Livre blanc

COMPRENDRE LA BLOCKCHAIN
A TRAVERS L'ETUDE D'UN CAS D'USAGE :

LE COVOITURAGE

« BLOCKCAR »

Elise GUILHAUDIS
Avocate
Fondatrice et Présidente de NUMETIK AVOCATS

Master 2 – Droit du Multimédia et des Systèmes d'Information
DEA – Histoire du Droit, Droit et Droit de l'homme
Maîtrise de Droit des Affaires

Mis à jour le 10 octobre 2018

TABLE DES MATIERES

COMPRENDRE LA BLOCKCHAIN
A TRAVERS L'ETUDE D'UN CAS D'USAGE : LE COVOITURAGE

« BLOCKCAR »

Comprendre la blockchain et les enjeux juridiques associés grâce à un exercice pratique est l'objectif de cette étude, qui se veut, certes juridique, mais avant tout pragmatique. Avant d'aborder le droit, il faut essayer d'appréhender la technologie en elle-même et identifier le type de blockchain le plus adapté au cas étudié.
Nous ferons ensuite un tour d'horizon des principales questions juridiques pouvant se poser. La présente étude se veut synthétique (donc non exhaustive) ; elle tente d'appréhender la blockchain dans sa globalité.

Nous envisagerons un exemple simple et concret : **le covoiturage**, dont le service est aujourd'hui assuré par des plateformes web d'intermédiation – et tenterons de voir ce que la technologie blockchain pourrait changer, apporter de mieux. La blockchain pourrait-elle, comme l'affirment certains, bouleverser le fonctionnement d'un service comme celui du covoiturage ?

Pour comprendre la blockchain, technologie du futur, commençons par nous souvenir du passé : rappelons-nous les fondements du droit (droit naturel/droit positif), la théorie du contrat social de Thomas Hobbes. Dans « *Le Léviathan* » : l'homme, à l'état primitif, est un homme sauvage, de la "*guerre de tous contre tous*", dominé par la bestialité. Pour survivre, il n'aura pas d'autre choix que de faire appel à un **tiers de confiance** (le Leviathan). Il lui donnera sa liberté et en échange, le Leviathan assurera sa protection dans un environnement où règnent l'insécurité et le chaos.
La théorie du contrat social, est la théorie de la confiance que des hommes doivent mettre dans un système, une société, un état, pour survivre malgré l'insécurité naturelle.

Mais ce contrat social peut-il aujourd'hui résister dans un monde sans frontière, et en particulier dans le cyberespace ? Comment maintenir la confiance des hommes dans des services, des activités qui sont bouleversées par la révolution numérique et sont la cible de cyberattaques de plus en plus nombreuses[1] ? Rebecca McKinnon, dans « *Consent of the Networked: The Worldwide Struggle for Internet Freedom* » explique que nous vivons actuellement dans l'âge hobbesien du cyberespace, un nouvel état de nature antérieur à tout contrat social définissant un cadre juridique capable de garantir les droits et devoirs des citoyens du Net (les « netizens »).
La révolution numérique aurait à ce point bouleversé l'équilibre des choses que le contrat social de Thomas Hobbes serait selon certains en voie de disparaître. L'homme revenu à l'état de nature serait à la recherche d'une nouvelle forme de confiance. Mais qui, à l'échelle de la planète, pourrait assurer cette confiance, et comment ?

Selon certains, la technologie blockchain serait capable de gérer, de façon autonome, la défiance qui existe naturellement entre les hommes. La blockchain serait à même de remplacer certains tiers de confiance traditionnels (tels que les banques, les notaires, des services de l'Etat) mais aussi, de « disrupter » (de faire disparaître) des plateformes web de mise en relation.
Nombreux sont les acteurs de la finance et de l'économie qui s'intéressent de très près à cette technologie. Les potentialités de la blockchain seraient énormes[2]. Les projets blockchain se multiplient à travers la planète et les levées de fonds en capital-risque atteignent des sommes vertigineuses[3].

