. Suite à cela la transaction va être convertie en hash grâce à la fonction de hachage sha256. Puis comme expliqué plus haut, le root hash va être calculé ainsi que le nonce qui va permettre d'avoir le numéro d'authentification du block pour voir le bloc se créer. La dernière étape est que ce bloc soit rajouté dans la blockchain.

Seulement à partir de ce moment-là, nous pouvons définitivement affirmer que la transaction a été validée. Ces différentes étapes sont parfaitement illustrées auprès de la figure ci-dessous. [17]

Figure 4:Processus de transaction



SAPRA & DHALIWAL, 2021, PP.6

17 SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 18 mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

2.4 Catégorie de blockchain

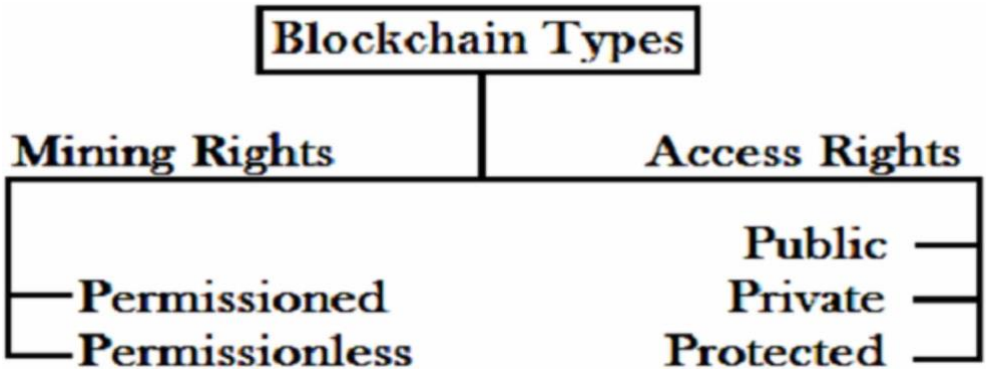
Il existe plusieurs catégories de blockchain que nous pouvons distinguer. Il y a celles qui sont catégorisées par les droits de minage et celles qui le sont par les droits d'accès. Dans la première catégorie, nous avons les « permissioned » blockchain et les « persmissionless » blockchain. Depuis le début de ce travail, nous avons parlé de la « permissionless » blockchain où il y a une pleine décentralisation. Dans ce type de blockchain, aucun utilisateur n'a plus de pouvoirs que d'autres utilisateurs. Cette blockchain permet une grande sécurité des données car il faudrait attaquer plusieurs points de la blockchain afin d'être efficace dans cette attaque. Ainsi que le faite qu'il n'y ait pas besoin d'une tierce personne dans la validation des données. Tout le monde peut lire et écrire dans la blockchain. Contrairement à la « permissionless » blockchain, la « permissioned » blockchain ne permet qu'a quelques personnes de valider les blocs, de les lire et de les écrire. Elle est notamment utilisée lorsqu'il y a des partenariats entre plusieurs organisations qui doivent donc transcrire et lire ces transactions. Seul ces organisations-là pourront lire et écrire dans la blockchain.

L'autre type de catégorie est en fonction de l'autorisation ou non de lire et écrire dans la chaine de blocs. Mais aucunement sur les droits de vérification, contrairement à la première catégorie. Nous avons donc la blockchain publique qui se rapproche de la blockchain « permissionless ». Dans cette blockchain, tout le monde peut vérifier les transactions. De ce fait c'est la blockchain préférée des crypto-monnaies mais également celle la plus répandue. La seconde blockchain est la blockchain de consensus. Elle n'est pas totalement décentralisée, puisqu'elle n'autorise pas à n'importe qui de participer dans le processus de vérification des transactions. Mais elle est plus rapide que la blockchain publique. Ensuite la blockchain privée, elle autorise l'écriture qu'à une seule personne ou bien à une seule organisation et la lecture des transactions est seulement autorisée à certaines personnes. Avec cette dernière, on perd en décentralisation étant donné que seul un nombre limité de personnes peut écrire dedans. Elle reste tout de même la blockchain préférée des banques car elle leur permet d'avoir une certaine maitrise des opérations. [18]

[18] CASH,Michael & BASSIOUNI Mostafa, 2018. *Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing*. [en ligne]. 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018, pp. 138-144, doi:10.1109/SmartCloud.2018.00031.[consutlé le 18 mars 2021]. Disponible à l'adresse : https://ieeexplore.ieee.org/abstract/document/8513729

De plus, la confiance dans cette blockchain est moins présente, par rapport à une blockchain public où on a intérêt à faire confiance à une grande partie du réseau car ils ont accès à tout (écriture et lecture). [19]

Figure 5: Types de blockchain



SAPRA & DHALIWAL, 2021, PP. 8

19 SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 1er mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

2.5 Caractéristiques

La blockchain plaît beaucoup, notamment grâce à ces différentes caractéristiques tel que :

- Sécurité
- Décentralisation
- Immuabilité
- Transparence
- Anonymat
- Absence d'intermédiaire

L'un des principes les plus connus sur la blockchain c'est bien évidement sa sécurité grâce notamment à la fonction de hachage. Toutes données modifiées dans un bloc pourront tout de suite être aperçue. Ce qui en fait en théorie une technologie très sure en termes de sécurité des données. En effet, lorsque l'on va modifier une donnée, son hash va lui aussi automatiquement changer, mais également son merkle root. Étant donné que le root hash est rattaché au root hash du bloc suivant, ce changement dans le bloc n-1 va automatiquement changer le root du bloc n, ainsi que du bloc n+1 jusque fin s'en suive.

Une autre caractéristique importante qui rejoint également la sécurité des données, est la décentralisation. Chaque membre du réseau aura accès à la blockchain car c'est public, même si nous avons vu que c'est un plus complexe que cela. De ce fait si une attaque va être tentée par un individu, il devra le faire pour tous les membres du réseau car tous les membres du réseau ont une copie de la blockchain. Si ce même individu tente de manipuler les informations, toutes les personnes le verront et ne valideront pas cette modification. Si on compare cela à un système centralisé, comme une banque, on peut s'apercevoir qu'il suffit de s'attaquer à la banque afin de pouvoir atteindre tous les membres de réseau (clients) car ils n'ont aucune copie, contrairement au système blockchain.

L'immuabilité de la blockchain est également très importante car cela consiste à ce que chaque donnée stockée dans la blockchain ne puisse pas être modifiée. S'il y a réellement le besoin de modifier une information dans le bloc pour quelconque raison, une nouvelle transaction sera créée. [20]

[20] SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 3 mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

Les informations stockées au sein de la blockchain, sont visibles par chaque membre du réseau. On ne peut rien caché à un autre membre. Ce qui fait de la blockchain une technologie transparente.

L'identité de chaque utilisateur est inconnue. En effet, dans une blockchain l'identité de chaque utilisateur est associée à une adresse en utilisant une fonction cryptographique. Une des raisons pour laquelle les crypto-monnaies sont énormément appréciée par les criminelles, c'est qu'on ne sait pas qui est le donneur d'ordre et qui est le receveur de cet ordre. Contrairement au système bancaire où l'on connaît votre nom, votre adresse, votre âge, votre numéro de téléphone. La traçabilité est bien plus efficace avec ce système-là.

Et pour finir la blockchain ne fait pas appel aux intermédiaires car la validation est faite directement par les membres du réseau contrairement au système bancaire qui lui s'occupe de valider les transactions. Lorsque l'on effectue un versement, la banque va contrôler qu'il y ait assez d'argent dans le compte à débiter en vérifiant également que le compte du bénéficiaire existe réellement. Ce travail d'intermédiaire qui est tout de même coûteux, sera effectué directement par les membres du réseau.[21]

2.6 Les problèmes de la blockchain

On a pu voir que la blockchain est une technologie qui offre beaucoup de solutions extrêmement intéressantes du point de vue de la décentralisation, sécurité, stockage des données. Malgré tous les aspects positifs de cette technologie, beaucoup de question et de doutes se propagent sur cette technologie comme par exemple l'aspect environnemental du fait de la haute consommation en énergie dans la preuve du travail. En effet, nous avons vu plus haut le fonctionnement de ce protocole. Ce dernier nécessite une grande puissance de calcul. Cela prend énormément d'énergie en termes d'électricité. Le bitcoin qui utilise le consensus de la preuve du travail, consomme 15,77 térawatts par heures. Ce qui correspond à 0,08% de la consommation mondiale d'électricité. Un certain investissement en termes de matériel est nécessaire, afin de résoudre l'équation. Il y a besoin d'investir dans des ordinateurs avec de grandes capacité

21 SAPRA, Riya, & DHALIWAL, Parneeta, 2021. *Blockchain: The Perspective Future of Technology.*[en ligne].International Journal of Healthcare Information, Systems and Informatics (IJHISI), 16(2), 1-20.[consulté le 3 mars 2021]. Disponible à l'adresse : http://doi.org/10.4018/IJHISI.20210401.oa1

mais également les mettre dans un environnement assez froid afin que la machine ne se refroidisse pas.[22]

Il existe même ce qu'on appelle des fermes de minage qui sont des entrepôts (comme dans l'image ci-dessous) dans lesquels il y a plusieurs rangées où sont stockés plusieurs ordinateurs qui vont travailler afin de résoudre l'équation dans le cadre de la preuve de travail. [23]

Figure 6: Ferme de minage

Malnov, 2017[24]

Ensuite, nous avons également des interrogations sur la durabilité de ce protocole puisqu'à cause de la popularité de ce système, une forte augmentation du nombre mineurs arrive. Afin de prévenir cette concurrence, les mineurs vont former des pools de minage afin d'augmenter leurs possibilités de gain. De plus, chaque bloc miné correspond à 12,5 nouveau bitcoins pour les mineurs. Le problème est que le nombre de bitcoins est déterminé. En effet, le nombre de bitcoins créé ne dépassera pas les 21 millions, et le dernier bitcoin sera créé en 2021. Tous les 2 ans le montant de chaque bloc miné diminue de moitié. Afin que le système continue, le bitcoin a un réel besoin que les mineurs

22 SZALACHOVSKI Pawel, REIJSBERGEN Daniël, HOMOLIAK Ivan, 2019. *StrongChain : Transparent and Collaborative Proof-of-work Consensus* [en ligne] 28th Security Symposium. [consulté le 25 mars 2021]. Disponible à l'adresse : https://www.usenix.org/system/files/sec19-szalachowski.pdf

23 NAUDIN Julie, 2019. Le jour où je suis entrée dans les coulisses du métier de mineur de crypto. Finance Mag. [en ligne] 16 janvier 2019 [consulté le 25 mars 2021]. Disponible à l'adresse : https://finance-mag.com/minage-cryptomonnaies-metier-julie-naudin/

24 MALANOV Alexey, 2017. Explication : Minage des bitcoins, *kaspersky daily*. [en ligne]. 25 avril 2017. [consulté le 25 mars 2021]. Disponible à l'adresse : https://www.kaspersky.fr/blog/mining-easy-explanation/9305/

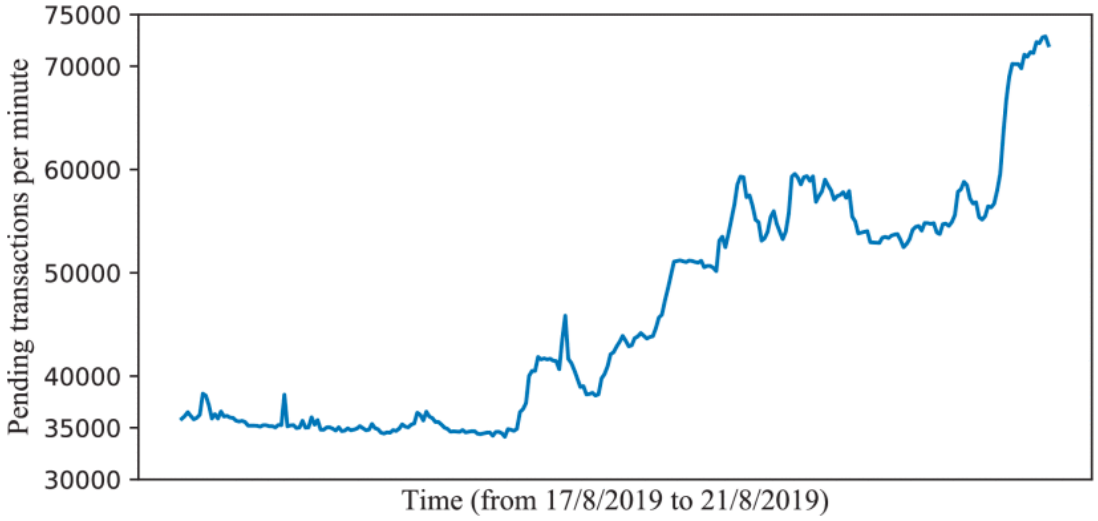
effectuent ce travail. Le problème étant que plus le temps passe et moins ce travail est rentable en termes de récompense pour les mineurs, pour les diverses raisons expliquées plus haut. Quel sera donc l'intérêt des mineurs d'ici quelques années ?[25]

Également la scalabilité pose problème car afin de valider les transactions dans un bloc, il faudra miner ce bloc. Ainsi, dans le but que le bloc soit validé et qu'il soit propagé auprès de tous les pairs du réseau, il faut qu'un intervalle soit mise en place entre la validation de deux blocs. Plus il y aura de transactions, plus cela demandera du temps pour les valider. En effet, il se peut qu'à certains moments il y ait tellement de transactions en attente que la validation de certaines transactions reste en attente. En effet, les mineurs vont choisir les transactions qu'ils voudront valider, en fonction de la récompense, car pas toutes les transactions sont rémunérées de la même manière. Tout naturellement, ils valideront les transactions les plus rentables. Il faut aussi savoir que la taille du bloc est limitée s'il y a vraiment une grande latence, certaines transactions seront à peine regardées. Certaines fois il peut y avoir énormément de transaction en suspens comme on peut le voir avec Ethereum qui utilisait la preuve du travail jusqu'à la version 2.0 de la plateforme. [26]

25 SZALACHOVSKI Pawel, REIJSBERGEN Daniël, HOMOLIAK Ivan, 2019. *StrongChain : Transparent and Collaborative Proof-of-work Consensus* [en ligne] 28th Security Symposium. [consulté le 25 mars 2021]. Disponible à l'adresse : https://www.usenix.org/system/files/sec19-szalachowski.pdf

26 ZHOU Qiheng, HUANG Huawei, ZHENG Zibin, BIAN Jing, 2020. *Solutions to Scalability of Blockchain: A Survey* [en ligne]. in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.[consulté le 25 mars 2021]. Disponible à l'adresse :https://ieeexplore.ieee.org/abstract/document/8962150

Figure 7:Transactions en attente sur Ethereum



ZHOU & HUANG & ZHENG & BIAN, 2020, PP.16442

Comme on peut le voir sur ce graphique, le nombre de transactions en attente par minutes est passé 35000 à presque 75000 sur une période de 5 jours. Pour certaines transactions, ce n'est pas extrêmement gênant qu'elle se retrouve en attente, mais il y en a certaines dont c'est le cas, comme par exemple les transactions en crypto-monnaies. Étant donné la volatilité de ces monnaies, lorsqu'un ordre est placé il est nécessaire qu'il soit exécuté au montant voulu par le donneur d'ordre puisqu'en 5 jours, le prix peut baisser de 40% par exemple entre le moment où l'on lance l'ordre et le moment où l'ordre va être validé.[27]

Depuis que cette technologie est apparue et s'est médiatisée, on a toujours venté, et dans ce travail également, sa sécurité. Le fait que la blockchain est une technologie qui est sûre en tant que sauvegarde des données et également contre des attaques malveillantes. Pour conclure cette partie sur la blockchain, nous allons voir une attaque importante qui est apparue dans la plateforme Ethereum, qu'il est important de prendre en compte.

The DAO est le nom d'une organisation automatique décentralisées (DAO). Il s'agit d'une organisation qui est régie par un smart contract, donc uniquement par du code. Cette

27 ZHOU Qiheng, HUANG Huawei, ZHENG Zibin, BIAN Jing, 2020. *Solutions to Scalability of Blockchain: A Survey* [en ligne]. in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.[consulté le 25 mars 2021]. Disponible à l'adresse :https://ieeexplore.ieee.org/abstract/document/8962150

organisation n'est dirigée par aucune entité centrale.[28] Elle est distribuée auprès des membres qui ont investi des jetons dans cette organisation et qui ont donc un pouvoir de décision. Nous avons donc des développeurs qui vont écrire le code afin de créer la société. Cette organisation devra tout de même être financée. Pour se faire les personnes qui sont intéressées par cette organisation et qui veulent faire partie cette dernière, ils vont payer afin d'avoir des « tokens » qui leurs procurent des droits de vote.[29]

La DAO la plus connue est appelée « the DAO », cette DAO va investir dans des projets d'applications décentralisé. Les droits de vote que les investisseurs vont acquérir seront donc pour décider dans quelles applications décentralisées ils veulent que l'organisation investisse. Ils ont réussi à se faire financer à hauteur de 150 millions d'ether. En effet, étant donné que cela se passe sur Ethereum, l'investissement est fait en ether. A l'époque, cela représentait 14% des ethers en circulation.

Lorsqu'une personne a voté contre la majorité pour l'investissement auprès d'une application décentralisée, le smart contract, permettait de retirer les parts que cette personne avait investies, dans le but de ne pas investir dans un projet pour lequel elle ne croyait pas. Cette partie de code était vulnérable, et une personne a utilisé cette vulnérabilité contre l'organisation. En effet, elle a utilisé la fonction de retrait de son investissement plusieurs fois. La faille dans le code est que malgré la faite qu'elle ait déjà retiré une fois le montant de son investissement, il était tout de même possible de continuer à retirer et donc de prendre l'investissement des autres membres. C'est donc ce qu'elle a fait, jusqu'à atteindre 50 millions de dollars d'ether. [30]

---

28 INVESTEREST, 2016. Ether explained – Chapter 4 : The Decentralized Autonomous Organization (DAO). *INVESTEREST*. [en ligne]. 29 juillet 2019. [consulté le 27 juin 2021] Disponible à l'adresse : https://investerest.vontobel.com/en-dk/articles/13374/ether-explained--chapter-4-the-decentralized-autonomous-organisaion-dao/

29 SIEGEL David, 2020. Understanding the DAO attack. *Coindesk*. [en ligne]. 25 juin 2016. 17 décembre 2020. [consulté le 27 juin 2021]. Disponible à l'adresse : https://www.coindesk.com/understanding-dao-hack-journalists

30 INVESTEREST, 2016. Ether explained – Chapter 4 : The Decentralized Autonomous Organization (DAO). I*NVESTEREST*. [en ligne]. 29 juillet 2019. [consulté le 27 juin 2021] Disponible à l'adresse : https://investerest.vontobel.com/en-dk/articles/13374/ether-explained--chapter-4-the-decentralized-autonomous-organisaion-dao/

3. L'assurance et les insurtech

L'arrivée des assurances se fait au moyen-âge, les assurances étaient à cette époque publiques et s'appliquaient notamment lors d'accidents naturelles tel que des incendies. Mais la première assurance privée en Suisse a été la Mobilière. [31] En suisse, on peut distinguer les assurances obligatoires et les assurances facultatives.

Tableau 3: Assurances obligatoires et facultatives

Assurances	
Obligatoires	Facultatives
Assurances maladies	Assurance véhicule
AVS-AI-APG-AC	Assurance maldie complémentaire
Assurances accident	Assurance bâtiment
Assurance auto	Assurances responsabilité civile privée
	Assurance inventaire ménage
	Assurance protection juridique

○ **32**

31 SWISSRE, 2017. *Histoire de l'assurance suisse*. Compagnie suisse de réassurance SA. [en ligne][Consulté le 28 avril 2021] Disponible à l'adresse : https://www.swissre.com/dam/jcr:c4313ff1-60fc-43af-b33e-a0dbd8819189/150Y_Markt_Broschuere_Schweiz_FR_Inhalt.pdf

32 Allianz. Quels sont les assurances obligatoires en Suisse ?. *Allianz*.[en ligne] [consulté le 28 avril 2021]. Disponible à l'adresse : https://www.allianz.ch/fr/clients-prives/guide/vie-quotidienne/assurances-obligatoires-suisse.html

3.1 Assurances en suisse

3.1.1 Assurance obligatoire

Dans les assurances obligatoires, nous avons donc l'assurance maladie qui est extrêmement importante en suisse. Cette assurance permet aux assurés, de se faire rembourser certains soins et certains médicaments en cas de maladie. L'assurance accident agit comme son nom l'indique lors d'accidents. Lorsqu'on travaille plus de 8 heures par semaine, on cotise pour l'assurance accident automatiquement. Concernant l'assurance auto, même si elle est obligatoire uniquement pour les détenteurs d'automobiles, on peut tout de même la considérer dans cette catégorie, étant donné qu'énormément de personnes détiennent un ou plusieurs véhicules de ce type. [33]

3.1.2 Assurances facultatives

En termes d'assurances facultatives, la liste est longue car il existe un nombre important d'assurance comme par exemple des assurances complémentaires avec l'assurance maladie et l'assurance auto qui offre aux contracteurs d'assurances des prestations supplémentaires, mais de ce faite, elles sont supérieurs à l'assurance de base en termes monétaires qui n'assure que le minimum. Nous avons également l'assurance bâtiment qui est obligatoire pour toutes personnes qui détiennent un bâtiment.[34]

33 Allianz. Quels sont les assurances obligatoires en Suisse ?. *Allianz*.[en ligne] [consulté le 28 avril 2021]. Disponible à l'adresse : https://www.allianz.ch/fr/clients-prives/guide/vie-quotidienne/assurances-obligatoires-suisse.html

34 Allianz. Quels sont les assurances obligatoires en Suisse ?. *Allianz*.[en ligne] [consulté le 28 avril 2021]. Disponible à l'adresse : https://www.allianz.ch/fr/clients-prives/guide/vie-quotidienne/assurances-obligatoires-suisse.html

3.1.3 L'assurance en chiffres

Dans cette partie, nous mettrons en évidence les résultats financiers du marché de l'assurance suisse. Le marché de l'assurance est un secteur extrêmement important dans le PIB suisse et a donc un poids important. Tous les chiffres cités ci-dessous sont extraits du rapport sur le marché des assurances en 2019 par la FINMA.[35] Le nombre total d'assurances étudiées dans le rapport de la FINMA sont de 198, comprenant :

- 118 assureurs de dommages
- 50 réassureurs
- 19 assurances vies
- 11 assureurs vies

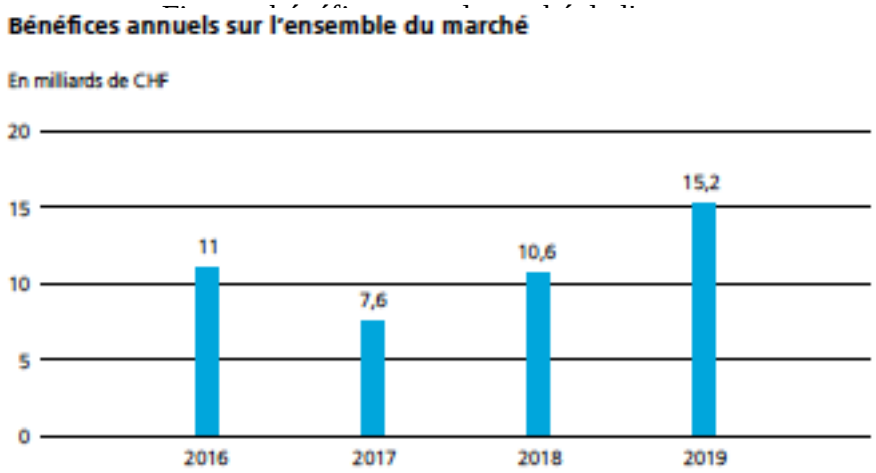
La majorité des recettes de ces entreprises proviennent bien entendu des primes payées par leur clients chaque mois contre une prestation en fonction de leur contrat d'assurance. En 2019, les recettes des primes ont augmentés de 13%, elles sont passées de CHF 114'023'955'000.– à CHF 129'167'737'000.– en 2019. Ayant une répercussion importante sur le bénéfice du marché qui est passé de CHF 10'575'877.– à CHF 15'219'352. – soit une variation de +43,9%.[36]

35 FINMA 2019. Rapport 2019 sur le marché de l'assurance. *Autorité fédérale de surveillance des marchés financiers FINMA*.[en ligne] [consulté le 1 mai 2021]. Disponible à l'adresse :https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/versicherungsbericht/20200910-versicherungsmarktbericht-2019.pdf?la=fr

36 FINMA 2019. Rapport 2019 sur le marché de l'assurance. Autorité fédérale de surveillance des marchés financiers FINMA.[en ligne] [consulté le 1 mai 2021]. Disponible à l'adresse :https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/versicherungsbericht/20200910-versicherungsmarktbericht-2019.pdf?la=fr

On peut également s'apercevoir que cette progression ne s'étend pas seulement entre 2019 et 2018 mais c'est bien une progression constante du marché de l'assurance de ces dernières années. [37]

Figure 8:Bénéfices annuels marché de l'assurance



FINMA, 2019, PP.6

3.2 Fintech

Maintenant que nous avons vu brièvement ce qu'est l'assurance en suisse mais également les types d'assurances. Nous allons voir ce que sont ces nouvelles assurances qui grandissent de plus en plus dans le marché depuis quelques années. Il faut savoir que l'insurtech est un des éléments qui fait partie de la notion « fintech ». Thomas Puschmann , nous donne cette définition de la Fintech : « *The term "fintech" is a contraction of "financial technology"* ».[38]*(PUSCHMANN, 2017, pp.70)* Toujours d'après le même auteur, cette notion a été introduite dans les années 90 par le président de Citycorp (nouvellement Citigroup) de l'époque John Reed dans le cadre d'un consortium entre des entreprises et des industries.

37 FINMA 2019. Rapport 2019 sur le marché de l'assurance. *Autorité fédérale de surveillance des marchés financiers FINMA*.[en ligne] [consulté le 1 mai 2021]. Disponible à l'adresse :https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/versicherungsbericht/20200910-versicherungsmarktbericht-2019.pdf?la=fr

38 PUSCHMANN Thomas, 2017. *Fintech*. Business Information System Engineering 59, 69–76 [en ligne] [consulté le 1 mai 2021] Disponible à l'adresse : https://link.springer.com/content/pdf/10.1007/s12599-017-0464-6.pdf

La finance peut être fortement impactée par la technologie puisque dans ce domaine on traite principalement des données. En effet, si on prend quelques exemples de produits financiers, nous avons les transactions de titres, les contrats de crédits ou bien les opérations de paiement. On remarque que nous n'avons presque pas d'éléments physique parmi ces produits financiers. Tout ce qui est traité sera de l'ordre de données. C'est donc la raison pour laquelle le mariage entre finance et technologie peut aboutir, en théorie. En fintech, on peut distinguer les innovations financières en 4 différentes catégories :

- Produits et services
- Structures organisationnelles
- Les processus
- Les systèmes

Pour la première catégorie, nous trouvons majoritairement des services plutôt que des produits. Lorsqu'on parle de structures organisationnelles, on parle notamment d'externalisation de certaines tâches ou bien de certains processus. Le 3ème point pourrait être défini comme rattachée de près à l'activité financière, c'est toutes les innovations qui peuvent être faites à travers les différents processus qui vont se rattacher à des activités bien précises. Le dernier point se sont les systèmes qui vont être innover mais dans ce cas on va plus parler de technologie. L'exemple le plus parlant est celui de la blockchain dont nous en avons parlé grandement. C'est pour cela qu'on peut également distinguer deux différentes catégories parmi celles ci-dessus. Nous avons donc les trois premières catégories qui sont associées à la finance et la dernière qui est associée aux technologies. Ce qui est cohérent et qui rejoint la définition de la fintech.[39]

En termes de fintech, on peut les distinguer en 4 catégories :

- Banques
- Assurances
- non-banques
- non-assurances

Les solutions de fintech sont souvent proposées par des starts up comme Revolut ou bien N26. Mais les banques ont bien compris qu'il fallait, qu'elles aussi saisissent l'opportunité

39 PUSCHMANN Thomas, 2017. *Fintech*. Business Information System Engineering 59, 69–76 [en ligne] [consulté le 1 mai 2021] Disponible à l'adresse : https://link.springer.com/content/pdf/10.1007/s12599-017-0464-6.pdf

grandissante de la fintech. C'est pourquoi, elles aussi proposent des solutions fintech comme par exemple « secure sign » de crédit-suisse ou bien même Twint qui est fortement présent dans le quotidien de nombreuses personnes et qui leurs facilitent la vie.

Bien que les banques aient été les premières à saisir cette opportunité, les assurances ne sont pas restées passives très longtemps. La fintech permet de couvrir différents processus du milieu de l'assurance tels que l'assurance-vie et non-vie, le conseil aux clients ou bien même la gestion des sinistres. Dans le cas de la gestion des sinistres, la fintech permet par exemple d'analyser le dégât d'un accident à l'aide d'un drone au lieu d'envoyer un être humain.

Comme il a été énoncé plus haut, les non- banques participent pleinement à l'émancipation de la fintech. Les non-banques permettent de faire à moins des banques en tant qu'intermédiaire. Les non-banques sont constitués de start up ou bien même de multinationales qui désirent conquérir un nouveaux marchés tel qu'Apple par exemple avec leur « Apple pay ». La plupart des solutions fintech qui sont disponible sur le marché sont fournies par les non-banques qui peuvent être rachetées par les banques. En effet, toutes ces solutions fintech demandent du temps, des connaissances et de l'argent. Les banques n'ont pas toutes ces denrées à leurs dispositions. c'est pourquoi au lieu de mettre en place leurs propres solutions, elles achètent des start up qui ont développé ces produits. On peut citer Goldman Sachs qui a racheté la star up indienne ZestMonney, ce qui leur permet de s'accaparer de nouveaux clients ainsi que d'avoir des revenus sur une activité qu'ils ne produisaient pas.

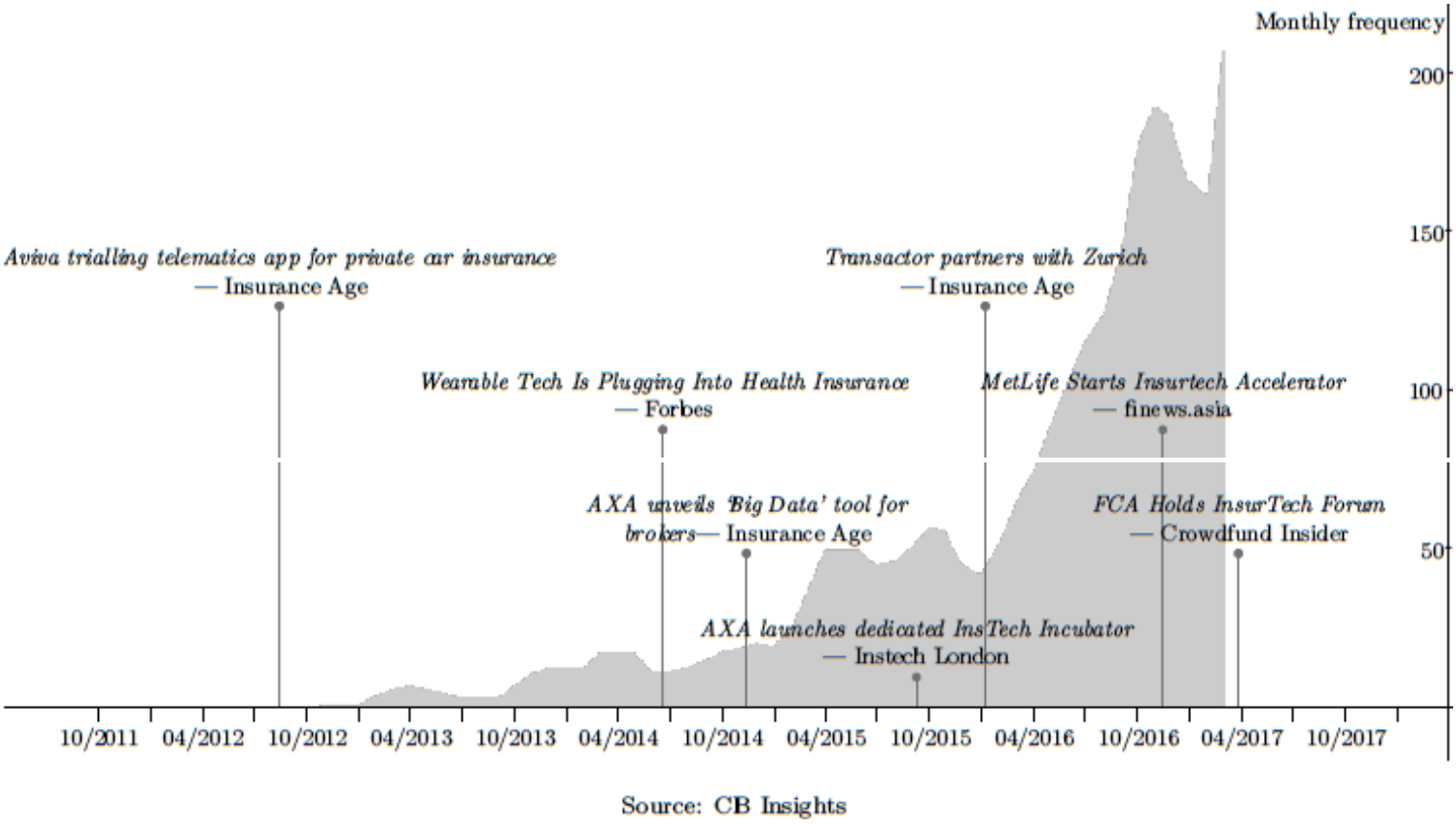
Tout comme les banques, les assurances ne produisent pas les solutions fintech. Pour la plupart ce sont des starts up. Ces starts up offrent différentes solutions pour leurs clients. Tout comme la banque beaucoup de ces nouveaux modèles vont permettre de faire à moins de l'assurance en tant qu'intermédiaire. Un des modèles que nous pouvons citer est l'assurance pair-à-pair, dont nous parlerons en détails plus loin. [40]

[40] PUSCHMANN Thomas, 2017. *Fintech*. Business Information System Engineering 59, 69–76 [en ligne] [consulté le 1 mai 2021] Disponible à l'adresse : https://link.springer.com/content/pdf/10.1007/s12599-017-0464-6.pdf

3.2.1 Insurtech

Le terme insurtech a commencé à apparaître en 2012 mais n'a commencé à se répandre dans les médias qu'en 2015. Depuis, il ne fait que prendre de plus en plus d'ampleur. En effet, on peut s'apercevoir qu'une des premières apparitions de l'insurtech dans un média a été faite en août 2012, sans avoir eu un impact immédiat. Cela a commencé gentiment à grandir à la fin 2014, suite à l'apparition de l'insurtech dans différents médias dont notamment, dans le célébrissime magazine Forbes. Avant d'atteindre son apogée médiatique en 2016 selon ce graphique.[41]En vue de l'avènement des insurtechs, comme nous l'avons expliqué avec les banques, elles investissent dans ces starts up afin de saisir cette opportunité de marché.

Figure 9: Apparition des fintechs dans les médias



BRAUN & SCHREIBER,2017,PP.18

41 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 5 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

Figure 10: Investissement des assurances dans des starts up

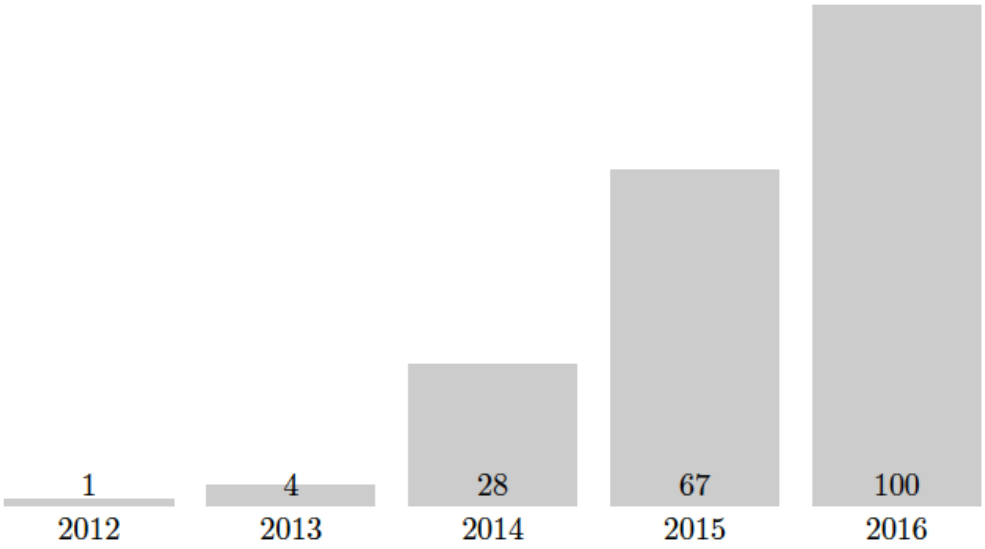
Source: CB Insights (2017a)

Alexander BRAUN & SCHREIBER, 2017, PP.30

Ce tableau nous montre une liste non-exhaustive de l'investissement des assurances traditionnelles auprès des différentes starts up. On voit à quel point les assurances ont logiquement compris l'opportunité que cela pourrait représenter pour elles. Mais à la place de le développer en interne, qui demanderait un certain nombre de ressources que ce soit en temps, en argents, et en connaissances techniques.

Elles investissent auprès des starts up qui se concentrent uniquement sur cette activité et qui maîtrisent parfaitement leur sujet. Ces investissements auprès de ces startups, ne font qu'augmenter depuis qu'elles ont débutés et ces chiffres ne vont faire qu'augmenter face à l'augmentation de ces starts up.

Figure 11: Nombre d'investissement dans des starts up



Source: CB Insights (2017c)

Alexander BRAUN & SCHREIBER, 2017, PP.18

Ce graphique nous montre à quel point ces startups sont prises en considération par ces assurances. Entre 2012 et 2016 le nombre de ces investissements a augmenté de 10'000%.

En plus de ces investissements, les assurances ont su profiter de la venue de ces incubateurs qui aident les startups à se développer dans leurs projets, en leur fournissant une structure, de l'aide des conseils, ainsi que des ressources financières. De ce fait, certaines assurances créent leurs propres incubateurs pour ces starts up voire même de conduire un partenariat avec ces dernières. Par exemple, Munich Re offre un service de réassurance à la startup « Lemonade ». Cette stratégie de la part de ces assurances traditionnelles montre bien l'inquiétude qui a commencé à naître après la venue de ces starts up sur le marché.[42]

42 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 6 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

3.2.1.1 Les types d'insurtech

Comme nous avons pu le voir en introduction, il existe une multitude d'insurtech. Nous allons à présent les voir afin de connaître leurs spécificités.

Les sites de comparaison :

Ce sont des sites dans lesquels il est possible de comparer les différentes assurances sur le marché afin de pouvoir choisir la meilleure par rapport à sa situation. Si on prend l'exemple de l'assurance maladie, une personne jeune, en bonne santé qui n'a pas d'antécédents médicaux spécifiques, n'aura pas besoin que l'assurance lui offre les mêmes prestations qu'une personne âgée. Elle ira potentiellement moins chez le médecin et du coup n'aura pas besoin de payer une prime qui comprend de multiples prestations. Cette personne n'aura besoin que des services de base. Ces sites de comparaison peuvent être utilisés pour de nombreuses assurances, tel que : [43]

- Assurance maladie
- Assurance automobile
- Assurance voyage
- Assurance pour les entreprises

En suisse, un des sites de comparaison qui existe est « comparis », qui permet de comparer différentes assurances. Ce site offre aussi des prestations pour les véhicules en termes de leasing, de marché, afin de trouver son véhicule, mais également aussi en immobilier notamment pour un crédit hypothécaire. Ce site permet de comparer l'assurance automobile, l'assurance ménage, l'assurance juridique, l'assurance maladie, l'assurance voyage. Cela permet de faciliter la vie des consommateurs pour trouver la meilleure assurance en fonction de leur profil.[44]

43 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 6 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

44 COMPARIS. *Comparis*. [en ligne]. [Consulté le 27 juin 2021 d]. Disponible à l'adresse : https://fr.comparis.ch/.

Les courtiers numériques :

A travers des plateformes ou bien des applications mobiles, les courtiers numériques sont des intermédiaires entre l'assurance et le client. A travers l'application, les clients reçoivent toutes les informations relatives à l'assurance. Le client peut entrer en contact avec leur courtier afin de recevoir différents conseils de la part de ce dernier. Bien entendu, cela se fait à travers la plateforme numérique du courtier. Etant donné que ce service est entièrement gratuit pour le client, ces courtiers numériques ont des revenus grâce à des commissions qui vont être versées par les assurances traditionnelles.[45]

Les assurances « cross seller »:

Ce genre d'assurances permet d'assurer un produit dès qu'il a été acheté en ligne. Grâce à l'application, les clients peuvent gérer toutes les différentes polices pour leurs produits. Tout comme les courtiers numériques, les clients peuvent prendre contact avec leurs courtiers à travers l'application, pour toutes questions ou conseils. Une des starts up les plus connues pour ce type d'assurance est « simplesurance ».[46]

Les assurances pair-à-pair :

L'assurance pair à pair fonctionne comme l'assurance mutuelle, c'est-à-dire que ce sont les personnes qui font parties du réseau qui vont indemniser la personne lésée par un accident. A la fin d'une période (annuellement par exemple) , s'il reste de l'argent au sein du « pool » créé, il sera soit rendu aux différents membre ou bien il sera déduit sur la prime de l'année suivante[47]. Mais chaque assurance détermine ces modalités de paiement. Par exemple « Friendsurance » Une partie des primes des membres sera versée auprès d'un pool de remboursement et l'autre partie sera versée auprès d'une assurance traditionnelle. Une prime de remboursement sera versée à hauteur de 40% maximum de la prime totale si aucun sinistre n'aura été constaté au sein de tous les

45 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 6 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

46 SIMPLESURANCE, 2012. Que faison-nous ? *Simplesurance* [en ligne]. [consulté le 10 mai 2021]. Disponible à l'adresse : https://www.simplesurance.com/fr/que-faisons-nous/

47 Abdikerimova Samal and Feng Runhuan, 2019. *Peer-to-Peer Multi-Risk Insurance and Mutual Aid* [en ligne] [consulté le 10 mai 2021]. Disponible à l'adresse : https://ssrn.com/abstract=3505646

membres du groupe. Cette prime correspond à environ 100 euros en moyenne. Dans le cas où il y aurait des sinistres durant l'année, la prime de remboursement diminuerait en conséquence. Dans le cas où le coût des sinistres s'élèverait à un montant supérieur au total des primes, les sinistres seront couverts par un contrat d'assurance externe.