[1] Vers un contrat social du cyberespace ? : https://www.wethenet.eu/2012/09/vers-un-contrat-social-pour-le-cyberespace/
[2] Article du 27 juin 2016 du Raconteur : « https://www.raconteur.net/business/the-future-of-blockchain-in-8-charts »
[3] On peut ici se référer à deux articles : « L'adoption massive de la blockchain est prévue pour 2025 » du site l'Usine Digitale du 27 juin 2016 : http://www.usine-digitale.fr/article/l-adoption-massive-de-la-blockchain-est-prevue-pour-2025.N399357 ainsi que l'article

Révolution ou pas, cette technologie, particulièrement complexe à appréhender, semble en tous les cas remettre en cause certains paradigmes.
Elle pose de nombreuses questions, tant au plan philosophique, éthique, politique, que juridique. Elle interroge au fond sur la place de l'homme et celle de la technologie dans la cité de demain.

Pourquoi le covoiturage ?
Etudier la blockchain au travers de cet exemple n'a pas été choisi au hasard : le covoiturage présente de nombreux avantages : réaliser des économies, réduire la pollution, les embouteillages. Il a également une vocation sociale puisqu'il contribue à renforcer le lien entre des individus. C'est donc un service d'avenir.
Mais faire du covoiturage nécessite d'avoir confiance. L'être humain, par nature méfiant, sera réticent à verser des fonds, monter dans le véhicule d'un inconnu, à moins que le service de covoiturage soit organisé par un tiers de confiance, qui assure les réservations, la vérification des identités, permis de conduire, assurances et gère le séquestre des fonds entre les utilisateurs, moyennant le paiement de frais de services.
Le développement d'internet a vu émerger des tiers de confiance d'un nouveau genre : des plateformes de mise en relation, surfant sur l'essor de l'économie collaborative. Parmi elles, on trouve une plateforme web française, qui propose un service de covoiturage présent dans une vingtaine de pays et se ventant d'offrir ses services à plusieurs millions d'utilisateurs.
On peut imaginer, au vu d'un tel succès, que le service rendu et la confiance assurée par cet opérateur sont excellents. Mais en réalité, on constate que la confiance, la satisfaction ne sont pas toujours au rendez-vous. Les frais prélevés par l'opérateur sont en général assez élevés (autour de 20 %). A ces frais s'ajoutent les frais de fonctionnement des banques des utilisateurs. La vérification par l'opérateur des identités des utilisateurs ainsi que des permis de conduire et assurance des conducteurs est souvent insuffisante, voire inexistante. La vie privée des utilisateurs et, en particulier leurs données personnelles, ne sont pas assez protégées. Enfin, les utilisateurs de la plateforme web, ne sont pas à l'abri de pirates informatiques (usurpation d'identité - détournement des fonds versés par les utilisateurs - etc).
La confiance attendue par les utilisateurs n'est donc pas réellement assurée.

Une blockchain pourrait-elle remplacer les intermédiaires actuels : l'opérateur de plateforme et les banques ? Et permettre ainsi de réduire le coût du service de covoiturage pour les utilisateurs ?
Quels sont les principaux problèmes juridiques qui se posent dans le cadre de la mise en place d'un tel projet ?

Voici les questions auxquelles nous allons tenter de répondre par l'étude du projet « BLOCKCAR ». Toutefois, avant d'entrer dans le vif du sujet, il est nécessaire de préciser ce qu'est une blockchain et quels sont les types de blockchain.

Article d'Hubert de Vauplane du 15 octobre 2016 : « les applications pratiques de la blockchain » : https://fr.linkedin.com/pulse/les-applications-pratiques-de-la-blockchain-hubert-de-vauplane

QU'EST-CE QU'UNE BLOCKCHAIN ?