Les assurances sur demande :

L'assurance sur demande est une assurance qui permet de couvrir les clients à un moment précis. Au lieu de se faire assurer sur 12 mois, il est possible de se faire assurer qu'un seul mois par exemple. Lorsqu'on prend une assurance voyage, l'assurance sera activée uniquement lorsqu'on achète les billets ou bien pour une assurance auto, l'assurance sera activée au moment où l'on utilise la voiture. [48]

Les assurances digitales :

L'assurance digitale est une assurance entièrement digitalisée. Toutes les étapes de la chaîne de valeurs sont digitalisées. La vente, la souscription, le marketing, la résiliation, la gestion des sinistres, absolument tout est digitalisé.

Analyse de big data& logiciel d'assurances

Comme on a pu le voir, les assurances utilisent énormément de données. Ces assurances ont à leurs dispositions de grandes bases de données. Compte tenu du fait que toutes ces données soient décentralisées, il est difficile d' y accéder. Cette insurtech permet de faciliter la tâche à ces assureurs dans le but de les aider dans leur activité d'analyse de données. Il existe plusieurs starts up qui développent des logiciels afin d'aller dans ce sens. Nous avons par exemple « Getmelns » qui offre une solution pour limiter les actes de fraudes auprès de ces assurances mais également permet d'améliorer la solution d'assurance qui est personnalisée pour les différents clients. Il y a également « Zenefits » qui n'aide pas uniquement les assurances mais aussi d'autres types d'entreprises comme les petites et moyennes entreprises. En effet, cette start up offre un logiciel pour gérer au mieux la gestion des ressources afin de les aider dans cette tâche. Elle permet également d'offrir une solution à leurs employés afin de trouver la meilleure assurance pour eux. Ce qui a comme impact de supprimer l'intervention des courtiers. [49]

---

48 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 6 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

49 BRAUN, Alexander; SCHREIBER, Florian 2017. *The Current InsurTech*

Blockchain & smart contracts

Nous avons vu que l'assurance utilise une grande quantité de données. Nous avons également vu que durant cette dernière décennie une nouvelle technologie a vu le jour sous le nom de blockchain qui permet de traiter et stocker des informations de manière immuable et transparente. Il est donc tout à fait logique que des entrepreneurs ont décidé de fusionner la blockchain avec l'assurance. Ce qui a donné naissance à des starts up tel que « Everledger » qui offre un registre distribué afin de déterminer les propriétaires de diamants. En collaboration avec des assurances, elle va permettre de limiter les actes frauduleux dans ce domaine. [50]

Jusqu'à présent nous avons vu la blockchain ainsi que l'assurance et les insurtech afin de comprendre comment elles fonctionnent et qui elles sont. Maintenant, nous allons voir la confiance et la transparence qui sont deux éléments importants dans ce travail.

Landscape: Business Models and Disruptive Potential [en ligne] I.VW HSG Schriftenreihe, No. 62, ISBN 978-3-7297-2009-1, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St.Gallen. [consulté le 6 mai 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646

50 SIMPLESURANCE, 2012. Que faison-nous ? *Simplesurance* [en ligne]. [consulté le 10 mai 2021]. Disponible à l'adresse :]https://www.simplesurance.com/fr/que-faisons-nous/

4. La confiance

4.1 Économie

Laurent ELOI défini la confiance de cette manière : « *la confiance est une espérance de fiabilité dans les conduites humaines, qui suppose un rapport à un autre être humain, dans le cadre d'une situation incertaine, dans un but et contexte précis, cette espérance de fiabilité étant le fruit d'une volonté individuelle* »[51] *(ELOI , 2012, pp.5)*. Toujours le même auteur, affirme que la confiance peut être présente sous différentes formes et de différentes manières.

Georges AKERLOF est un économiste américain qui a notamment étudié les imperfections de marché. C'est notamment grâce à ces travaux sur les imperfections de marché, qu'il a remporté le prix Nobel d'Économie en 2001.[52] A partir des années 1970, Akerlof a relevé que la confiance fait partie des différentes garanties informelles qui ont une certaine importance dans les échanges de manière générale ainsi que dans la production. En effet, la confiance est la base de tous les types de rapports ou de relations que cela soit économique ou bien social. Même si la base de la confiance économique est avant tout une confiance sociale entre plusieurs acteurs.[53] Si on revient sur la définition de la confiance énoncée plus haut, on constate que selon cette définition, lors d'un rapport de confiance, les parties de cette relation espèrent donc que chacune des parties soit fiable et respecte ses intentions initiales.

L'un des plus grands exemples de l'importance de la confiance en économie est sans doute le cas de Bernard Lawrence MADOFF qui a mis en place une pyramide de Ponzi qui a débutée à la fin des années 1990 pour se conclure en 2009. L'arnaque pour laquelle il a dérobé jusqu'à 65 milliards de dollars. Madoff avait créé une société d'investissement dans laquelle, il offrait des rendements aux alentours de 15% chaque années. Malgré les crises et les fluctuations économiques, il a toujours réussi à satisfaire ses clients. Pour se

51 ELOI, Laurent,2012. *Économie de la confiance* [en ligne]. Paris : La Découverte, Paris, 2012, 128 [consulté le 18 juin 2021]. Disponible à l'adresse : https://cdn.reseau-canope.fr/archivage/valid/N-2305-11466.pdf

52 MINISTERE DES ECONOMIES DES FINANCES ET DE LA RELANCE. *Georges Akerlof*. [en ligne]. [consulté le 18 juin 2021].Disponible à l'adresse :https://www.economie.gouv.fr/facileco/georges-akerlof

53 ELOI, Laurent,2012. *Économie de la confiance* [en ligne]. Paris : La Découverte, Paris, 2012, 128 [consulté le 18 juin 2021]. Disponible à l'adresse : https://cdn.reseau-canope.fr/archivage/valid/N-2305-11466.pdf

faire, tant qu'il y avait de nouveaux clients et que la somme qui rentrait dans son fonds d'investissement était supérieure à la somme qui en sortait. Il utilisait l'argent des nouveaux clients afin de payer les rendements des clients déjà présents dans son fonds. Les périodes économiques de calme plat, il n'y avait pas trop de problèmes, à assurer ces rendements. Lors des différentes crises ou les personnes voulaient récupérer leurs argents, il a dû mettre en avant son charisme et son pouvoir de persuasion. Les gens lui faisaient confiance puisqu'il était le fondateur du NASDAQ et qu'il était une personne extrêmement respectée à Wall Street qui a prouvé son talent à travers les années. Même au moment où l'organisme de régulation des marchés financiers (SEC) n'avait qu'à appeler la DTC (société dépositaire de titre)[54] pour savoir si les opérations de titres avaient bien été effectuées comme le prétendait la société d'investissement de Madoff, elle ne l'a pas fait, tout simplement parce qu'ils n'avaient rien trouvé lorsqu'ils ont fait leur audit auprès de Madoff L. Security ainsi que de la confiance que la SEC avait en Bernard Madoff. [55]

En soit c'est cette confiance que les gens avaient en Bernard Madoff, qui lui ont permis de réussir son arnaque aussi longtemps dans le temps. [56]

54 KLENTON Bill, SCOTT Gordon.Depository trust company (DTC) *Investopedia*.[en ligne]. 29 mai 2021. [consulté le 18 juin 2021] Disponible à l'adresse : https://www.investopedia.com/terms/d/dtc.asp

55 FRANCE24, 2021. Bernard Madoff, ancien financier et plus grand escroc de l'Histoire, est mort, *France24*. [en ligne]. 14 avril 2021. [consulté le 18 juin 2021]. Disponible à l'adresse : https://www.france24.com/fr/amériques/20210414-bernard-madoff-ancien-financier-et-plus-grand-escroc-de-l-histoire-est-mort

56 ROBBINS BEN [réalisateur], 2016. Madoff, l'arnaque du siècle [film]. USA : ABC.

4.2 Blockchain

Le directeur de Synergix a effectué une conférence sur *« Comment améliorer la confiance des donateurs grâce à la transparence et aux technologies ? »*[57] *(SYNERGIX)* selon lui, pour obtenir de la confiance, par exemple pour une ONG qui cherchent des donateurs, elle va devoir démontrer de la transparence. Un des éléments sur lequel l'ONG doit travailler pour développer la confiance c'est la transparence.[58] Comme nous l'avons vu plus haut, dans la blockchain, cet aspect de transparence est une des caractéristiques de la blockchain. Cette transparence est liée au fait que toutes les transactions peuvent être visibles. Nous allons voir à présent de quelle manière ces informations sont visibles dans la blockchain.

Pour se faire, nous allons prendre l'exemple de la plateforme d'Ethereum. Sur Ethereum comme sur toutes les blockchains il est possible de voir toutes les transactions et tout l'historique de transactions des différents contrats qui ont été créés sur Ethereum. On appelle ce genre d'outil un explorateur de blockchain. L'explorateur pour Ethereum se nomme Etherscan. Avant de rentrer dans les détails d'Etherscan, il est important de prendre connaissance des types de codes qui existent lorsqu'on programme. Les différents langages de programmation que nous utilisons tels que C++, java, python etc…, sont appelés code source. Ce code source est uniquement compréhensible pour un être humain. Une machine ne va pas pouvoir lire ce code. Le langage qui est compréhensible par la machine s'appelle le code machine. De ce fait, afin que la machine puisse lire le code qu'un programmeur a écrit, il va devoir être transformé en code machine. Les langages de programmation qui sont appelés « langage de programmation de haut niveau » tel que C par exemple utilisent un compilateur pour transformer le code source en code machine. En revanche, il existe des langages de programmation tel que solidity par exemple qui utilise un code intermédiaire qui s'appelle le byte code. Nous avons dit que pour passer d'un code source à un code machine on utilise un compilateur. Solidity quant à lui va utiliser un compilateur pour passer du code source au byte code et ensuite

57 SYNERGIX. ONG : Comment améliorer la confiance des donnateurs grâce à la transparance et à la technologie ? *Synergix*. [en ligne]. [consulté le 27 juin 2021]. Disponible à l'adresse :]http://www.synergix.ch/fr/info/news/ong-ameliorer-confiance-donateurs-transparence-technologie

58 SYNERGIX. ONG : Comment améliorer la confiance des donnateurs grâce à la transparance et à la technologie ? *Synergix*. [en ligne]. [consulté le 27 juin 2021]. Disponible à l'adresse :]http://www.synergix.ch/fr/info/news/ong-ameliorer-confiance-donateurs-transparence-technologie

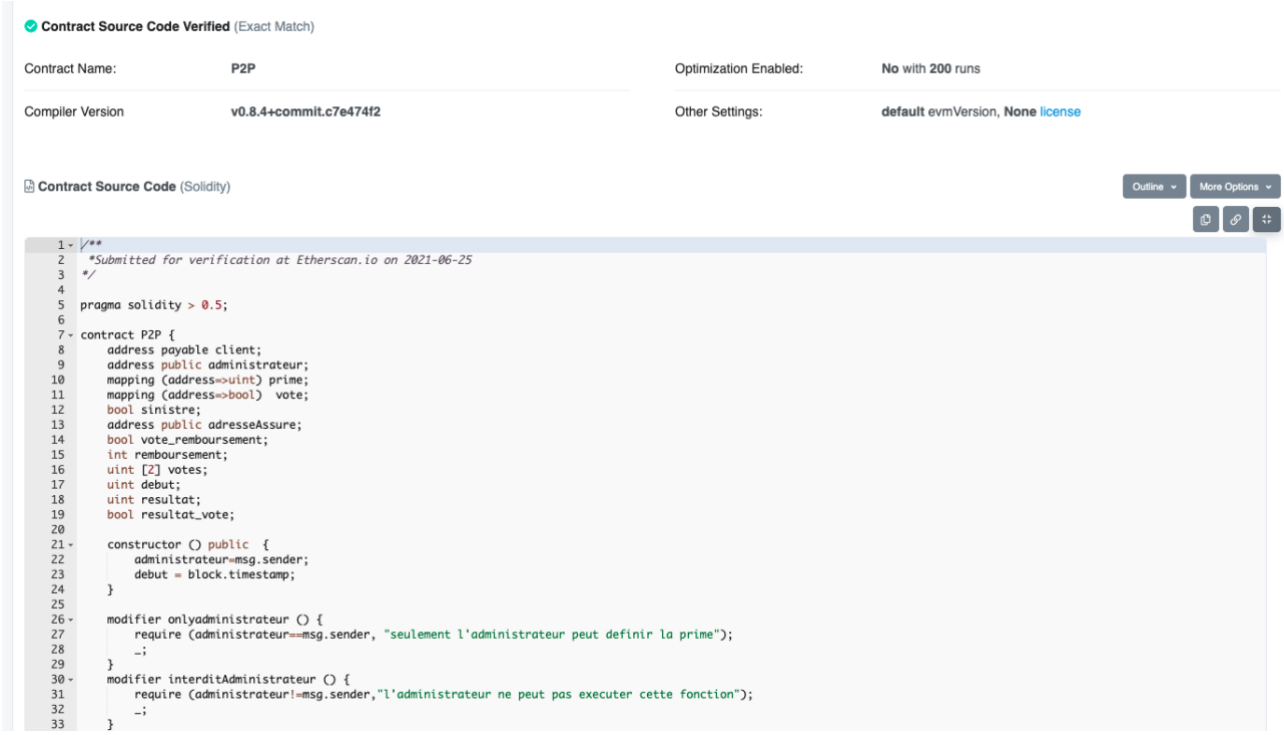
il va utiliser une machine virtuelle pour passer du code intermédiaire (byte code) au code machine. [59]

Lorsqu'une personne télécharge son contrat sur Ethereum, la seule version qui sera stockée sera le byte code. De ce fait, si une personne s'intéresse à connaître le code source qui a été utilisé pour créer son contrat dans une optique de transparence, il ne va pas pouvoir. C'est pourquoi Etherscan permet aux développeurs du contrat de montrer le code source sur Etherscan. Le mécanisme utilisé par Etherscan pour montrer le code source s'appelle la vérification du contrat. Pour cette vérification, le créateur du contrat va devoir télécharger le code source du contrat ainsi que définir quel compilateur il a utilisé pour développer son contrat sur remix solidity. Après avoir fait cela, Etherscan va compiler le code source avec le compilateur que le développeur a annoncé plus tôt. Si le résultat de cette compilation (byte code) est la même que le byte code qui a été stocké lors du téléchargement du contrat sur Ethereum, alors le code source va être validé par Etherscan et deviendra public. [60] A la page suivante, nous allons pouvoir aller sur Etherscan et voir un contrat que j'ai créé ainsi que toutes les informations qui sont fournies.

59 SWAKINOME. Différence entre le code source et le bytecode. *SWAKINOME* [en ligne]. [consulté le 27 juin 2021]. Disponible à l'adresse : https://fr.sawakinome.com/articles/programming/difference-between-source-code-and-bytecode.html

60 Oliva G.A., Hassan A.E., Jiang Z.M, 2020. *An exploratory study of smart contracts in the Ethereum blockchain platform*. [en ligne]. Empir Software Eng 25, 1864–1904 (2020). [consulté le 27 juin 2021]. Disponible à l'adresse : https://doi.org/10.1007/s10664-019-09796-5

Figure 13: Etherscan (1/2)



Contract Source Code Verified (Exact Match)

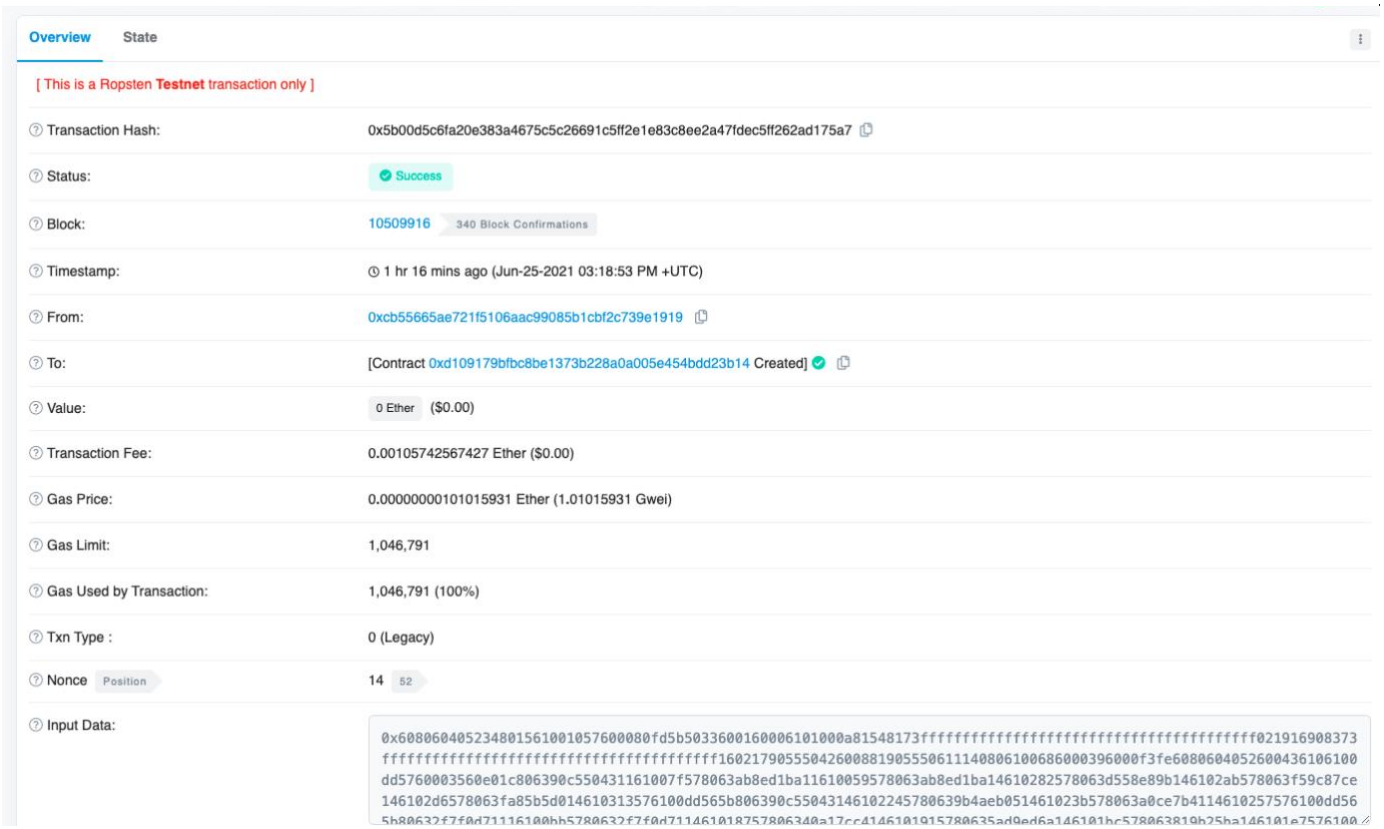
Contract Name:	P2P	Optimization Enabled:	No with 200 runs
Compiler Version	v0.8.4+commit.c7e474f2	Other Settings:	default evmVersion, None license

Contract Source Code (Solidity)

Outline | More Options

```
/**
 *Submitted for verification at Etherscan.io on 2021-06-25
*/

pragma solidity > 0.5;

contract P2P {
    address payable client;
    address public administrateur;
    mapping (address=>uint) prime;
    mapping (address=>bool)  vote;
    bool sinistre;
    address public adresseAssure;
    bool vote_remboursement;
    int remboursement;
    uint [2] votes;
    uint debut;
    uint resultat;
    bool resultat_vote;

    constructor () public  {
        administrateur=msg.sender;
        debut = block.timestamp;
    }

    modifier onlyadministrateur () {
        require (administrateur==msg.sender, "seulement l'administrateur peut definir la prime");
        _;
    }
    modifier interditAdministrateur () {
        require (administrateur!=msg.sender,"l'administrateur ne peut pas executer cette fonction");
        _;
    }
```

Figure 12: Etherscan (2/2)



Overview | State

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0x5b00d5c6fa20e383a4675c5c26691c5ff2e1e83c8ee2a47fdec5ff262ad175a7
Status:	Success
Block:	10509916 340 Block Confirmations
Timestamp:	1 hr 16 mins ago (Jun-25-2021 03:18:53 PM +UTC)
From:	0xcb55665ae721f5106aac99085b1cbf2c739e1919
To:	[Contract 0xd109179bfbc8be1373b228a0a005e454bdd23b14 Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.00105742567427 Ether ($0.00)
Gas Price:	0.000000001015931 Ether (1.01015931 Gwei)
Gas Limit:	1,046,791
Gas Used by Transaction:	1,046,791 (100%)
Txn Type :	0 (Legacy)
Nonce Position	14 52
Input Data:	0x6080604052348015610010576000080fd5b5033600160006101000a81548173ffffffffffffffffffffffffffffffffffffffff021916908373ffffffffffffffffffffffffffffffffffffffff1602179055504260088190555061114080610068600039600f3fe6080604052600436106100dd5760003560e01c806390c550431161007f578063ab8ed1ba11610059578063ab8ed1ba14610282578063d558e89b146102ab578063f59c87ce146102d6578063fa85b5d014610313576100dd565b806390c550431461022457806390b4aeb051461023b578063a0ce7b4114610257576100dd565b80632f7f0d71116100bb5780632f7f0d7114610187578063340a17cc4146101915780635ad9ed6a146101bc578063819b25ba146101e7e7576100

Au sein de la première illustration, nous avons le code source que j'ai vérifié en utilisant le mécanisme décrit plus haut en utilisant le byte code pour confirmer le code source de cette transaction. Toutes ces informations sont certes assez techniques. De ce fait, si une personne n'est pas intéressée par ce code, ces informations sont inutiles. Une personne qui n'est pas intéressée ne va même pas regarder ces aspects-là. En revanche, les personnes à qui ces informations intéressent, elles sont très importantes et très intéressantes pour ces dernières. Cette transparence d'informations amène une confiance de la part de l'organisation qui a mis tout cela en place puisque les parties prenantes peuvent absolument tout voir. Ainsi, on ne peut rien cacher et tout ce sait, ce qui permet d'augmenter la confiance de la part des clients, et cela, que le client s'intéresse à ces informations techniques ou pas.

Sur la seconde illustration, on peut voir la transaction de la création de mon contrat. Nous pouvons voir énormément d'informations tel que le hash de la transaction, le nonce, les différentes valeurs en termes de gas et même en termes de transactions, mais également la date à laquelle le contrat a été faites, les deux parties du contrat et également ce dont j'ai parlé plus haut le byte code du contrat.

Avec l'ajout de certains éléments comme je l'ai fait en ajoutant le code source sur Etherscan, cela permet d'augmenter encore plus cette transparence mais cela dépend uniquement du bon vouloir du développeur du contrat.

4.3 Assurance pair-à-pair

Nous l'avons vu dans ce travail, l'assurance pair-à-pair permet à un groupe de s'assurer entre eux. Une prime va être payée par les différents membres et une certaine proportion de fonds sera allouée au paiement des assurés en cas de sinistres. Le but étant de faire disparaître l'assureur et diminuer les coûts des primes qui sont très souvent discutés. Dès qu'une personne est lésée, les membres vont voter pour ou contre le paiement du sinistre de tel assuré. Le paiement de cette prime dépend fortement du bon vouloir de l'assuré en question.[61]La solidarité ainsi que la responsabilité des différents membres sont des notions essentielles au bon fonctionnement de cette assurance étant donné qu'il n'y a pas d'assureur qui tranche sur les différentes décisions. Et étant donné qu'à la fin ils peuvent se partager le bénéfice s'il reste une valeur dans le fond cela augmente encore plus l'importance des deux notions citées plus haut.[62]

De ce fait, une partie de confiance est prise en compte dans ce processus et à une importance cruciale. Les membres doivent se faire confiance afin de pouvoir aller de l'avant avec cette assurance. Par exemple, le paiement de la prime, si la confiance disparaît où n'est tout simplement pas présente il risque d'y avoir de nombreux problèmes tel que des refus volontaires d'indemnisation. Prenons un exemple, dans lequel un assuré a dû faire plusieurs demandes de remboursement. Étant donné que le nombre de demande de cet assuré est bien au-dessus de la moyenne des demandes du réseau. Certains décident alors de refuser cette demande. L'assuré lésé a été mécontent de cette réaction des autres membres et ils décident de se venger et donc refuser également à son tour les demandes de remboursement de ces autres collègues. De ce fait, un climat de méfiance s'installe dans ce réseau et donc ce réseau ne marche plus ou plutôt moins bien. La confiance a une part extrêmement importante dans tous ces projets pair-à-pair.

61 SIAPARTNERS, 2020. L'assurance « peer-to-peer » : vers un essor de l'assurance communautaire ?. *Siapartners*.[en ligne]. 25 juin 2020. [consutlé le 4 juillet] Disponible à l'adresse : https://www.sia-partners.com/fr/actualites-et-publications/de-nos-experts/lassurance-peer-peer-vers-un-essor-de-lassurance

62 DAVTIAN Wlly, 2018. Blockchain et assurance : espérance démesurée ou nouvelle ère. *Revue-banque*. [en ligne]. 15 mai 2018. [consulté le 4 juillet 2021]. Disponible à l'adresse : http://www.revue-banque.fr/banque-detail-assurance/article/blockchain-assurance-esperance-demesuree-nouvelle

5. La transparence

Dans la partie de la confiance on a pu voir qu'il pourrait y avoir une certaine relation entre la confiance et la transparence. Mais qu'en est-t-il véritablement ?

D'après le Larousse la définition de la transparence est : « *Parfaite accessibilité de l'information dans les domaines qui regardent l'opinion publique* ».[63]*(LAROUSSE)* En partant de cette définition, nous allons voir la transparence à travers 3 parties :

- La transparence en économie/finance
- La transparence dans la blockchain
- La transparence dans l'assurance-pair-à-pair

5.1 Économie

Selon les auteurs du livre « Une analyse informationnelle de la crise financière récente », le manque de transparence au sein des marchés financiers durant la crise de 2008 fait partie des différentes raisons qui ont causé la crise des subprimes. Afin de répondre à cette crise, les autorités de régulation des marchés financiers ont décidé d'augmenter la transparence.[64] En effet, avec les nouveaux accords de Bâle II et de Bâle III, l'augmentation de la transparence a été mise en place en augmentant le flux des informations tel que leurs niveaux de risques et leurs niveaux de capitaux par exemple. Elles ont notamment le devoir de décrire d'où viennent leur fonds propre, c'est-à-dire la source de ces fonds, mais également annoncer le montant de capital qu'elles ont besoin pour les différentes catégories de risque. De plus, elles doivent montrer les procédures de gestion du risque qu'elles ont décidés de mettre en place. Elles doivent donc divulguer des informations tel que leurs expositions globales au risque, la zone géographique[65].

Cette notion de transparence n'a pas impacté uniquement les banques mais également les différents clients des banques suisses. Ces dernières années, on nous a déjà demandé au moins une fois si nous étions résidents américains. En effet, depuis 2014 les

63 LAROUSSE. Transparence. Larouse[en ligne] [consulté le 20 juillet 2021]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/transparence/79194

64 ALLEGRET Jean-Pierre, CORNAND Camille, Une analyse informationnelle de la crise financière récente, *Revue française d'économie*. ,[en ligne]2013/3 (Volume XXVIII), p. 213-264. DOI : 10.3917/rfe.133.0213.[consulté le 10 juillet 2021]. Disponible à l'adressee: https://www.cairn.info/revue-francaise-d-economie-2013-3-page-213.htm

65 FARVAQUE Étienne, REFAIT-ALEXANDRE Catherine, Les exigences de transparence des accords de Bâle : aubaine ou fardeau pour les pays en développement ? [1] *», Mondes en développement*. [en ligne] 2016/1 (n° 173), p. 131-147. DOI : 10.3917/med.173.0131. [consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.cairn.info/revue-mondes-en-developpement-2016-1-page-131.htm

banques suisses ont une obligation de renseignement auprès des autorités fiscales américaines concernant leurs citoyens ayant des comptes en suisse. Cela dans le but de lutter contre l'évasion fiscale. La transparence est donc une notion qui a son importance en économie et qui a bien augmenté ces dernières années. [66]

5.2 Blockchain

Nous l'avons évoqué plus haut, la transparence est une notion importante dans la blockchain. Toutes personnes disposant de la clé publique pourraient avoir accès à tout ce qui passe dans cette chaîne, que ces soit les différentes transactions, les auteurs de ces dernières, ou bien quand cela a été fait[67]. Nous avons également pu voir cette transparence dans les explorateurs de blockchains dans la partie confiance.

Cette transparence est devenue une plus-value importante dans de nombreux domaines, par exemple dans la traçabilité alimentaire. Il suffit donc de scanner un QR code qui est sur l'aliment que vous mangez ou bien que vous désirez manger. Cela ouvrira une page internet et vous donnera de nombreuses informations tel que d'où vient l'aliment, par où il est passé avant d'arriver dans votre assiette, comment est-t-il venu jusqu'à vous.

D'après Clément LESAFRE, cette transparence permet de créer une sorte de lien entre le producteur et le consommateur final comme si le consommateur faisait entièrement partie de la chaîne qui amène l'aliment du producteur jusqu'au consommateur. Toujours selon le même auteur, un des avantages de la blockchain pour ce type d'utilisation c'est d'amener de la confiance dans la chaîne de production. [68]

5.3 Assurance-pair-à-pair

On a vu plus haut que ce soit dans la partie insurtech ou bien la partie de la confiance ce qu'est l'assurance pair-à-pair et ce qu'elle permet de faire. Nous avons vu en termes de

---

66 WELSCH, Fabrice, 2017. Pourquoi me demande-t-on si je suis américain quand je veux ouvrir un compte bancaire ? *BCV* [en ligne]. 07 août 2017. [consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.bcv.ch/pointsforts/Votre-argent/2017/Pourquoi-me-demande-t-on-si-je-suis-americain-quand-je-veux-ouvrir-un-compte-bancaire

67 CHANDEZE, Aurélie, 2019. Partie 2 : la blockchain au service de la transparence. *Le monde informatique*. [en ligne]. 05 décembre 2019. [consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.lemondeinformatique.fr/les-dossiers/lire-la-blockchain%C2%A0au-service-de-la%C2%A0transparence%C2%A0-1026.html

68 LESAFFRE Clément, 2021. Traçabilité alimentaire : grâce à la blockchain, la transparence s'invite sur les emballages. *Europe 1*.[en ligne]. 02 mai 2021. 02 mai 2021. [consulté le 10 juillet 2021]. Disponible à l'adresse : LESAFFRE https://www.europe1.fr/economie/tracabilite-alimentaire-grace-a-la-blockchain-la-transparence-sinvite-sur-les-emballages-4042081

confiance ce qu'elle offre ainsi que ces risques. En revanche, lorsqu'on regarde de plus près, ces assurances sont-elles vraiment transparentes ?

En effet, lorsqu'on regarde l'assurance Lemonade », où nous allons nous arrêter sur son processus plus tard, les clients n'ont pas un grand accès à l'information, ils sont obligés de faire confiance que ce soit à Lemonade elle-même mais également aux autres clients.

J'ai téléchargé leur application mobile et que ce soit sur leur application mobile ou bien sur leur site internet les membres n'ont pas accès aux transactions des autres personnes ou bien même les primes des autres membres. L'aspect de transparence est manquant. Nous n'avons pas accès à énormément d'informations concernant les autres membres et cela est assez dérangeant étant donné que la transparence est une information assez importante dans ce genre d'assurance. Il serait intéressant de voir les primes des autres membres, le montant qu'ils ont payé. Mais Lemonade ne partage pas ces informations.

6. Méthodologie

La méthodologie utilisée dans le cadre de ce travail est principalement axée sur une analyse comparative des deux modèles d'assurance pair-à-pair. C'est-à-dire l'assurance avec la blockchain et celle sans l'utilisation de la blockchain. Avant d'arriver à cette partie d'analyse il était important d'avoir une revue de littérature complète afin d'avoir les bonnes notions pour attaquer cette comparaison.

Dès que cette revue de littérature sur la blockchain, l'assurance pair-à-pair ainsi que de la confiance et de la transparence ont été faites, la partie d'analyse pouvait commencer. Mon analyse s'est basée sur une comparaison de l'assurance-pair-à-pair sans l'utilisation de la blockchain et de son processus, avec l'assurance-pair-à-pair, dont la blockchain et les smarts contracts sont présents.

J'ai donc analysé une assurance présente sur le marché qui est « Lemonade », en ce qui concerne l'assurance pair-à-pair sans blockchain. Pour ce faire, j'ai récolté les informations dont j'avais accès, dans le but de reproduire le processus complet de cette assurance sous forme d'ordinogramme. Ces informations ont été récoltées sur le site internet de Lemonade, dans leur application, ou bien même auprès d'une police d'assurance de Lemonade. Dans certains cas où je n'avais pas accès aux informations escomptées, j'ai tout simplement posé la question aux services de Lemonade qui m'ont répondu par mail.

Ensuite pour l'assurance-pair-à-pair avec la blockchain, j'ai créé directement un contrat d'assurance pair-à-pair (c'est-à-dire du code) et effectué l'ordinogramme de ce processus. Pour cette partie de code, j'ai pris contact avec le professeur de la Haute Ecole de Gestion de Genève de la filière informatique de gestion Mr. Rolf HAURI afin de me conseiller et m'aider à structurer mon assurance pair-à-pair. Mais également sur certains éléments en termes de code.

Dès que les deux processus ont été faits, j'ai pu énoncer les résultats de cette comparaison. Le but de cette comparaison est donc de démontrer quel est l'impact de la blockchain et des smarts contracts en termes de confiance et de transparence pour les assurés d'une assurance pair-à-pair. Ainsi que de connaître la façon d'intégrer la blockchain avec l'assurance pair-à-pair.

7. Analyse assurances pair-à-pair

A présent, nous allons voir les différences en termes de procédure entre l'assurance pair-à-pair traditionnelle et celle où la blockchain ainsi que les smart contracts sont présents.

7.1 Assurance pair-à-pair sans blockchain

L'insurtech que nous allons analyser pour cette comparaison sera « Lemonade » en effectuant une modélisation sous forme d'ordinogramme afin de connaître tout le processus de cette assurance. Lemonade propose différentes couvertures d'assurance. En effet, cette start up américaine propose des couvertures, pour les propriétaires de bien immobilier, les locataires pour les animaux ainsi que l'assurance vie, de plus bientôt ils proposeront également une assurance automobile.[69] Leurs solutions sont entièrement digitalisées avec notamment l'intégration de l'intelligence artificielle dans leurs processus. Cette start up a vu le jour en 2015. A présent, elle emploie plus de 500 personnes et est cotée au « New-York Stock Exchange ».[70]Lemonade est présente bien évidemment aux Etats-Unis, mais également en France, en Allemagne et au Pays-Bas.[71]

Tout ce passe sur leur application mobile, pour souscrire à une des assurances proposées par Lemonade. Il est possible d'utiliser leur site Internet, mais lorsqu'il y aura besoin de faire une demande de remboursement par exemple, il est primordial d'utiliser son téléphone portable. Lemonade utilise l'intelligence artificielle et notamment le machine learning. Selon HPE (Hewlett-Packard Entreprise), le machine Learning est définit comme tel :« *Le machine learning fait référence au processus par lequel les ordinateurs développent la reconnaissance de schémas ou l'aptitude à apprendre continuellement et à faire des prévisions basées sur des données, puis à faire des ajustements sans avoir été spécifiquement programmés pour le faire. Forme d'intelligence artificielle, le machine learning automatise de manière efficace le processus de création de modèle analytique et permet aux machines de s'adapter à de nouveaux scénarios de*

69 LEMONADE. *Lemonade* [en ligne]. [Consulté le 21 juin 2021]. Disponible à l'adresse : https://www.lemonade.com

70 CRUNCHBASE. Lemonade. *Crunchbase* [en ligne]. [Consulté le 22 juin 2021] Disponible à l'adresse : https://www.crunchbase.com/organization/lemonade/company_financials

71 DEVENTER Cate, 2021. Lemonade Insurance. *Bankrate* [en ligne] 05 mai 2021. [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.bankrate.com/insurance/homeowners-insurance/lemonade-insurance-review/

manière autonome. ».[72] *(HEWLETT PACKARD)* Le machine learning permet donc à la machine d'apprendre toute seule ainsi que de faire des prévisions selon certaines données qui lui ont été transmises. Dans le cas de Lemonade et de l'assurance en général cette technologie permet de prédire par exemple la prime exacte pour les assurés en fonction, des différents risques à prendre en compte lors de la tarification de ces primes. Les assurés ont tous des profils différents, le « machine learning » permet de regrouper au mieux les clients ayant un profil similaire et qui seraient susceptible de payer une prime similaire.[73] Cela est un élément très intéressant puisque cela permet de maximiser l'exactitude de la prime mais également de minimiser le coût de cette prime pour les clients.

72 HEWLETT PACKARD. Définition du machine learning. *Hewlett Packard*[en ligne]. [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.hpe.com/ch/fr/what-is/machine-learning.html

73 PETRA, 2018. Lemonade reinvents the insurance industry with machine learning. *Technology and operation management* [en ligne] 13 novembre 2018. [consulté le 22 juin 2021]https://digital.hbs.edu/platform-rctom/submission/lemonade-reinvents-the-insurance-industry-with-machine-learning/

7.1.1 Procédure

Nous allons voir la procédure de cette assurance dans les détails, séparé en trois parties afin d'illustrer le processus de manière plus précise. L'ordinogramme complet en une seule illustration se trouve en annexe

Figure 14: Processus Lemonade (1/5)

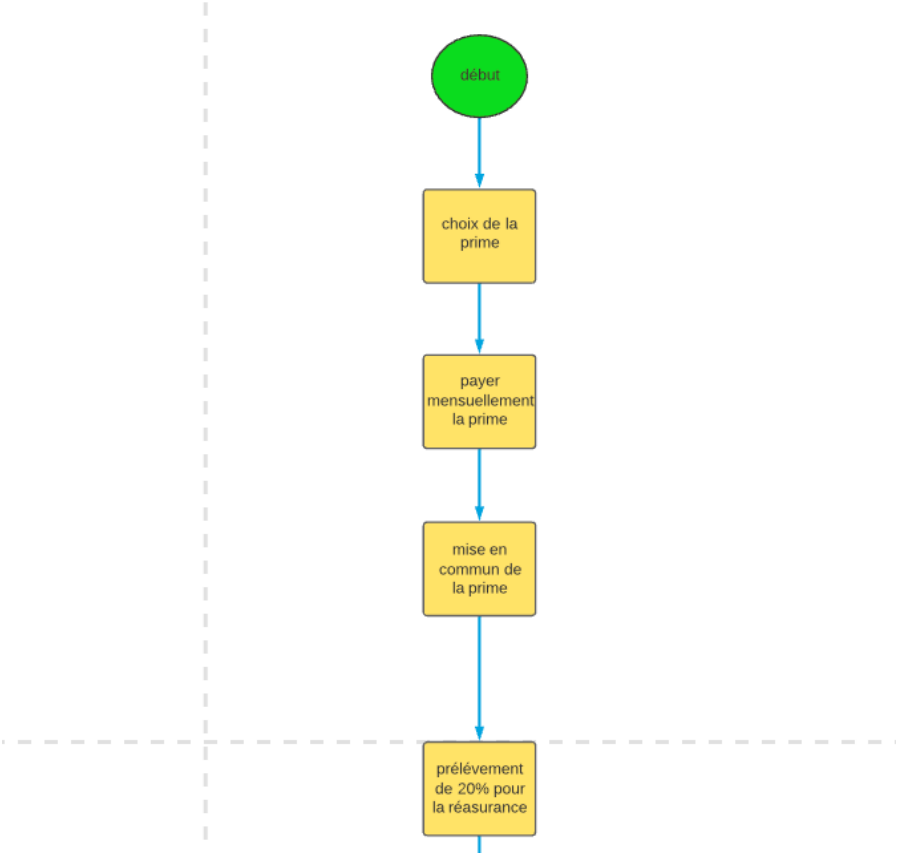


Figure 15: Processus Lemonade (2/5)