Pour en savoir plus, on peut notamment se référer à la série Réalité Industrielle des Annales des Mines : « *Blockchain et smart contract : des technologies de la confiance* » d'août 2017[1].

1) Il n'existe pas de définition officielle. En France, un premier texte fait référence à la blockchain, sans toutefois la citer : l'Ordonnance du 28 avril 2016 relative aux minibons (titres financiers), qui la présente comme « *un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations* »[1].
2) La blockchain est généralement présentée comme une base de données, ou encore un registre électronique, contenant l'enregistrement horodaté de toutes les opérations effectuées par ses utilisateurs.
3) La blockchain ne doit pas être confondue avec une technologie de stockage ou d'hébergement de données (comme le cloud). En effet, ce qui est enregistré sur la blockchain, ce n'est en principe pas une donnée, ni un document original (comme un contrat par exemple), mais une empreinte cryptographique. Sur ce sujet, nous renvoyons au point I A 1 pour plus d'explications.
Un document original (papier ou numérique) dont l'empreinte cryptographique sera enregistrée sur une blockchain, devra donc être, en parallèle, conservé en lieu sûr.
4) Le registre blockchain est celui d'un réseau distribué, c'est-à-dire que sa conservation n'est pas centralisée à un seul endroit, sur un serveur informatique unique, mais dupliquée sur plusieurs serveurs/ordinateurs situés à différents endroits de la planète. Chaque serveur/ordinateur compris dans ce réseau détient, quasiment au même moment, un exemplaire intégral de ce registre et des informations en principe cryptées qu'il contient.
5) Le registre blockchain est réputé infalsifiable, c'est-à-dire quasiment non piratable. C'est cet aspect fondamental de la blockchain qui fait son intérêt principal. Le niveau de sécurité informatique qu'elle présente serait exceptionnel. Cela est dû, selon les experts, à la combinaison de la cryptographie et, d'un protocole algorithmique innovant réalisé par les « nœuds du réseau », c'est-à-dire par plusieurs serveurs/ordinateurs du réseau sur lequel elle est distribuée, protocole destiné à vérifier, avant enregistrement, que l'information est exacte (les règles de vérification peuvent être variables – voir pour plus d'explication et un exemple le protocole Bitcoin étudié au point I A 1). Les experts expliquent que pour pirater le système, comme par exemple, falsifier une information, il faudrait qu'un hackeur parvienne à convaincre au moins 51% du réseau que l'information qu'il veut falsifier est la bonne (ce qui concrètement serait quasi-impossible).
6) La blockchain permet d'« historiser », en leur donnant une date certaine, les informations qu'elle enregistre. On parle souvent d'horodatage mais ça n'est pas totalement exact puisque les informations sont enregistrées non pas une par une, mais par bloc (chaque bloc de la chaîne comportant plusieurs séries d'informations).
7) Le registre est en principe transparent. Chaque membre du réseau peut vérifier les informations enregistrées sur le registre. Ce registre peut permettre d'assurer la traçabilité des opérations enregistrées sur la blockchain.
8) Il existe plusieurs types de blockchain, avec des caractéristiques bien différentes.

Les 3 types de blockchain
Se reporter aux « Premiers éléments d'analyse de la CNIL »
publiés le 24 septembre 2018

On peut retenir qu'il existe trois types de blockchain :

1) Une blockchain publique :
La blockchain est accessible à n'importe qui dans le monde. Toute personne peut lire le registre et en obtenir une copie (l'accédant), effectuer une transaction (le participant), participer au processus de validation des blocs (le mineur).
2-Une blockchain privée : les règles ici sont très différentes. Elle fonctionne comme un réseau privé (un peu comme un intranet) et appartient à un acteur déterminé qui décide seul des règles de fonctionnement et, en particulier des droits d'accès, de modification et de validation du registre. Le protocole peut donc être modifié selon le bon vouloir de l'administrateur du système.
Beaucoup d'auteurs considèrent ce type d'architecture comme trop éloigné des caractéristiques fondamentales de la blockchain.
3-Une blockchain « permissioned » ou à permission : a des règles définissant quelles personnes peuvent participer au processus d'approbation ou même effectuer des transactions. Elles peuvent, selon les cas, être accessibles à tous ou être en accès limité.

Abordons maintenant la faisabilité du projet BLOCKCAR : un service de covoiturage sur une blockchain.

Nous étudierons, dans une première partie, les aspects technologiques du projet (I) avant de présenter, les principales questions juridiques qui peuvent se poser (II).

PARTIE I –UNE BLOCKCHAIN POUR UN SERVICE DE COVOITURAGE : ANALYSE AU PLAN TECHNOLOGIQUE

Nous commencerons l'étude du projet BLOCKCAR en nous interrogeant sur la possibilité qu'il y a, au plan technologique de supprimer, grâce à une blockchain et à un smart contract, tout intermédiaire (**A-**). Nous aborderons ensuite les inconvénients et les risques potentiels que présente une blockchain, en particulier une blockchain publique (**B-**), avant d'arrêter le cadre technologique qui nous semblerait le plus adapté à un service de covoiturage désintermédié (**C-**). Enfin, nous ferons l'essai pratique d'un smart contract afin de comprendre comment un service de covoiturage pourrait fonctionner sur une blockchain, de manière autonome ou presque (**D-**).

A - LA DESINTERMEDIATION D'UN SERVICE DE COVOITURAGE

Deux types d'intermédiaires interviennent actuellement dans un service de covoiturage :

- les établissements bancaires : le passager rémunère le conducteur par l'intermédiaire de sa banque. Le conducteur encaisse quant à lui les fonds sur le compte qu'il détient auprès de sa propre banque.
- l'opérateur de plateforme en ligne : le service de covoiturage est le plus souvent organisé par une plateforme internet. L'opérateur de la plateforme devient destinataire des fonds, dès réception d'une demande de réservation faite par un utilisateur souhaitant réserver un trajet de covoiturage en tant que passager. Lorsque le trajet de covoiturage est terminé, l'intermédiaire reverse au conducteur le prix du covoiturage convenu avec le passager, sous déduction d'une commission qu'il encaisse sur le compte ouvert auprès de sa propre banque. L'opérateur gère également les annulations en assurant le remboursement des fonds selon les cas, soit au passager, soit au conducteur.

Comment supprimer ces intermédiaires grâce à une blockchain et à un smart contract ?

1° La suppression des intermédiaires bancaires dans le service de covoiturage

La suppression des établissements bancaires semble possible au plan technologique, grâce à la blockchain. A ce sujet, on peut se référer à la blockchain publique la plus mature à ce jour : **Bitcoin.** Bitcoin, née en 2009[4], permet à ses utilisateurs de se rémunérer directement, à l'occasion d'opérations diverses, sans passer par leur banque. Ces utilisateurs sont quasi anonymes. Ils utilisent des pseudonymes et se rémunèrent, à partir d'un portefeuille virtuel (wallet) et des adresses de paiement, en bitcoin, la monnaie cryptographique utilisée.

Cryptographie asymétrique

Pour bien appréhender les enjeux juridiques de la blockchain, il est important de comprendre la cryptographique utilisée dans le système Bitcoin, qui permet d'assurer l'identification d'une adresse de portefeuille utilisateur et l'intégrité d'un paiement auquel il se rattache. Deux fonctions cryptographiques sont utilisées ; les fonctions de signature électronique et de hachage.

La signature électronique fonctionne sur le principe d'un jeu de clés : une clé publique / une clé privée. Cette cryptographie est dite « asymétrique ». Cela signifie qu'une personne peut, à partir d'une clé privée, obtenir la clé publique correspondante mais pas l'inverse (la clé est à sens unique). Il est donc techniquement quasi-impossible de trouver le code de la clé privée (connu de son seul propriétaire) à partir de la clé publique.