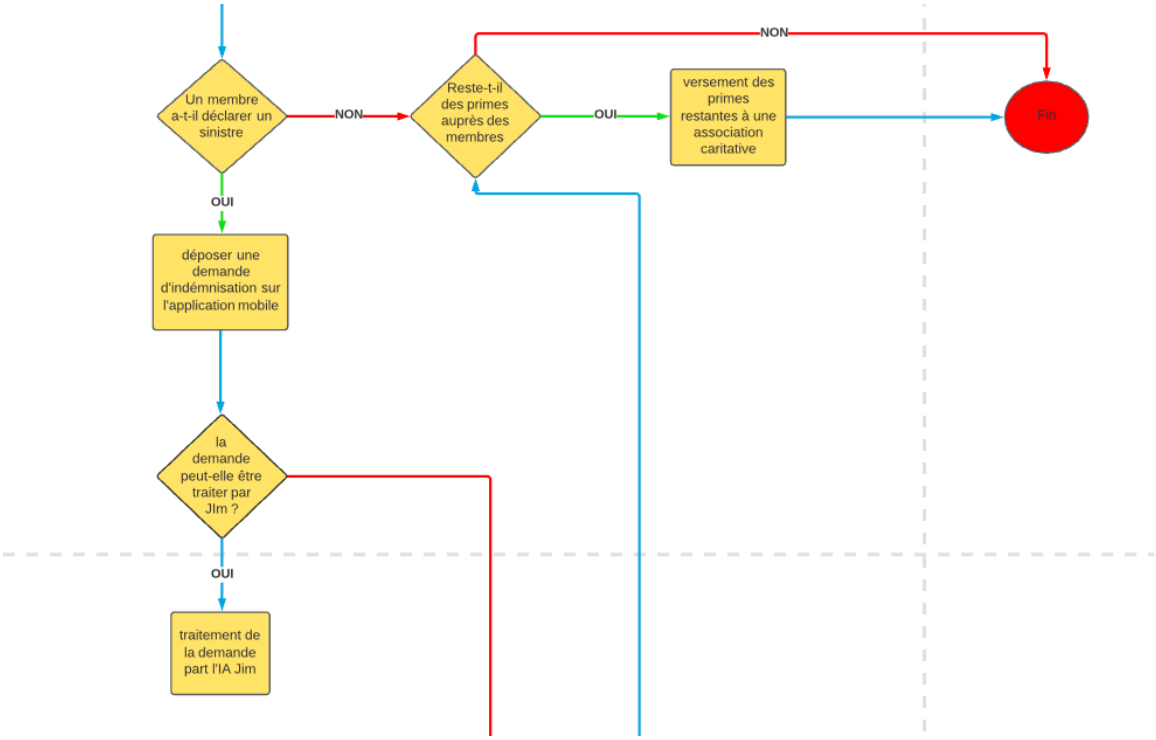


Figure 16: Processus Lemonade (3/5)

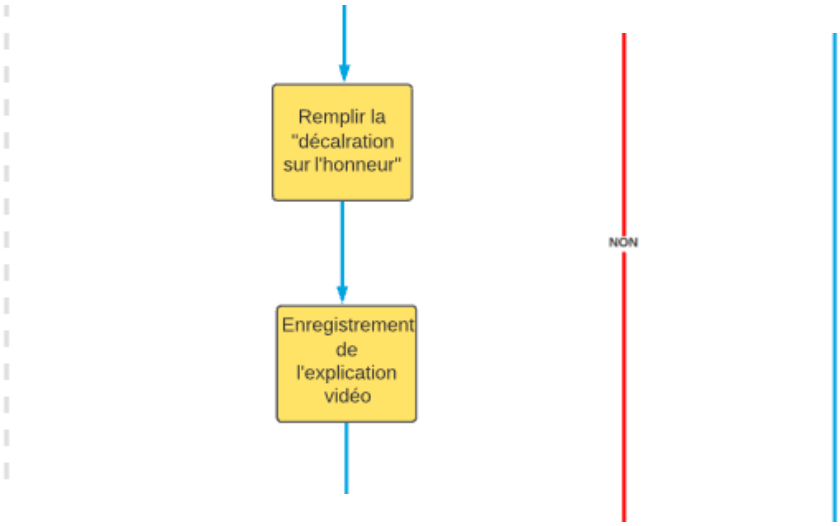


Figure 18: Processus Lemonade (4/5)

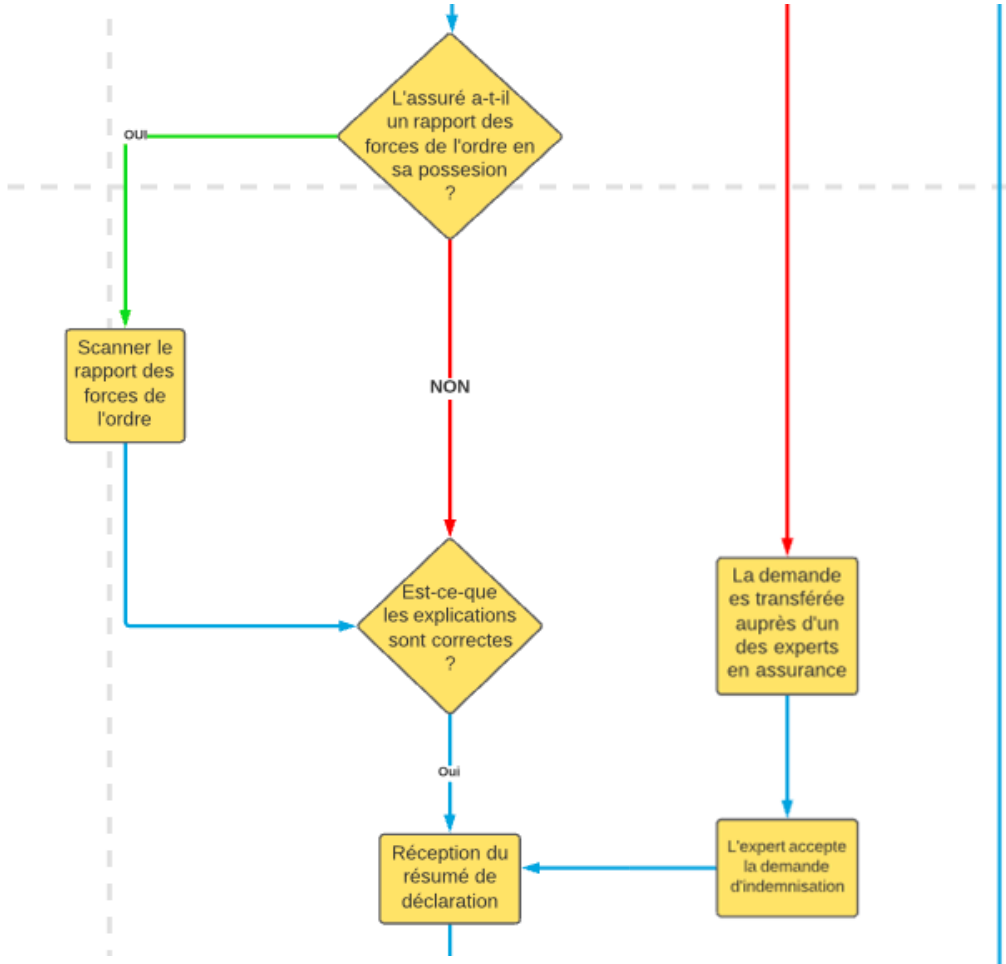
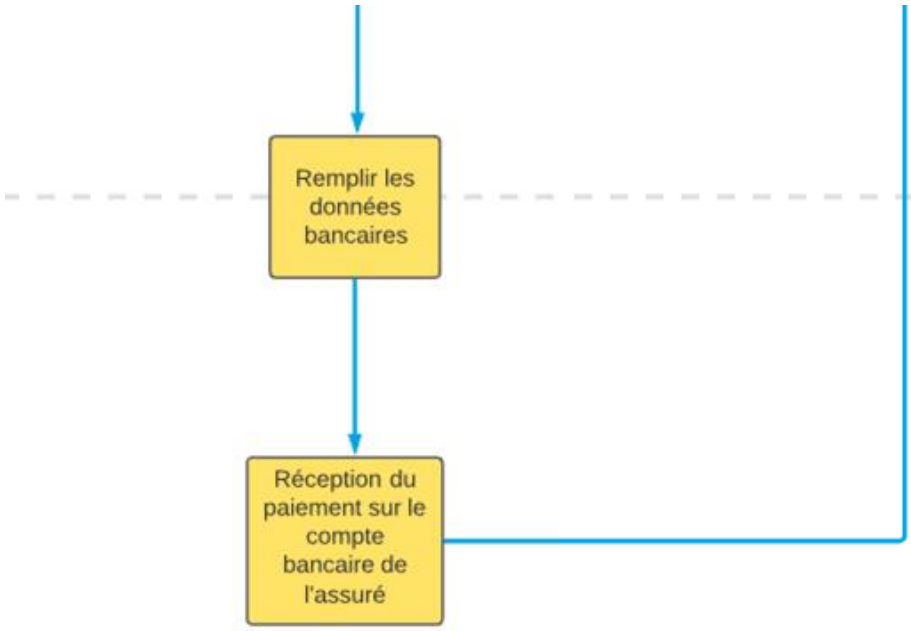


Figure 17: Processus Lemonade (5/5)



Souscription

Tout d'abord afin de souscrire à une des polices d'assurances proposées par « Lemonade », il faut aller sur leur site Internet ou bien sur leur application mobile. Afin de déterminer la prime idéale, l'assuré va devoir répondre à quelques questions qui vont être posées par de l'intelligence artificielle qui est nommée « Maya ». Mais avant tout, il est nécessaire de choisir quel type de police d'assurance l'assuré veut souscrire. Selon le pays dans lequel l'assuré se situe, il ne pourra pas avoir accès à toutes les assurances, par exemple en France il est seulement possible de souscrire à l'assurance habitation (propriétaire/locataire). Malgré le fait que la « start up » soit américaine, dans certains États américains il n'est pas possible de souscrire à toutes les polices d'assurances comme par exemple en Alabama où il est seulement possible de souscrire l'assurance pour les animaux de compagnies ainsi que l'assurance vie.[74] Après avoir répondu à quelques questions personnelles, « Maya » va poser des questions concernant la chose assurée. Si on prend l'exemple de l'assurance pour les animaux de compagnie, elle va demander notamment :

- Le type d'animal (chien/chat)
- Le nom de l'animal
- L'âge de l'animal
- Le lieu d'habitation
- Le type de race (pure/croisé)
- La race
- La santé de l'animal

Ces informations permettront de définir la meilleure prime en prenant compte des risques par rapport à la situation actuelle de l'assuré. Par exemple, selon certaines races, il y a plus de chances qu'ils soient malades ou bien selon l'âge voire même selon le quartier où ils vivent, le prix des vétérinaires est plus élevé que d'autres. Ce sont des paramètres très importants à prendre en compte afin de définir la prime. Dès lors que le souscripteur a répondu à toutes ces questions, la prime sera affichée ainsi que la police d'assurance dans laquelle est définie notamment ce que couvre cette assurance et ce qu'elle ne couvre pas. Si on veut augmenter la couverture d'assurance, il est possible moyennant

74 DEVENTER Cate, 2021. Lemonade Insurance. *Bankrate* [en ligne] 05 mai 2021. [Consulté le 22 juin 2021]. Disponible à l'adresse : https://www.bankrate.com/insurance/homeowners-insurance/lemonade-insurance-review/

une augmentation de la prime. La dernière étape qui devra être effectuée par l'assuré, c'est de définir la franchise. Ensuite, si l'assuré désire véritablement souscrire à cette assurance il n'aura qu'à remplir ces données bancaires afin d'activer l'assurance et payer la première prime de cette dernière.[75]

La prime sera mise en commun avec les autres assurés et qui sera ensuite utilisée en cas de sinistre. En revanche, le montant utilisé ne correspondra qu'à 80% de cette mise en commun. Le reste sera utilisé pour différents frais de fonctionnement ainsi que pour payer la prime auprès de la réassurance. Dans le cas où le montant de cette mise en commun serait inférieur au dédommagement du sinistre, alors la réassurance rentrera en compte pour couvrir ce manquement. [76]

Déclaration de sinistre

En cas de sinistre, l'assuré lésé va devoir faire une demande d'indemnisation qui est faite uniquement depuis l'application mobile. Contrairement à la partie souscription, la demande d'indemnisation ne peut pas être faite depuis le site internet. Cette demande sera traitée par l'intelligence artificielle nommée « Jim » dans le cas où le sinistre n'est pas très complexe. Cela correspond à 30% des indemnisations qui sont faites par Lemonade. Ce qui représente 1 millions de dollars. Dans le cas où il s'agirait d'un cas plus complexe, le dossier du client sera traité par un des experts en assurance qui travaillent pour « Lemonade »[77]

L'assuré devra répondre à différentes questions afin de savoir quelle est la cause du dommage, après avoir répondu à ces questions il devra remplir une déclaration sur l'honneur dans le but de confirmer la véracité des propos. Afin d'expliquer dans les détails ce qu'il s'est passé l'assuré devra envoyer une vidéo explicative. Selon la cause du dommage, et si l'assuré l'a en sa possession, il devra scanner le rapport de la police ou bien des pompiers. Pour effectuer correctement le remboursement, il va falloir également envoyer la facture des articles qui ont été volés. Cela permet donc de prouver l'appartenance de ces objets et de leur attribuer une valeur financière. Dès que toutes ces

75 LEMONADE. *Lemonade* [en ligne]. [Consulté le 24 juin 2021]. Disponible à l'adresse : https://www.lemonade.com/onboarding/2

76 OVERHOLT Maggie, 2020. How Lemonade Insurance Works ?, *Review*[en ligne]. 19 novembre 2020. [consulté le 25 juin 2021]. Disponible à l'adresse : https://www.reviews.com/insurance/homeowners/how-lemonade-insurance-works/

77 OVERHOLT Maggie, 2020. How Lemonade Insurance Works ?, *Review*[en ligne]. 19 novembre 2020. [consulté le 25 juin 2021]. Disponible à l'adresse : https://www.reviews.com/insurance/homeowners/how-lemonade-insurance-works/

étapes ont été faites, la personne lésée recevra un résumé de sa déclaration afin qu'elle confirme que toutes les informations qui ont été traitées par « Jim » ont été faites correctement. Ce document permettra également de définir sur quel compte en banque l'assuré désire se faire dédommager puisqu'il lui est demandé de fournir ses informations bancaires. La demande sera validée par 18 algorithmes anti-fraude mais également suivie par des experts en assurance, afin d'éviter les cas de fraudes à l'assurance. [78] Après cela, l'assuré en question recevra l'argent sur son compte. Que cela soit fait par un expert en assurance ou bien par « Jim », l'assuré sera toujours dédommagé car Lemonade ne refuse aucun cas contrairement à d'autres insurtechs du même type. [79]

Fin d'année

Lors de la souscription auprès de l'assurance, il a été demandé de choisir une œuvre de charité qui tenait à cœur les souscripteurs. A la fin de l'année, s'il reste encore de l'argent dans la mise en commun des différentes assurances, le montant sera envoyé aux différentes œuvres de charité. Ce montant sera proportionnel au poids que l'assuré prenait dans la mise en commun. Donc chaque année les montants présents au sein des différentes pot commun sont mis à zéro.

78 TEAM LEMONADE,2020. L'app Lemonade | Assurance Habitation pour locataires boostée à l'Intelligence Artificielle[enregistrement vidéo], *Vimeo* [en ligne]. 23 novembre 2020 [consulté le 25 juin 2021]. Disponible à l'adresse : https://vimeo.com/482550657

79 GALLO Meredith, 2020. Lemonade review : We tested an insurance company designed for people who hate to talk on the phone. *Chicago Tribune* [en ligne]. 18 mai 2020. [consulté le 25 juin 2021]. Disponible à l'adresse : https://www.chicagotribune.com/consumer-reviews/sns-bestreviews-lemonade-insurance-review-20200518-wdcqysvkgvbzxo2wazk6chdbwe-story.html

7.2 Assurance pair-à-pair avec blockchain

A présent que nous avons vu la procédure d'une assurance pair-à-pair qui n'a pas recours à la blockchain, nous allons voir une assurance pair-à-pair qui utilise la blockchain et les smart contracts. Cette assurance a été élaborée par mes soins à travers la plateforme solidity avec laquelle j'ai codé le smart contract qui permet la création de cette assurance pair-à-pair.

Avant de détailler toute la procédure pour cette assurance, il est important d'avoir connaissance d'un point théorique sur la blockchain concernant les oracles. Dans l'univers des smart contracts, les oracles sont définis par Ethereum sur leur site internet comme tel : « *An oracle is a bridge between the blockchain and the real world. They act as on-chain APIs you can query to get information into your smart contracts. This could be anything from price information to weather reports. Oracles can also be bi-directional, used to "send" data out to the real world.* »[80] *(ETHEREUM, 2021)*

Dans la blockchain, on ne peut pas avoir accès à des informations du « monde extérieur » comme par exemple la météo, ou bien les cotations au SMI des différentes entreprises. Afin de pouvoir traiter et utiliser ces informations dans la blockchain, il est donc nécessaire d'utiliser un oracle afin de relier ces informations du monde extérieur ou bien même inversement envoyer des données au monde extérieur. Dans ce contrat, il va être nécessaire d'utiliser un oracle afin de pouvoir inscrire différentes données dans le cadre d'une demande de remboursement et également pouvoir payer en dollars au lieu d'utiliser des crypto-monnaies dont on connaît malheureusement la volatilité. Un de ces deux oracles est "Chainlink".

80 GRIMAUD Pierre,2021. Oracles, *Ethereum* [en ligne]. 27 avril 2021 [consulté le 27 juin 2021]. Disponible à l'adresse : https://ethereum.org/en/developers/docs/oracles/

Chainlink est un oracle qui permet de pouvoir payer par exemple des tokens avec des monnaies fiduciaires à la place d'utiliser de l'ether. L'ether comme la plupart des crypto-monnaies est extrêmement volatil. Cela a souvent inquiété les personnes, le fait de devoir payer une certaine somme régulièrement et que d'une période à l'autre le prix augmente du double ou bien diminue du double. [81] La blockchain ne peut pas utiliser des données qui sont du monde « réel », ce qui fait que cela peut limiter l'utilisation de ces dernières. Les oralces sont des systèmes qui permettent de prendre des données extérieures afin de les utiliser dans les smart contracts. Ce que va permettre « Chainlink » est de pouvoir par exemple dans notre cas, de pouvoir payer les primes avec du dollar. En effet, il propose aux différents smart contracts de pouvoir traiter avec les différentes monnaies fiduciaires.

Figure 19: Chainlink

ARTIFICIAL LAWYER, 2018

Chainlink permet aussi d'offrir des informations des plateformes boursières telles que Bloomberg pour avoir le prix de certaines actions ou autres produits financiers. Et bien sûr ce qui nous intéresse le plus, des fournisseurs de paiements tel que Paypal et même les banques avec lesquels on paie toutes nos factures

Chainlink est déjà utilisé dans la finance décentralisée, comme avec Synthetix qui utilise cet oracle pour définir le prix des produits dérivés.[82] Cela permettra donc de répondre aux

81 HUXTABLE Jonny, 2018. Analysis of Chainlink – The decentralized Oracle Network. *Medium*. [en ligne]. 4 septembre 2018. [consulté le 27 juin 2021]. Disponible à l'adresse : https://medium.com/@jonnyhuxtable/analysis-of-chainlink-the-decentralised-oracle-network-7c69bee2345f

82 BITCOIN SUISSE, 2020. What is Chainlink ? *Bitcoin Suisse* [en ligne]. 5 octobre 2018. [consulé le 27 juin 2021]. Disponible à l'adresse : https://www.bitcoinsuisse.com/fundamentals/what-is-chainlink

craintes de certaines personnes envers les crypto-monnaies et donc d'utiliser les monnaies que nous utilisons tous les jours, même pour des projets décentralisés.

7.2.1 Procédure

Tout comme l'assurance vu plus haut, j'ai entrepris la conception de la procédure de mon assurance en différentes parties. Vous trouverez le processus complet de bout-en-bout en annexe. Pour ce faire je me suis inspiré des différentes assurances-pair-à-pair que j'ai découvert lors de mes recherches dans le cadre de ce travail ainsi que du cours d'atelier blockchain que j'ai eu au cours de ma 3ème année à la Haute Ecole de Gestion de Genève.

Figure 20: Procédure de mon contrat d'assurance (1/6)

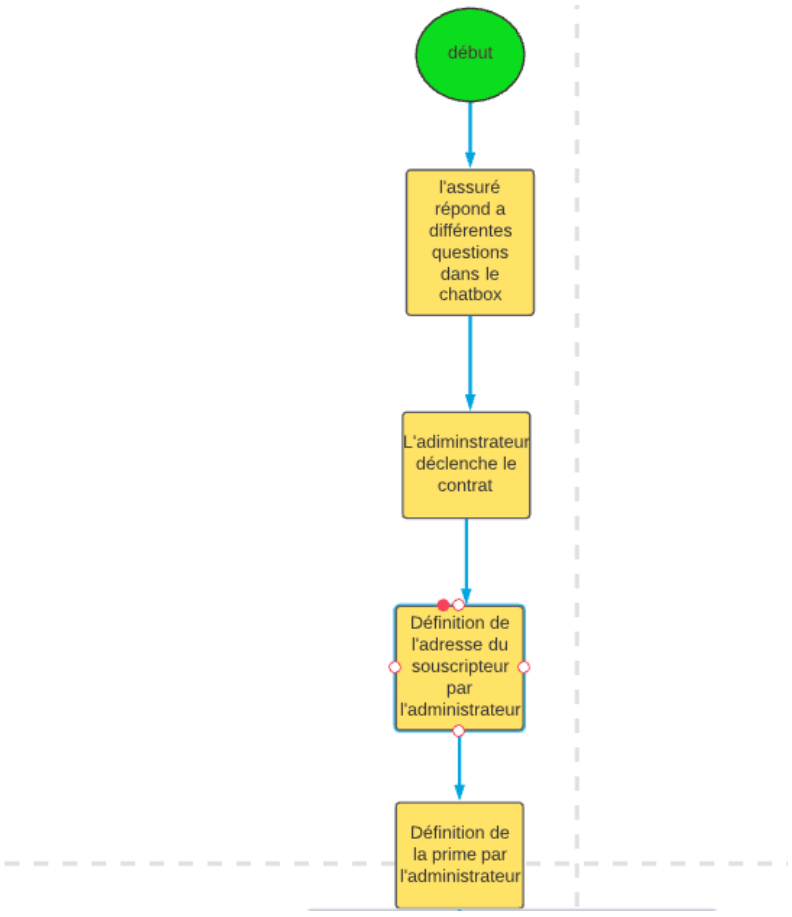


Figure 21:Procédure de mon contrat d'assurance (2/6)

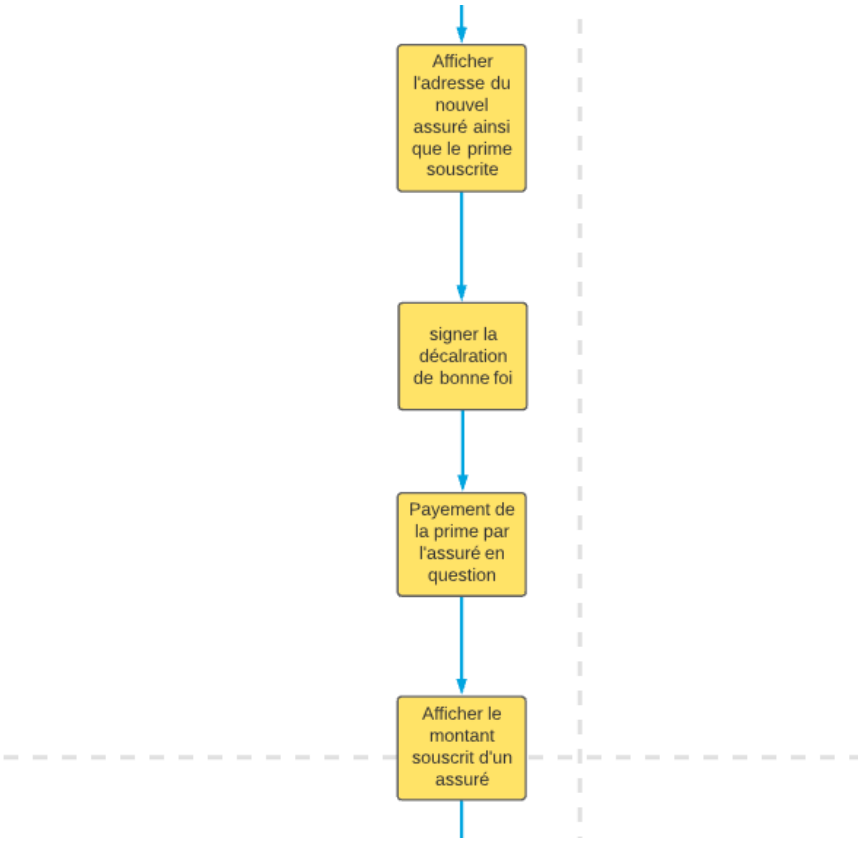


Figure 22: Procédure de mon contrat d'assurance (3/6)

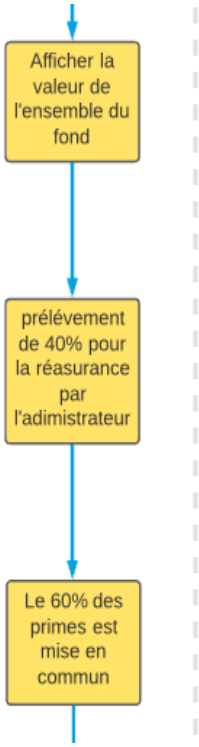


Figure 24: Procédure de mon contrat d'assurance (4/6)

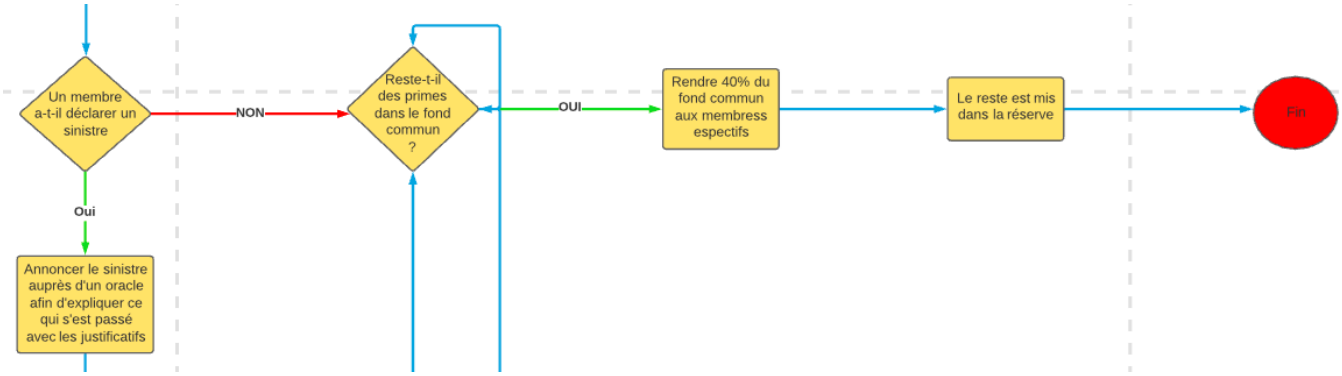


Figure 23: Procédure de mon contrat d'assurance (5/6)

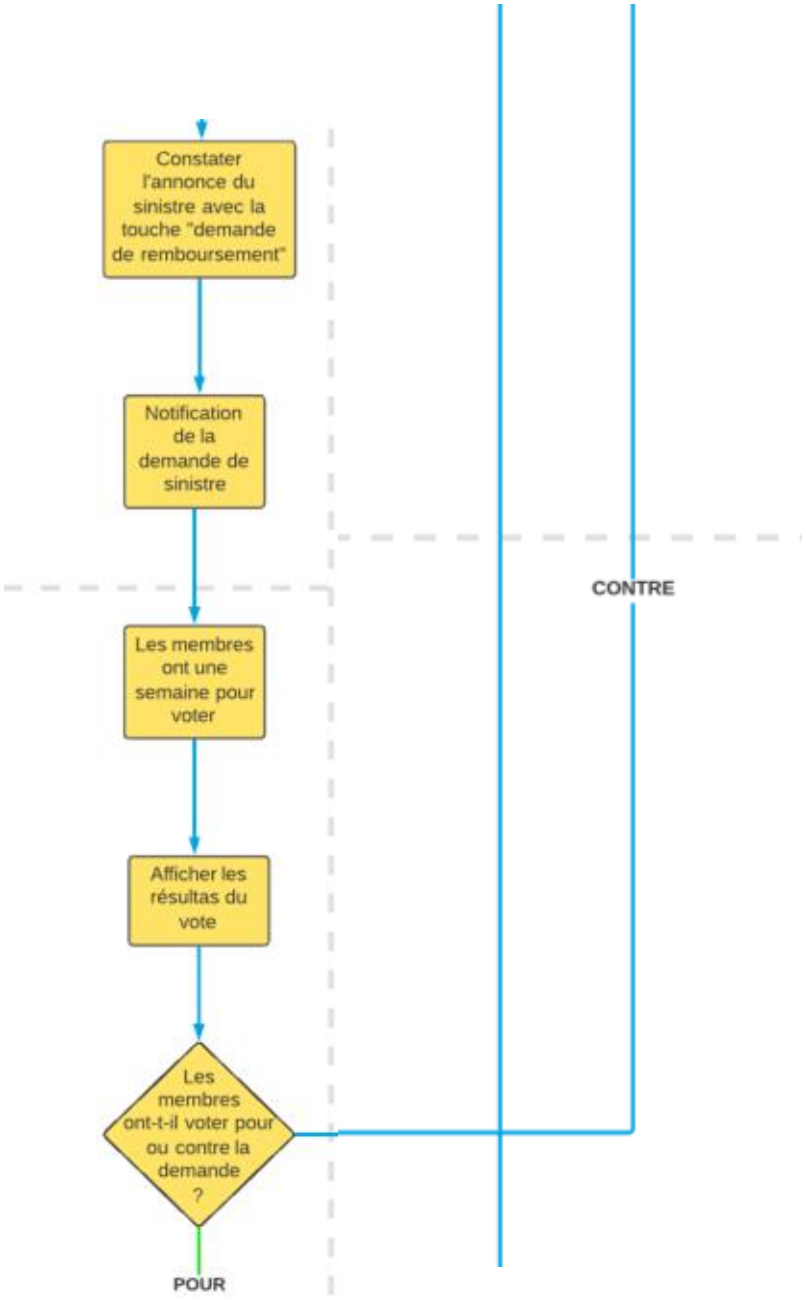
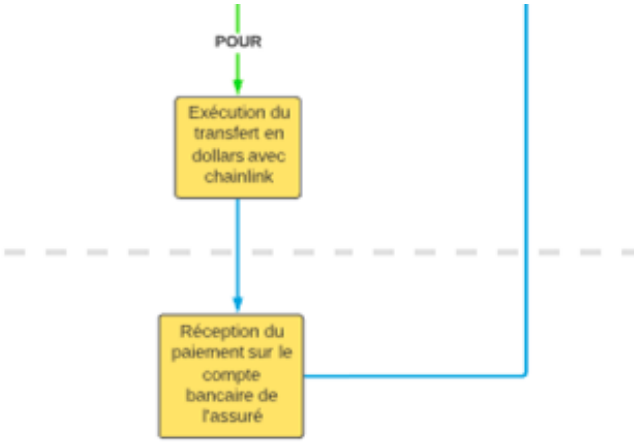


Figure 25: Procédure de mon contrat d'assurance (6/6)



Souscription

Tout comme l'assurance « Lemonade », avant de payer quelconque prime, il est nécessaire d'avoir certaines informations concernant le client. Pour ce faire, le client devra remplir un questionnaire, ce qui permettra de connaître le profil de l'assuré. Dès que cette étape a été faite, la personne qui va déclencher le contrat sera l'assureur, qui aura un rôle d'administrateur. Cet administrateur va indiquer l'adresse de l'assuré qui va souscrire au contrat d'assurance avec la fonction « adresseSousciprtion ». Dès que cela a été fait, il est possible donc de voir qu'elle est l'adresse de l'assuré qui va souscrire ce contrat grâce à la fonction « AdresseNouvelAssure. Ensuite, le montant de la prime va également être définie par l'administrateur, et tout comme l'adresse, il est également possible de voir le montant qui a été défini par la souscription de ce nouvel assuré dans la fonction « definitionPrime ». L'administrateur est l'unique personne ayant le droit d'inscrire l'adresse de l'assuré ainsi que le montant de la prime dans les deux fonctions respectives. De plus, dès lors où le contrat est déployé par l'administrateur, tout le monde peut avoir accès à l'adresse de l'administrateur. Dès que cela a été fait, l'assuré va pouvoir effectuer le transfert du montant de cette prime à travers « chainlink ». Par contre, avant d'effectuer le versement, l'assuré devra signer une déclaration de bonne foi qui promet de rester honnête dans tout type de situation, dès lors qu'il aura versé son argent. Il devra respecter toutes les règles qui seront inscrites dans cette déclaration, notamment en termes de retrait des montants. Si un des points de cette déclaration n'est pas respectée, de lourdes conséquences seront mises en œuvre contre cette personne. Il est nécessaire que tous les membres soient honnêtes dans ce genre de projet où la confiance est primordiale.

Ensuite, tous les assurés pourront voir le montant qui a été payé de la part de chaque assuré en indiquant l'adresse spécifique dans la fonction « voirprime ». Il est également possible de voir le cumul de toutes les primes avec la fonction « cumuldesprimes ». Ce montant ne correspondra pas à la somme totale qui va être utilisée en cas de dédommagement puisque 40% de ce montant sera alloué auprès d'une réassurance dans le cas où la valeur, qu'il y a dans le fonds de cette assurance, c'est-à-dire le 60% de « cumuldesprimes », n'est pas suffisant. Ces deux montants vont se trouver dans la fonction « réassurance » ainsi que « montantdisponible ».

Déclaration de sinistre

Lorsqu'un assuré a été lésé et demande un remboursement, il va devoir cliquer sur « annoncesinistre » afin qu'il demande le remboursement et qu'il envoi tous les justificatifs auprès d'un réseau privé qui se nomme IFPS, les membres pourront télécharger les documents et uniquement les personnes ayant la clé secrète partagée pourront avoir accès à ces documents. Si les membres n'ont pas cette clé de cryptographie, ils ne pourront pas lire ces documents[83]. Ceci est fait afin que tous les autres membres puissent prendre connaissance du cas spécifique. L'annonce du sinistre peut aussi être constatée en appuyant sur la fonction « demande_remboursement ».

Grâce à la même fonction une alerte par mail sera lancée afin que les autres assurés puissent ainsi constater le sinistre et pouvoir voter pour ou contre le remboursement de l'assuré lésé. De plus l'adresse de l'assuré lésé sera inscrite dans « assureLese ». Ils auront donc 7 jours à compter du moment où l'assuré aura cliqué sur « annoncesinistre ». Il devra voter par 0 ou par 1 à la demande. 0 correspond à non et 1 correspond à oui. À tout moment, les membres peuvent suivre l'évolution des votes avec la fonction « voirVotes ». A la fin des 7 jours, tout le monde pourra voir le choix des membres. Dans le cas où un membre ne vote pas pour quelconques raisons, sa non-réponse sera ignorée. A partir de 51% de vote positif pour la demande on considère cette dernière comme acceptée et l'assuré lésé pourra effectuer le transfert en dollars. En revanche, si moins de 50% des membres ont voté positivement à la demande, la demande est bien évidemment refusée mais il lui sera également impossible de retirer quoique ce soit.

83 ELEKS,2018. Secure Document Transfer Built on Top of Blockchain Technologies. *Eleks* [en ligne]. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://labs.eleks.com/2016/10/secure-document-transfer-built-top-blockchain-technologies.html

Fin du contrat

A la fin de l'année s'il reste des primes dans le fonds "cumuldesprimes", il sera versé 60% de ce montant dans la réserve. La réserve sera utilisée en cas de nécessité absolue. Le reste sera rendu aux différents membres proportionnellement aux montant de la prime payée. Ils ne pourront naturellement pas pouvoir retirer un montant supérieur au montant de leurs primes malgré le fait qu'il y ait de l'argent dans le fond commun.

Afin de pouvoir visualiser au sein du smart contract toute la procédure qui a été expliquée. Juste en dessous ainsi qu'à la page suivante, vous trouverez deux captures d'écran du smart contract d'assurance que j'ai mis en place.

Figure 26: mon smart contract d'assurance (1/2)

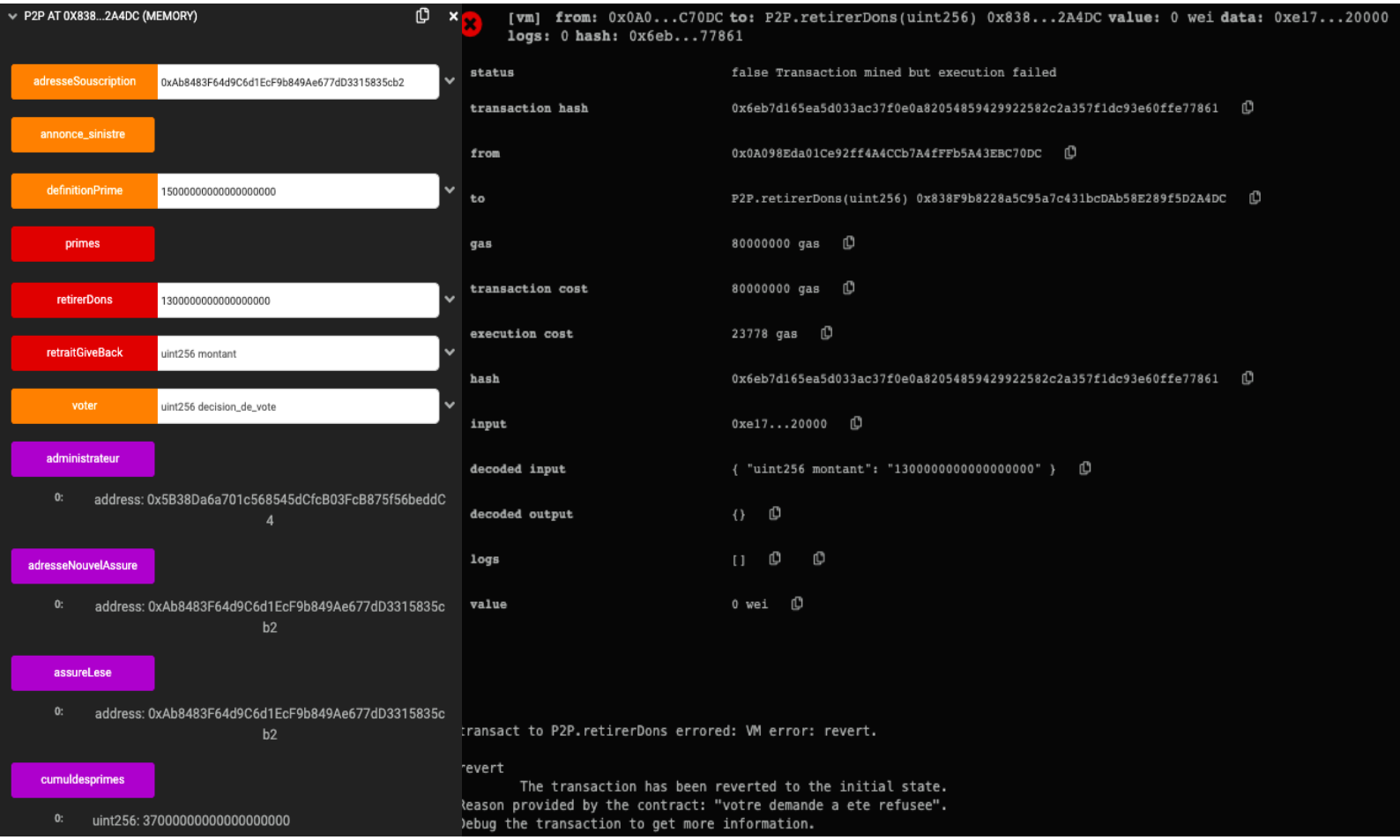
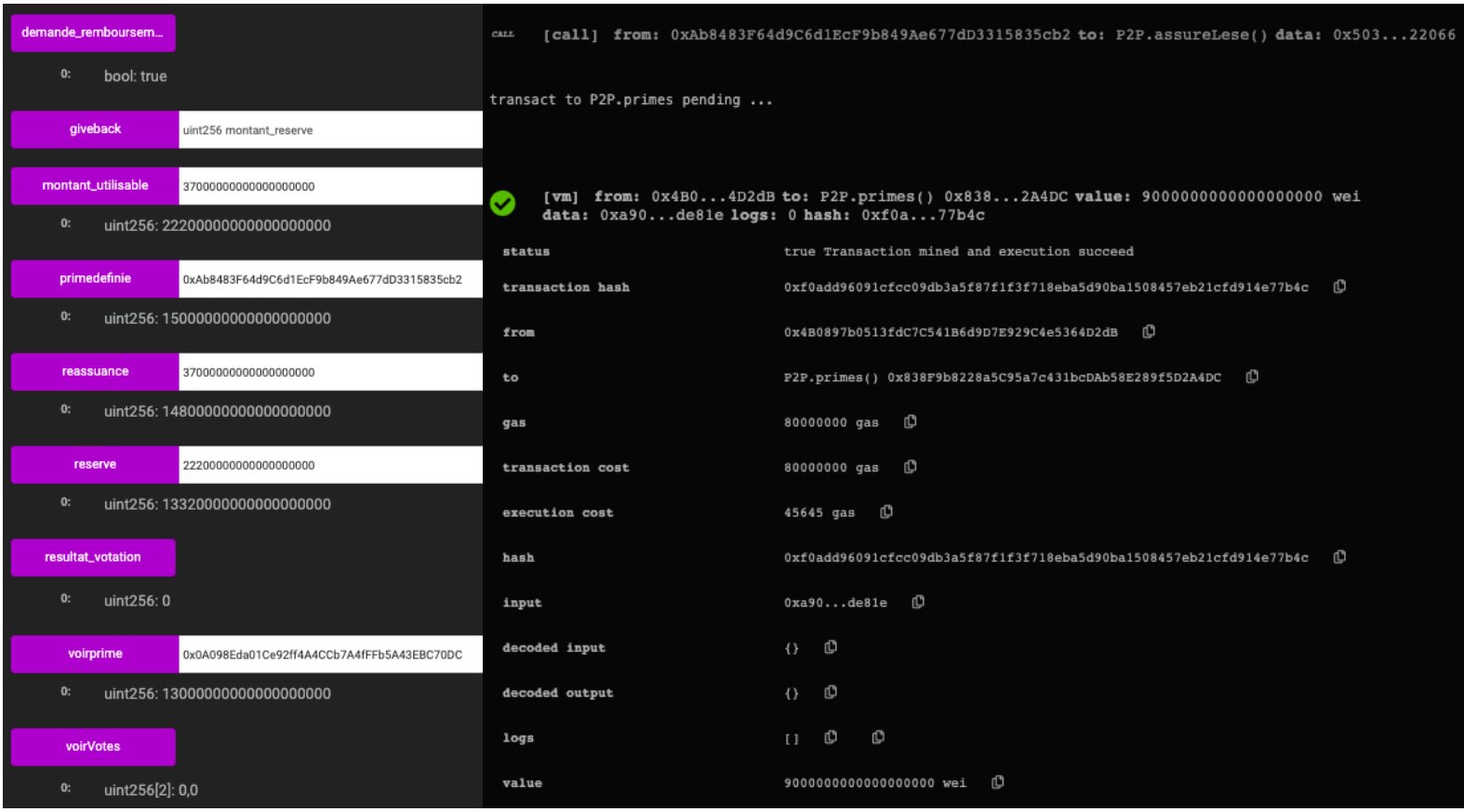


Figure 27: mon smart contract d'assurance (2/2)



Sur la partie de gauche vous trouverez toutes les fonctions et commandes qui ont été décrites plus haut. Sur la partie de droite nous avons la transaction avec quelques informations tel que son état, les valeurs ainsi que les adresses des acteurs de la transaction. De plus, on peut trouver différents messages d'erreurs lorsque par exemple une personne décide de retirer de l'argent alors que sa demande n'a pas encore été votée ou bien qu'elle a tout simplement été refusée.