Une empreinte cryptographique est le résultat d'une fonction de hachage appliquée à une donnée initiale. Pour une même donnée, on obtient toujours la même empreinte.

Comme la signature électronique asymétrique, cette empreinte est à sens unique : il est quasiment impossible de déterminer la donnée initiale à partir de son empreinte. De plus, toute modification des données initiales induira une empreinte différente.

Sur Bitcoin, chaque utilisateur dispose d'un portefeuille (il peut en avoir plusieurs). Ce portefeuille ne contient pas de bitcoin, mais des clefs de signature électronique permettant de les utiliser. Les bitcoins sont enregistrés dans la blockchain et sont rattachés à des adresses, avec des verrous. Ils ne peuvent être dépensés que si l'on déverrouille ces derniers avec la bonne clé.

Pour réaliser un paiement, l'utilisateur participant va générer à partir de son portefeuille un jeu de clé (clé privée / clé publique).

Une adresse de paiement (comme un RIB) est alors crée à partir de la clé publique (La construction de l'adresse se fait en 2 étapes : elle est calculée par un double hachage de la clé publique. Le résultat est ensuite encodé).

[4] Le protocole blockchain et Bitcoin auraient été inventés par un certain Satoshi Nakamoto. Bitcoin est une blockchain publique qui n'appartient à personne ou plutôt à l'ensemble du réseau. Son code source est public.

La signature électronique permet de s'assurer que l'utilisateur participant est propriétaire d'une adresse de paiement, qu'il possède bien la clé privée associée à cette adresse (une adresse a vocation à être utilisée que pour un seul paiement). L'utilisateur destinataire des fonds va, de son côté, générer une adresse de réception des fonds et une clef de déverrouillage. Le déverrouillage requiert la présentation d'une clef publique et d'une signature effectuée avec la clef privée correspondante (selon le principe du script "pay-to-public-hash").
La quasi-totalité des transactions consiste à transférer des bitcoins depuis des adresses émetteurs (inputs) vers des adresses destinataires (outputs).
Une fois la transaction émise par l'utilisateur émetteur, celle-ci sera envoyée aux nœuds du réseau pour vérification par les mineurs.
Le registre est transparent en ce sens que n'importe qui peut librement le consulter et lire le hash des clés publiques des adresses et des paiements effectués et donc voir que, tel jour à telle heure, un paiement d'un montant de X est intervenu entre deux adresses des deux participants.
Avec la cryptographie utilisée, il n'est en théorie pas possible pour les membres du réseau de remonter jusqu'à l'identité des participants à une transaction (puisque seul l'utilisateur dispose du code de sa ou ses clé(s) privée(s)). C'est pourquoi, le quasi-anonymat des participants est en principe permis (sur la blockchain seulement car si l'utilisateur ne préserve pas son identité avant de se connecter à la blockchain (en utilisant par exemple Tor, un réseau spécifique permettant de cacher l'adresse IP de connexion), et n'utilise qu'un seul portefeuille bitcoin, il pourrait être démasqué grâce au registre qui enregistre et trace toute opération effectuée).
A noter que la CNIL considère que les clés publiques des participants constituent des données personnelles dès lors qu'il est possible techniquement de remonter indirectement à leur identité.

Focus sur le protocole de vérification Bitcoin
Avant que le paiement soit enregistré, le protocole de vérification réalisé par les nœuds du réseau Bitcoin comporte les étapes suivantes[5] :

- Etape 1 : établir le lien entre deux adresses utilisateur et un paiement réalisé
- Etape 2 : s'assurer que l'utilisateur émetteur d'un paiement possède suffisamment de bitcoin sur son adresse pour réaliser ledit paiement
- Etape 3 : vérifier l'intégrité du paiement (qu'il n'intervient qu'une fois)

Cette dernière étape est la plus importante et constitue le cœur d'innovation de la blockchain : il s'agit de la mise à jour du registre grâce à « la preuve de travail » réalisée par les « mineurs » (certains nœuds du réseau). Cette étape consiste à vérifier la balance financière de chaque utilisateur du réseau, pour éviter les doubles dépenses (comme le ferait une banque dans un système centralisé). La blockchain peut être vue comme un grand livre de compte qui contient toute les transactions depuis le début de Bitcoin, permettant ainsi de suivre le devenir de chaque bitcoin. Toute entrée d'une transaction est nécessairement la sortie d'une autre transaction.
La mise à jour de ce grand livre de compte n'est pas simple puisque le réseau est décentralisé et que chaque nœud détient, à un instant déterminé, un exemplaire du registre. La mise à jour doit donc se faire, à plusieurs endroits, grâce à la recherche d'un consensus entre les nœuds. La preuve de travail se fait non pas par transaction mais par bloc de transactions.
Elle nécessite une puissance de calcul énorme, très consommatrice en électricité. Le premier mineur qui trouve la solution (la bonne balance financière) la transmet au réseau. D'autres nœuds vérifient alors la solution trouvée grâce à un calcul algorithmique. Si la solution trouvée est bien la bonne, le bloc est alors « validé », le paiement est confirmé et le mineur perçoit, en récompense de son travail, une rétribution (en bitcoin).
Le travail de minage des blocs est particulièrement long et compliqué à réaliser.

[5] Lire l'article de Gautier Marin-Dagannaud pour comprendre la blockchain bitcoin : https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/

C'est pour cette raison que les nœuds et les mineurs sont naturellement encouragés à coordonner leurs efforts pour trouver le bon résultat de la balance financière, plutôt que de tenter de détourner des bitcoins, ce qui nécessiterait de convaincre au moins 51 % des nœuds que la balance piratée est la bonne. C'est aussi pour cette raison que le minage sur Bitcoin est dans les faits, réalisé par des pools de mineurs (des coopératives), basées le plus souvent en Chine, là où l'électricité est la moins chère.
La difficulté, le coût en électricité et l'incitation du jeu poussent en définitive les nœuds du réseau à trouver un consensus, à respecter le protocole blockchain, plutôt qu'à le transgresser (en tentant de falsifier le registre, par exemple : de modifier le montant ou l'adresse de destination d'un paiement).

La formation de la chaîne des blocs
On rappelle que ça n'est pas un seul paiement (une transaction intervenue entre 2 participants) qui est vérifié puis enregistré sur la blockchain Bitcoin mais un bloc de transactions.
Une fois vérifié, le bloc est enregistré sur la blockchain. On dit qu'il est « accroché » au bloc précédemment enregistré car l'empreinte cryptographique (le hash) du bloc précédent est inscrite dans le nouveau bloc et, ainsi de suite, formant alors une « chaîne de blocs » ou encore un registre contenant l'enregistrement horodaté de toutes les opérations effectuées par ses utilisateurs.
Le registre Bitcoin est transparent et immuable. Plus la chaîne de blocs est longue et plus il devient statistiquement difficile de l'attaquer.

On voit ainsi qu'il est aujourd'hui possible, au plan technologique, d'utiliser une blockchain, comme Bitcoin, pour rémunérer directement un tiers, sans passer par une banque, pour l'achat d'un produit ou pour la réalisation d'une prestation de service, comme celle d'un covoiturage.
Cela suppose toutefois que les utilisateurs du service se rémunèrent, non pas en euro, mais en monnaie virtuelle (en bitcoin). Les utilisateurs doivent alors, au préalable, échanger des euros contre des bitcoin[6] et disposer de jeux de clés (clé privée – clé publique). Nous verrons plus loin (II B 2) qu'utiliser une monnaie virtuelle présente certaines incertitudes au plan juridique, mais que des solutions existent.
Rappelons à ce titre qu'une blockchain est un registre et peut fonctionner sans transaction financière. Son rôle premier est d'enregistrer une information. On pourrait d'ailleurs utiliser une monnaie reconnue légalement, comme l'euro ou le dollars, plutôt qu'une cryptomonnaie, et d'enregistrer l'information confirmant la transaction financière (comme l'avis de paiement) sur le registre.