7.3 Résultats

A présent que nous avons vu ces deux assurances nous pouvons faire une comparaison de ces assurances.

7.3.1 « Lemonade » : Avantages

Notoriété

Nous l'avons vu plus haut, « Lemonade » est une entreprise, qui est cotée en bourse, qui emploie plusieurs centaines de personnes et qui est connue de plus en plus à travers le monde. Son modèle marche, il se développe de plus en plus, non seulement en termes géographique puisqu'ils offrent leurs solutions dans différents pays dans le monde mais également en termes de solutions. Le nombre de solutions en termes d'assurance ne fait que croître. Prochainement ils vont également mettre en place une assurance automobile comme on peut le voir sur leur site internet.[84]

Le temps

Que ce soit lors de la souscription, ou bien de la demande de remboursement, cela prend très peu de temps. En l'espace de 3 minutes, il est possible de souscrire à une police d'assurance. En 10 minutes, on peut faire constater le sinistre. Les clients de « Lemonade » sont très souvent dédommagés sous les 24 heures.[85] Il n'est donc pas du tout contraignant de déclarer un sinistre. Comme le dit le CEO de Lemonade, en l'espace d'une coupure publicitaire il est possible de souscrire à leur assurance. Cela fait gagner un temps très important auprès de leurs clients.[86]

---

84 LEMONADE. *Lemonade* [en ligne]. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://www.lemonade.com

85 GALLO Meredith, 2020. Lemonade review : We tested an insurance company designed for people who hate to talk on the phone. *Chicago Tribune* [en ligne]. 18 mai 2020. [consulté le 25 juin 2021]. Disponible à l'adresse : https://www.chicagotribune.com/consumer-reviews/sns-bestreviews-lemonade-insurance-review-20200518-wdcqysvkgvbzxo2wazk6chdbwe-story.html

86 LEMONADE, 2020. Lemonade CEO Daniel Schreiber explains how Lemonade differs from traditional insurance companies. [enregistrement vidéo] *Youtube* [en ligne]. [Consulté le 10 juillet 2021]. Disponible à l'adresse : https://www.youtube.com/watch?v=4KC5gA3qJdU&t=288s

Le prix

En termes de prix, « Lemonade » offre également des prix extrêmement attractifs. En effet, ayant effectué une demande de prix chez « Lemonade », pour l'assurance habitation, le prix était de 6,72 euros. Ne proposant pas leurs solutions en Suisse, l'unique solution était de la tester pour un bien sur le territoire français. Les paramètres du profil de l'assuré concernant cette police d'assurance ont été les suivants :

- Locataire
- Valeur des objets inférieur à 5'000
- Cohabitation avec un animal de compagnie
- Pas de déclaration de sinistre sous les 3 ans
- Superficie de 68 M^2
- Sans caméra de sécurité ni alarme de sécurité
- Habitant au rez-de-chaussée

Selon le comparateur français « lelynx », l'assurance habitation serait de 158 euros dans la région Auvergne-Rhône-Alpes, ce qui correspond à environ 13 euros par mois.[87]

7.3.2 « Lemonade » : Inconvénients

Informations

L'accès aux différentes informations est limitée. En effet, d'après ce qu'on peut voir dans cette assurance, malgré le fait que la confiance a une place importante dans l'assurance pair-à-pair, étant donné que chaque membre va payer pour dédommager le membre lésé, il y a tout de même un manque de transparence qui pourrait être détecté auprès de cette assurance. En ce qui concerne les données, l'assuré n'a aucun accès aux données et ne sait pas où est-ce que les données sont stockées. Les autres membres ne peuvent même pas voir le sinistre des autres membres.

87 LELYNX. Prix d'assurance habitation. *Lelynx* [en ligne]. [consulté le 4 juillet 2021] Disponible à l'adresse : https://www.lelynx.fr/assurance-habitation/comparaison/pas-cher/prix/

Refuser aucune demande

Le fait de ne refuser aucune demande de remboursement est certainement un avantage auprès de leurs clients puisque quoi qu'il arrive le client va être dédommagé. Cependant, refuser une demande démontre qu'il ne suffit pas que l'on déclare un sinistre pour être dédommagé.

7.3.3 « Mon assurance » : Avantages

En plus des similitudes avec « Lemonade », en termes de vitesse d'exécution, ainsi que de prix, l'assurance P2P avec l'intégration de la blockchain, a d'autres avantages très importants.

Transparence

En ce qui concerne l'assurance pair-à-pair avec la blockchain ainsi que les smarts contracts, rien ne peut être caché puisque la transparence pourrait être définie comme importante dans ce processus. En effet, on peut voir les primes définies de l'administrateur auprès du nouveau membre, de même que le montant de la prime libérée. Les membres ont accès à toutes les informations concernant les primes des autres membres ainsi que tous les documents qui justifient une demande de remboursement. De plus, elle permet de donner le droit de décision aux membres concernant le remboursement ou non d'une demande d'un assuré.

Confiance

Le fait que la transparence est bel et bien présente dans le processus, cela amène une plus grande confiance de la part des membres que cela soit entre eux vu qu'ils ne peuvent rien cacher, mais également la confiance qu'ils ont auprès de l'organisation tout entière.

7.3.4 « Mon assurance » : inconvénient

Bien évidemment cette assurance n'est pas parfaite, puisque comme on l'a dit avec « the DAO », il est tout à fait possible qu'une personne s'y connaissant en programmation, et qu'elle puisse découvrir une faille et l'utiliser à des fins personnelles. En théorie, la personne qui va développer le code va faire en sorte que cette action soit impossible. Malgré tout rien n'est impossible en informatique et dans tout programme il peut y avoir une faille. Le fait de donner accès à toutes ces informations techniques à beaucoup de personnes, cela peut permettre de se faire attaquer plus facilement, que si ces informations sont cachées. Ceci est un parti pris de chaque organisation.

Il existe donc de nombreuses similitudes entre ces deux assurances, malgré le fait qu'elles soient différentes. Si on regarde le processus de manière générale, il est assez

similaire, nous avons une partie souscription, une partie déclaration de sinistre, ainsi qu'une partie remboursement des primes, en fin d'années. Mais en regardant les caractéristiques de l'assurance pair-à-pair, l'aspect de transparence et de confiance qu'amène l'utilisation de la blockchain est trop importante pour l'ignorer. Ces assurances avec la blockchain permettent d'avoir une plus-value plus importante que sans la blockchain, en amenant cette transparence.

8. Recommandation

Après avoir vu les différents points théoriques de la blockchain et de l'assurance pair-à-pair. A travers ce travail, je suggère d'utiliser les smarts contracts afin d'augmenter la confiance et la transparence qui était les deux principaux objectifs de ce travail. On a pu voir que ces deux notions peuvent aller de pair et qu'il pourrait y avoir une certaine relation entre la transparence et la confiance. Cette recommandation a des points positifs mais comme dans toute chose il y a également des points négatifs à souligner quant à la mise en place de cette recommandation.

Avantages de cette solution

Nous avons pu le voir à travers l'exemple que j'ai mis en place, d'un smart contract pour une assurance, que le smart contract permet d'ouvrir cette assurance dans les détails auprès des clients. En effet, nous avons pu voir que cette solution amène une transparence complète auprès des membres qui ont la volonté de faire partie de ce projet. Contrairement à l'assurance pair-à-pair traditionnelle, où la blockchain est absente, et de ce fait les assurés n'ont pas le choix de faire confiance à l'assurance en question, étant donné qu'ils ne voient rien. Ils sont obligés de croire ce que cette assurance leur promet. Ils n'ont donc pas la possibilité de vérifier ce qui est fait.

Avec ces contrats intelligent, ils ont le choix de faire confiance ou non à l'assurance par rapport à des faits qu'ils ont pu voir de leurs propres yeux. Il n'est pas forcément nécessaire de tout regarder dans les moindres détails, notamment le code source qui n'est peut-être pas très compréhensible pour beaucoup de personnes et pas très agréable à lire non plus. Mais déjà le fait de pouvoir vérifier si tel assuré a bien libéré le bon montant, ou bien de voir le cumul de la valeur du fond, ce sont des éléments très important afin de montrer aux membres qu'ils peuvent leur faire confiance et il n'y a donc aucun moyen de tricher. Dans le cas où l'assuré a le moindre doute il pourra partir de cette assurance. Mais sans ce smart contract, on ne laisse pas la possibilité à l'assuré d'avoir des doutes.

Inconvénient de cette solution

Dans la vie rien n'est parfait et tout peut être amélioré. Cette solution n'est pas une exception. Cette solution amène quelques risques à cause des vulnérabilités informatiques qui peuvent être perçues si cela n'a pas été fait correctement. En effet, tout comme le projet « the DAO » il est possible de voir une faille dans le code source et de l'utilisée contre les autres membres notamment lorsqu'il faut retirer une somme d'argent. De plus cette confiance et transparence qui a été traitée plus haut peut être faite uniquement si l'assurance le veut. Tous ce qui a été fait dans mon code était une volonté de ma part de ne rien cacher aux assurés et de tout leur montrer. Mais cela n'est pas obligé avec les smart contracts, le développeur du code peut faire le strict minimum et n'est pas obligé de tout montrer. Si cette solution doit être mise en place il faut absolument tout dévoiler sinon cela ne permettra pas vraiment d'augmenter la confiance.

9. Conclusion

Dans ce travail, nous avons pu voir que la blockchain et les smart contracts peuvent apporter une plus-value importante en la fusionnant avec des projets qui ont des caractéristiques similaires, tel que l'assurance pair-à-pair. La confiance et la transparence qu'apportent cette technologie dans cette assurance peut lui permettre d'améliorer sa crédibilité sur le marché et amener de plus en plus de nouvelles personnes à s'intéresser et à se lancer dans ces projets.

On a pu apercevoir une trajectoire intéressante que pouvait poursuivre cette assurance. En revanche, ce travail n'est pas totalement complet pour définir totalement le potentiel de la fusion, des deux principaux éléments de ce travail. Certains points n'ont pas été évoqués durant ce travail malgré le fait qu'ils ont une certaine importance, pour répondre à cette problématique. Un point que je n'ai pas pu traiter, et qu'il serait intéressant de voir dans les prochains travaux serait la partie financière dans la blockchain avec l'assurance pair-à-pair. Un autre point important serait la réglementation de la blockchain et des assurances. Ces deux points pourront donc être traités dans le cadre d'un travail de master afin de développer les réflexions qui ont été faites dans ce travail.

Durant ce travail, j'ai également mis en avant une compétence dans laquelle je n'ai jamais été trop à l'aise avant cette dernière année à la Haute Ecole de Gestion de Genève dans la filière économie d'entreprise. En effet, la programmation n'est pas une discipline dans laquelle on exige d'avoir de grandes compétences et que ces compétences soient mises en pratique de la manière dont je l'ai mis en avant dans ce travail. Ce travail m'a permis de développer mes compétences en programmation ainsi que de surpasser une limite personnelle qui me permet d'aller de l'avant avec cette dernière et non pas contre.

Étant donné l'importance de la programmation dans la période au sein de laquelle nous vivons, ce travail m'a offert la possibilité de m'apporter une plus-value pour clore mon cursus à la Haute École de Gestion de Genève.

10. Bibliographie

ABDIKERIMOVA, Samal et FENG, Runhuan, 2019. ID 3505646 : *Peer-to-Peer Multi-Risk Insurance and Mutual Aid* [en ligne]. SSRN Scholarly Paper. Rochester, NY. Social Science Research Network. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://papers.ssrn.com/abstract=3505646.

ALLEGRET, Jean-Pierre et CORNAND, Camille, 2013. Une analyse informationnelle de la crise financière récente. In : *Revue francaise d'economie*. 2013. Vol. Volume XXVIII, n° 3, pp. 213-264.

ARTIFICIAL LAWYER, 2018. ChainLink: Solving the Smart Contract Fiat Money Problem – Artificial Lawyer. In : [en ligne]. 3 septembre 2018. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.artificiallawyer.com/2018/09/03/chainlink-solving-the-smart-contract-fiat-money-problem/.

ALLIANZ Les assurances obligatoires et facultatives en Suisse | Allianz. In : *allianz.ch* [en ligne]. [Consulté le 27 juin 2021 n]. Disponible à l'adresse : https://www.allianz.ch/fr/clients-prives/guide/vie-quotidienne/assurances-obligatoires-suisse.html.

BAI, Chong, 2019. State-of-the-Art and Future Trends of Blockchain Based on DAG Structure. In : DUAN, Zhenhua, LIU, Shaoying, TIAN, Cong et NAGOYA, Fumiko (éd.), *Structured Object-Oriented Formal Language and Method*. Cham : Springer International Publishing. 2019. pp. 183-196. ISBN 978-3-030-13651-2.

BCV, [sans date]. Pourquoi me demande-t-on si je suis américain quand je veux ouvrir un compte bancaire? In : [en ligne]. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://www.bcv.ch/pointsforts/Votre-argent/2017/Pourquoi-me-demande-t-on-si-je-suis-americain-quand-je-veux-ouvrir-un-compte-bancaire.

BITCOIN SUISSE, 2020. What is Chainlink? | Research & Fundamentals | Bitcoin Suisse. In : [en ligne]. 5 octobre 2020. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.bitcoinsuisse.com/fundamentals/what-is-chainlink.

BIT2ME, Académie, 2018. Qu'est-ce qu'un NONCE. In : *Bit2Me Academy* [en ligne]. 9 juillet 2018. [Consulté le 15 juillet 2021]. Disponible à l'adresse : https://academy.bit2me.com/fr/qu%27est-ce-que-le-nonce/.

BRAUN, Alexander et SCHREIBER, Florian, 2017. 62 : *The Current InsurTech Landscape: Business Models and Disruptive Potential* [en ligne]. Research Report. S.l. I.VW HSG Schriftenreihe. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.econstor.eu/handle/10419/226646.

CASH, Michael et BASSIOUNI, Mostafa, 2018. Two-Tier Permission-ed and Permission-Less Blockchain for Secure Data Sharing. In : *2018 IEEE International Conference on Smart Cloud (SmartCloud)*. S.l. : s.n. septembre 2018. pp. 138-144.

CHANDEZE,Aurélie, 2019. La blockchain au service de la transparence. In : *LeMondeInformatique* [en ligne]. [Consulté le 11 juillet 2021 i]. Disponible à l'adresse : https://www.lemondeinformatique.fr/les-dossiers/lire-la-blockchain au-service-de-la transparence -1026.html.

CHANUT, Guillaume, 2019. Qu'est ce que la machine virtuelle Ethereum (EVM) ? - *Cryptoast*. In : [en ligne]. 25 avril 2019. [Consulté le 26 juin 2021]. Disponible à l'adresse : https://cryptoast.fr/quest-ce-que-la-machine-virtuelle-ethereum/.

COMPARIS. Comparer et économiser – comparis.ch. In : [en ligne]. [Consulté le 27 juin 2021 d]. Disponible à l'adresse : https://fr.comparis.ch/.

CRUNCHBASE. Lemonade - Funding, Financials, Valuation & Investors. In : *Crunchbase* [en ligne]. [Consulté le 27 juin 2021 k]. Disponible à l'adresse : https://www.crunchbase.com/organization/lemonade/company_financials.

DAVTIAN, Willy, 2018. Blockchain et assurance : espérance démesurée ou nouvelle ère ? In : [en ligne]. 15 mai 2018. [Consulté le 3 juillet 2021]. Disponible à l'adresse : http://www.revue-banque.fr/banque-detail-assurance/article/blockchain-assurance-esperance-demesuree-nouvelle.

DEVENTER Cate. 2021. Lemonade Insurance | *Bankrate*. In : [en ligne]. 12 mai 2021. [Consulté le 27 juin 2021 l]. Disponible à l'adresse : https://www.bankrate.com/insurance/homeowners-insurance/lemonade-insurance-review/.

ELEKS. 2016. Secure Document Transfer Built on Top of Blockchain Technologies. In : *Eleks Labs* [en ligne]. 7 octobre 2016. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://labs.eleks.com/2016/10/secure-document-transfer-built-top-blockchain-technologies.html.

ELOI, Laurent,2012. *Économie de la confiance* [en ligne]. Paris : La Découverte, Paris, 2012, 128 [consulté le 18 juin 2021]. Disponible à l'adresse :

https://cdn.reseau-canope.fr/archivage/valid/N-2305-11466.pdf

ERNST YOUNG, 2019. EY Global FinTech Adoption Index 2019. In : [en ligne]. 25 avril 2019. [Consulté le 26 juin 2021]. Disponible à l'adresse : https://www.ey.com/en_gl/ey-global-fintech-adoption-index.

FARVAQUE, Étienne et REFAIT-ALEXANDRE, Catherine, 2016. Les exigences de transparence des accords de Bâle : aubaine ou fardeau pour les pays en développement ? In : *Mondes en developpement*. 5 avril 2016. Vol. n° 173, n° 1, pp. 131-147.

GALLO, Meredith, 2020. Lemonade review: We tested an insurance company designed for people who hate to talk on the phone - Chicago Tribune. In : [en ligne]. 18 mai 2020. [Consulté le 28 juin 2021]. Disponible à l'adresse : https://www.chicagotribune.com/consumer-reviews/sns-bestreviews-lemonade-insurance-review-20200518-wdcqysvkgvbzxo2wazk6chdbwe-story.html.

FINMA 2019. Rapport 2019 sur le marché de l'assurance. Autorité fédérale de surveillance des marchés financiers FINMA.[en ligne] [consulté le 1 mai 2021]. Disponible à l'adresse :https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/versicherungsbericht/20200910-versicherungsmarktbericht-2019.pdf?la=fr

GRIMAUD Pierre,2021. Oracles, In : *Ethereum* [en ligne]. 27 avril 2021 [consulté le 27 juin 2021]. Disponible à l'adresse : https://ethereum.org/en/developers/docs/oracles/

HEWLETT PACKARD. Qu'est-ce que le machine learning ? Définitions | HPE Suisse. In : [en ligne]. [Consulté le 27 juin 2021 s]. Disponible à l'adresse : https://www.hpe.com/ch/fr/what-is/machine-learning.html.

HUXTABLE, Johny, 2018. Analysis of Chainlink — The Decentralised Oracle Network | by Jonny Huxtable | Medium. In : [en ligne]. semptembre 2018. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://medium.com/@jonnyhuxtable/analysis-of-chainlink-the-decentralised-oracle-network-7c69bee2345f.