Examinons à présent s'il est possible de supprimer, au plan technologique, le second intermédiaire intervenant dans le service de covoiturage : l'opérateur de plateforme en ligne.

2° La suppression de l'opérateur de plateforme en ligne dans un service de covoiturage

L'étude de cette question nous permet d'aborder une autre technologie, au moins aussi passionnante que la blockchain, pour des juristes : **le smart contract.**

Définition du smart contract
Le smart contract est un concept inventé en 1993 par l'informaticien Nick Szabo. C'est un programme informatique qui permet de programmer à l'avance l'exécution automatique de conditions prédéfinies (si…., alors….)[7].

[6] Actuellement 1 bitcoin (BTC) = 6 719 € (la valeur du bitcoin varie en fonction de l'offre et de la demande). Pour acheter des bitcoins, il faut en général passer par des plateformes de change : https://bitcoin.fr/acheter-bitcoin/
[7] Pour en savoir plus sur les smart contract : Wikipédia contrats intelligents

Ces conditions sont rédigées en code informatique. Son avantage est double : permettre d'automatiser certains process d'exécution et de réduire leur coût de fonctionnement manuel, tout en augmentant la force d'exécution des conditions qu'il contient.
Par ailleurs, si on déploie un smart contract dans une blockchain, l'exécution programmée d'une fonction prédéfinie devient définitive et quasi-inattaquable. C'est ce que propose la blockchain Ethereum.

Ethereum
Un jeune canadien Vitalik Buterin a eu l'ingénieuse idée d'associer la technologie Bitcoin au smart contract, en créant en 2013, la blockchain Ethereum[8]
Ethereum reprend le concept du smart contract pour l'intégrer dans une blockchain publique. Celle-ci fonctionne un peu comme un « ordinateur mondial » distribué, à partir duquel il devient possible de développer sa propre application décentralisée (grâce à un ou plusieurs smart contract).
Ethereum permet donc à toute personne (sachant coder) de créer un smart contract, de programmer ainsi la réalisation automatique d'un ou plusieurs évènement(s) et d'enregistrer sur la blockchain les hashs des clés publiques générées (leur empreinte) pour réaliser des opérations, afin qu'elles bénéficient d'un niveau de sécurité informatique inédit.
Un smart contract contient du code informatique. Il peut également en théorie contenir des données en clair. Le contenu d'un smart contract dépendra en définitive de celui qui le construit et des données qu'il souhaite intégrer pour son application.
Comme avec Bitcoin, le registre Ethereum est immuable[9] et transparent[10]. N'importe quel membre du réseau peut le consulter, ou encore participer à la preuve de travail (et donc contribuer à l'exécution des smart contracts). Une version grand public d'Ethereum, dénommée Metropolis, est actuellement en cours de développement.
La monnaie virtuelle utilisée est l'ether. Elle sert à rémunérer les nœuds du réseau et les mineurs, dont le rôle consiste à vérifier l'exécution des fonctions programmées des smart contracts[11].

L'intégration de la technique du smart contract à une blockchain permettrait de supprimer l'opérateur de plateforme dans un service de covoiturage.
On pourrait en effet imaginer de programmer dans un smart contract l'exécution d'un service de covoiturage : et plus précisément, les demandes de réservation faites par les utilisateurs, le versement des fonds à titre de séquestre, la confirmation des réservations, la libération des fonds après parfaite exécution du service de covoiturage, le remboursement des fonds en cas d'annulation, etc. Tous ces services, ou presque, pourraient finalement être automatisés (cf notre essai pratique de smart contract au point I D).
La blockchain permettrait quant à elle d'enregistrer certaines informations liées au service et d'assurer la sécurité informatique du service.