INVESTERESTS,2019 . Ether Explained – Chapter 4: The Decentralized Autonomous Organisaion (DAO). In : [en ligne]. 29 juillet 2019. [Consulté le 27 juin 2021 f]. Disponible à l'adresse : https://investerest.vontobel.com/en-dk/articles/13374/ether-explained--chapter-4-the-decentralized-autonomous-organisaion-dao/.

JACQUES-OLIVIER-BUSI, [sans date]. Prix Assurance Habitation : Devis Gratuits ⇒ LeLynx.fr. In : *LeLynx.fr* [en ligne]. [Consulté le 30 juin 2021]. Disponible à l'adresse : https://www.lelynx.fr/assurance-habitation/comparaison/pas-cher/prix/.

KLENTON Bill, SCOTT Gordon 2021. Depository trust company (DTC) *Investopedia*.[en ligne]. 29 mai 2021. [consulté le 18 juin 2021] Disponible à l'adresse : https://www.investopedia.com/terms/d/dtc.asp

LAROUSSE, Éditions, [sans date]. Définitions : transparence - Dictionnaire de français Larousse. In : [en ligne]. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://www.larousse.fr/dictionnaires/francais/transparence/79194.

LEMONADE., [sans date]. Insurance Built For the 21st Century | Lemonade. In : [en ligne]. [Consulté le 27 juin 2021 h]. Disponible à l'adresse : https://www.lemonade.com/.

LEMONADE. Sign Up for Lemonade Renters & Home Insurance | Lemonade. In : [en ligne]. [Consulté le 27 juin 2021 t]. Disponible à l'adresse : https://www.lemonade.com/onboarding/1.

LESAFFRE Clément,2021. [sans date]. Traçabilité alimentaire : grâce à la blockchain, la transparence s'invite sur les emballages. In : [en ligne]. 02 mai 2021. [Consulté le 11 juillet 2021 w]. Disponible à l'adresse : https://www.europe1.fr/economie/tracabilite-alimentaire-grace-a-la-blockchain-la-transparence-sinvite-sur-les-emballages-4042081.

LEMONADE, [sans date]. *Lemonade CEO Daniel Schreiber explains how Lemonade differs from traditional insurance companies* [en ligne]. [Consulté le 11 juillet 2021]. Disponible à l'adresse : https://www.youtube.com/watch?v=4KC5gA3qJdU&t=288s.

LEMONADE Team, 2020. *L’app Lemonade | Assurance Habitation pour locataires boostée à l’Intelligence Artificielle* [en ligne]. 23 novembre 2020. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://vimeo.com/482550657.

MALANOV, Alexey, 2017. Le minage des bitcoins et la disparation des cartes graphiques. | Blog officiel de Kaspersky. In : [en ligne]. 24 juillet 2017. [Consulté le 26 juin 2021]. Disponible à l'adresse : https://www.kaspersky.fr/blog/mining-easy-explanation/9305/.

MARRAST, Philippe, 2018. Blockchain : Éléments d'explication et de vulgarisation, Pourquoi s'intéresser à la blockchain aujourd'hui ? In : *Blockchain et Santé : Perspectives d'applications et enjeux juridiques (Séminaire IFERISS)* [en ligne]. Toulouse, France : IFERISS. octobre 2018. [Consulté le 26 juin 2021]. Disponible à l'adresse : https://hal.archives-ouvertes.fr/hal-01973507.

MINISTERE DES ECONOIES DES FINANCES ET DE LA RELANCE. Georges Akerlof. In : [en ligne]. [Consulté le 26 juin 2021 g]. Disponible à l'adresse : https://www.economie.gouv.fr/facileco/georges-akerlof.

NAUDIN Julie, 2019. Finance MagLe jour où… je suis entrée dans les coulisses du métier de mineur de cryptos. In : *Finance Mag* [en ligne]. 16 janvier 2019. [Consulté le 15 juillet 2021]. Disponible à l'adresse : https://finance-mag.com/minage-cryptomonnaies-metier-julie-naudin/.

OLIVA, Gustavo A., HASSAN, Ahmed E. et JIANG, Zhen Ming, 2020. An exploratory study of smart contracts in the Ethereum blockchain platform. In : *Empirical Software Engineering*. mai 2020. Vol. 25, n° 3, pp. 1864-1904. [consulté le 25 mars 2021]. Disponible à l'adresse : DOI 10.1007/s10664-019-09796-5.

OVERHOLT Maggie, 2019. How Lemonade Insurance Works. In : *Reviews.com* [en ligne]. 26 juillet 2019. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.reviews.com/insurance/homeowners/how-lemonade-insurance-works/.

PUSCHMANN, Thomas, 2017. Fintech. In : *Business & Information Systems Engineering*. février 2017. Vol. 59, n° 1, pp. 69-76. DOI 10.1007/s12599-017-0464-6.

SIEGEL david,2016. The DAO Attack: Understanding What Happened – CoinDesk. In : [en ligne]. 25 juin 2016. [Consulté le 27 juin 2021]. Disponible à l'adresse : https://www.coindesk.com/understanding-dao-hack-journalists.

SAPRA, Riya et DHALIWAL, Parneeta, 2021. Blockchain: The Perspective Future of Technology. In : *International Journal of Healthcare Information Systems and Informatics (IJHISI)*. 2021. Vol. 16, n° 2, pp. 1-20. DOI 10.4018/IJHISI.20210401.oa1.

SAWAKINOME. Différence entre le code source et le bytecode / La programmation | La différence entre des objets et des termes similaires. In : [en ligne]. [Consulté le 26 juin 2021 e]. Disponible à l'adresse : https://fr.sawakinome.com/articles/programming/difference-between-source-code-and-bytecode.html.

SIAPARTNERS. L'assurance « peer-to-peer » : vers un essor de l'assurance communautaire ? In : [en ligne]. [Consulté le 3 juillet 2021 j]. Disponible à l'adresse : https://www.sia-partners.com/fr/actualites-et-publications/de-nos-experts/lassurance-peer-peer-vers-un-essor-de-lassurance

SIMPLESURANCE. Que faisons-nous | Tout sur nous chez simplesurance. In : *simplesurance* [en ligne]. [Consulté le 27 juin 2021 r]. Disponible à l'adresse : https://www.simplesurance.com/fr/que-faisons-nous/.

SWISSRE, [sans date]. *150Y_Markt_Broschuere_Schweiz_FR_Inhalt.pdf* [en ligne]. S.l. : s.n. [Consulté le 26 juin 2021 a]. Disponible à l'adresse : https://www.swissre.com/dam/jcr:c4313ff1-60fc-43af-b33e-a0dbd8819189/150Y_Markt_Broschuere_Schweiz_FR_Inhalt.pdf.

SYNERGIX. ONG : Comment améliorer la confiance des donateurs grâce à la transparence et aux technologies ? - Synergix News. In : [en ligne]. [Consulté le 26 juin 2021 p]. Disponible à l'adresse : http://www.synergix.ch/fr/info/news/ong-ameliorer-confiance-donateurs-transparence-technologie.

SZALACHOWSKI, Pawel, REIJSBERGEN, Daniel, HOMOLIAK, Ivan et SUN, Siwei, [sans date]. StrongChain: Transparent and Collaborative Proof-of-Work Consensus. In : . pp. 19. [consulté le]25 mars 2021 Disponible à l'adresse : https://www.usenix.org/system/files/sec19-szalachowski.pdf

TABORA, Vincent, 2019. A Decomposition Of The Bitcoin Block Header. In : *DataDrivenInvestor* [en ligne]. 21 novembre 2019. [Consulté le 15 juillet 2021]. Disponible à l'adresse : https://www.datadriveninvestor.com/2019/11/21/a-decomposition-of-the-bitcoin-block-header/.

TASATANATTAKOOL, Pinyaphat et TECHAPANUPREEDA, Chian, 2018. Blockchain: Challenges and applications. In : *2018 International Conference on Information Networking (ICOIN)*. S.l. : s.n. janvier 2018. pp. 473-475.

TBS CERTIFICATS. Tout sur les algorithmes de hachage SHA1, SHA2 et le SHA256. In : [en ligne]. [Consulté le 26 juin 2021 v]. Disponible à l'adresse : https://www.tbs-certificats.com/FAQ/fr/sha256.html.

TECHNOLOGY AND OPERATIONS MANAGEMENT, 2018. Lemonade reinvents the insurance industry with machine learning. In : *Technology and Operations Management* [en ligne]. 13 novembre 2018[Consulté le 27 juin 2021 m]. Disponible à l'adresse :

https://digital.hbs.edu/platform-rctom/submission/lemonade-reinvents-the-insurance-industry-with-machine-learning/.

ZHOU, Qiheng, HUANG, Huawei, ZHENG, Zibin et BIAN, Jing, 2020. Solutions to Scalability of Blockchain: A Survey. In : *IEEE Access*. 2020. Vol. 8, pp. 16440-16455. DOI [Consulté le 26 juin 2021] Disponible à l'adresse : 10.1109/ACCESS.2020.2967218.

ZHOU Qiheng, HUANG Huawei, ZHENG Zibin, BIAN Jing, 2020., [sans date]. Solutions to Scalability of Blockchain: A Survey | IEEE Journals & Magazine | IEEE Xplore. In : [en ligne].. Disponible à l'adresse : https://ieeexplore.ieee.org/abstract/document/8962150.

11. Annexes

- **Annexe 1 : Code source du smart-contract d'assurance**

```
pragma solidity ^0.5.11;

contract P2P {
    address payable client;
    address public administrateur;
    address public adresseNouvelAssure;
    address public assureLese;
    bool montantPrime;
    bool sinistre;
    bool vote_remboursement;
    int remboursement;
    mapping (address=>uint) prime;
    mapping (address=>bool) vote;
    uint debut;
    uint montantDeLaPrime;
    uint [2] votes;
    uint resultat;


    constructor () public  {
        administrateur=msg.sender;
        debut = block.timestamp;
    }

    modifier aDejaVote () {
        require(!vote[msg.sender],"vous avez deja vote");
        _;
    }

    modifier demande_accepte ( uint ) {
        require (resultat >7, "le remboursement est accepte");
        _;
    }

    modifier demandeRefusee () {
        require (votes[1]>=7,"votre demande a ete refusee");
        _;
    }

    modifier impossibleDeRetirer(uint montant) {
      require (prime[msg.sender]>=montant,"il ne peut pas retirer");
        _;
    }
```

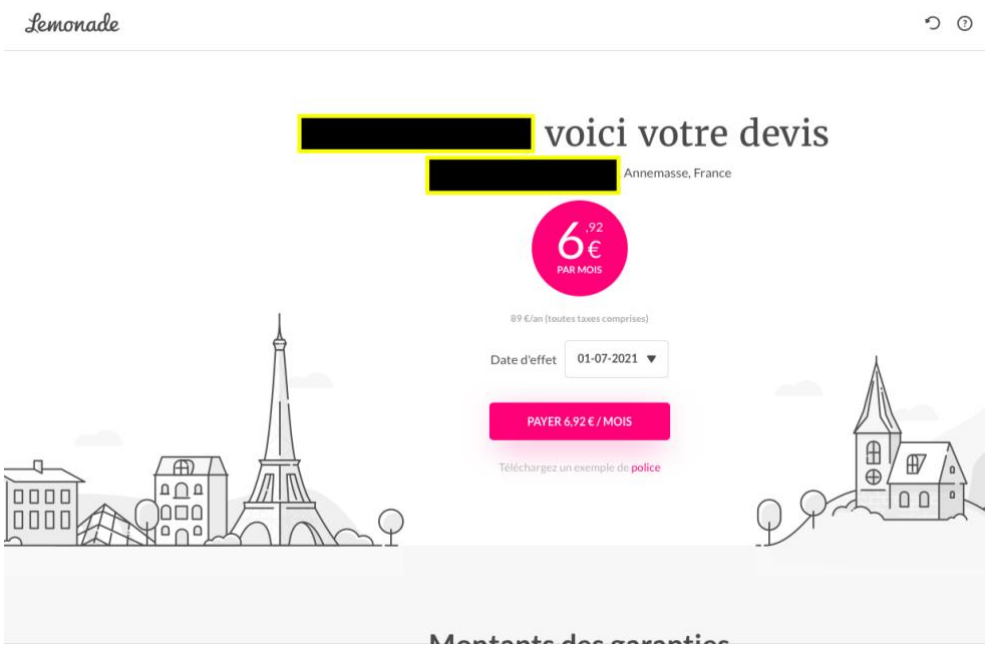
```
    modifier interditAdministrateur () {
        require (administrateur!=msg.sender,"l'administrateur ne peut pas executer cette fonction");
        _;
    }

    modifier onlyadministrateur () {
        require (administrateur==msg.sender, "seulement l'administrateur peut definir la prime");
        _;
    }

     modifier propositionValide (uint laProposition) {
        require (laProposition>=0 && laProposition<3);
        _;
    }

    modifier temps_ecoule () {
        require (block.timestamp-debut<=604800, "le temps valable de 7 jours pour voter est ecoule");
        _;
    }

    modifier temps_ecoule2() {
        require(block.timestamp-debut>=604800, "Vous pouvez encore voter");
        _;
    }

    modifier versement_reserve () {
        require (block.timestamp-debut>=31536000, "Le reste du montant_utilisable peut etre transfere a la reserve chaque annee");
        _;
    }


    //l'administrateur défini l'adressse qui va payer la prime correspondant à la fonction definitionPrime
    function adresseSouscription (address uneAdresse) public onlyadministrateur   {
        adresseNouvelAssure=uneAdresse;
    }

    //annonce du sinistre afin de faire une demande de remboursement
    function annonce_sinistre () public interditAdministrateur{
        sinistre=true;
        assureLese=msg.sender;
    }
```

```
    modifier aDejaVote () {
        require(!vote[msg.sender],"vous avez deja vote");
        _;
    }

    modifier propositionValide (uint laProposition) {
        require (laProposition>=0 && laProposition<3);
        _;
    }

    modifier demande_accepte ( uint ) {
        require (resultat >7, "le remboursement est accepte");
        _;
    }

    modifier versement_reserve () {
        require (block.timestamp-debut>=30, "Le reste du montant_utilisable peut etre transfere a la reserve chaque annee"); //31536000
        _;
    }

    modifier impossibleDeRetirer() {
      require (prime[msg.sender]<=prime[client],"il ne peut pas retirer");
        _;
    }

    //paiement de la prime
    function primes () public payable interditAdministrateur {
        prime[msg.sender]+=msg.value;
    }

    //annonce du sinistre afin de faire une demande de remboursement
    function annonce_sinistre () public interditAdministrateur{
        sinistre=true;
        assureLese=msg.sender;
    }

     function demande_remboursement () public view  returns (bool) {
        return sinistre;
    }
     //permet de voter pour ou contre la demande de remboursement de l'assure lese
     function voter (uint decision_de_vote) public propositionValide(decision_de_vote)   temps_ecoule aDejaVote { //aDejaVote
        votes[decision_de_vote] =  votes[decision_de_vote] + 1;
    }
```

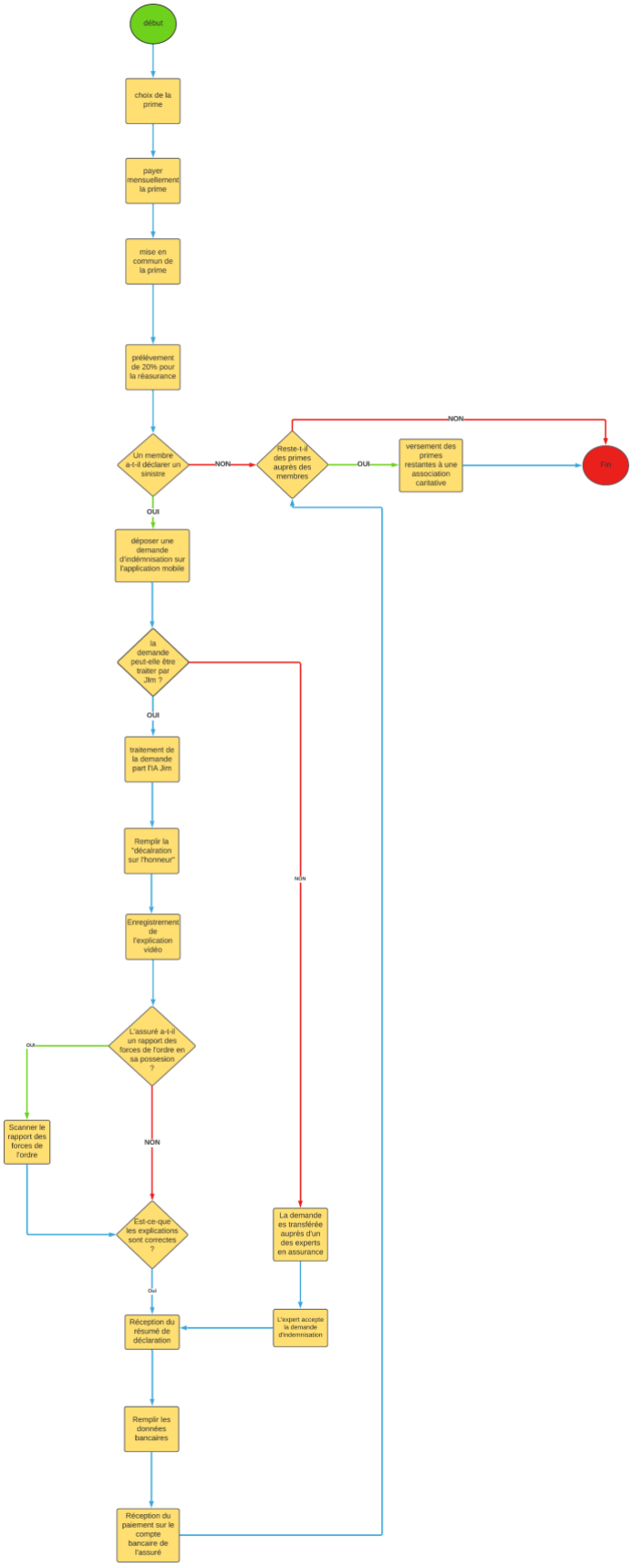
```
    //montant allant auprès d'une réassurance dans le cas où le montant_utilisable est insuffisant
    function reassuance (uint montant_cumuldesprimes) public view onlyadministrateur returns (uint256) {
        return montant_cumuldesprimes *40/100;
    }

    //affiche le montant attribuer à la réserve en fin d'annéee s'il existe de l'argent dans le fond commun
    function reserve (uint montant_reserve) public view versement_reserve returns (uint) {
        if (montant_reserve >0) {
            return montant_reserve*60/100;
        }else {
            return 0;
        }
    }

    //affiche le resultat de votation
    function resultat_votation () public view temps_ecoule2 returns (uint) {
      if (votes[1]>7) return 1;
      if (votes[1]<=7) return 0;
    }

    //permet de retirer les dons si la demande a été accetpée
   function retirerDons(uint montant) public payable demandeRefusee   {
     prime[msg.sender]-=montant;
      msg.sender.transfer(montant);
    }
```

```
    //permet de retirer le montant de la fonction giveback
    function retraitGiveBack (uint montant) public payable impossibleDeRetirer (montant){
        prime[msg.sender]-=montant*10/100;
        msg.sender.transfer(montant*10/100);
        }

     //permet de voir la prime d'un assuré spécifique
    function voirprime (address assure) public view returns(uint) {
        return prime [assure];
    }

    //permet de  voir le nombre de voix pour et le nombre de voix contre la demande de remboursement
    function voirVotes () public view returns (uint [2] memory) {
        return votes;
    }

     //permet de voter pour ou contre la demande de remboursement de l'assure lese
     function voter (uint decision_de_vote) public propositionValide(decision_de_vote)   temps_ecoule aDejaVote {
        votes[decision_de_vote] =  votes[decision_de_vote] + 1;
        vote[msg.sender]=true;
    }
}
```

Annexe 2 : prime d'assurance « lemonade »



Annexe 3 : Processus « Lemonade » en entier


début
choix de la prime
payer mensuellement la prime
mise en commun de la prime
prélèvement de 20% pour la réasurance
Un membre a-t-il déclarer un sinistre
NON
Reste-t-il des primes auprès des membres
NON
OUI
versement des primes restantes à une association caritative
Fin
OUI
déposer une demande d'indémnisation sur l'application mobile
la demande peut-elle être traiter par Jim ?
NON
OUI
traitement de la demande part l'IA Jim
Remplir la "décalration sur l'honneur"
Enregistrement de l'explication vidéo
L'assuré a-t-il un rapport des forces de l'ordre en sa possesion ?
OUI
Scanner le rapport des forces de l'ordre
NON
Est-ce-que les explications sont correctes ?
La demande es transférée auprès d'un des experts en assurance
Oui
Réception du résumé de déclaration
L'expert accepte la demande d'indemnisation
Remplir les données bancaires
Réception du paiement sur le compte bancaire de l'assuré

Annexe 4 : Processus « mon assurance » pair-à-pair en entier