Plusieurs start-up, comme Slock.it, travaillent actuellement au développement d'applications particulièrement ambitieuses, à partir du protocole Ethereum et pourraient, selon certains, remplacer des plateformes d'intermédiation comme Uber ou AirBnB.

[8] Ethereum est une blockchain publique, dont le code source est ouvert, mais qui est encore à ce jour contrôlée (du moins en partie) par la Fondation Ethereum présidée par Vitalik Buterin
[9] Immuable en théorie car l'affaire The DAO montre qu'un fork (une rupture de la chaîne) reste possible.

[11] Peu d'articles permettent à ce jour de comprendre clairement comment fonctionne le protocole Ethereum, d'autant que ce dernier est en cours d'évolution (la preuve de travail évoluerait vers un protocole différent : the proof of stake, moins énergivore)[11].
Pour en savoir plus, on peut lire le livre blanc d'Ethereum : https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/ ainsi que l'article de Simon Polrot Avocat : https://www.ethereum-france.com/quest-ce-que-lethereum/

Ainsi, plusieurs aspects d'une blockchain publique, comme Bitcoin et Ethereum, semblent intéressants à explorer pour notre cas d'usage « BLOCKCAR » :

- Grâce au smart contract, le paiement du service de covoiturage pourrait se faire directement entre les utilisateurs, sans aucun intermédiaire, permettant ainsi un service de pair à pair, plus économique ;
- le protocole blockchain permettrait d'assurer l'enregistrement historisé et non modifiable des opérations du service de covoiturage, assurant ainsi un certain niveau de confiance, du moins au plan de la sécurité informatique, des utilisateurs dans le système.

Cependant, une blockchain publique présente plusieurs inconvénients et risques qu'il convient d'identifier, avant d'envisager de lancer un projet de blockchain et, en particulier, un service de covoiturage.

B- INCONVENIENTS ET RISQUES POTENTIELS D'UNE BLOCKCHAIN PUBLIQUE

L'utilisation d'une blockchain publique comme Bitcoin ou Ethereum, pose selon nous, un certain nombre de questions importantes qui sont susceptibles de générer, au plan juridique, des risques d'insécurité.

Voici la liste des inconvénients et risques qui nous semblent les plus manifestes.

1° Le quasi anonymat des acteurs

Dans une blockchain publique telle que Bitcoin ou Ethereum, les utilisateurs sont quasi-anonymes. Ils sont identifiés grâce à leur clé publique de signature électronique.
Or, dans le cadre d'un service de covoiturage, il est essentiel que les acteurs du service soient clairement identifiés et soient susceptibles d'engager leur responsabilité en cas de défaillance du système causant un préjudice à un utilisateur.
A défaut d'identification suffisante, qui serait responsable en cas de dysfonctionnement de la blockchain, ou encore en cas de comportement défaillant d'un smart contract, causant un préjudice à un utilisateur ou à un tiers ? Voir sur cette question, notre développement au paragraphe II C 2.

2° L'intangibilité du registre

Cet aspect, caractéristique majeure d'une blockchain interroge au plan juridique.
L'immutabilité du registre comportant des informations comme un paiement est-elle compatible avec le principe de nullité des actes juridiques qui permet en particulier, à une personne qui serait victime d'un vice du consentement lors de la formation d'un contrat, de solliciter et d'obtenir en justice la nullité de ce contrat et donc son effacement rétroactif (un contrat annulé est censé n'avoir jamais existé) ?
Est-ce que l'effet rétroactif de la nullité d'un contrat est compatible avec l'inscription immuable sur la blockchain d'un paiement réalisé au titre de ce contrat ?

3° L'absence d'authentification des informations enregistrées sur la blockchain

C'est un point très important : la blockchain permet d'enregistrer une information. Mais à ce jour, le protocole de vérification n'a pas pour fonction d'authentifier cette information au sens juridique.
Ex : il est possible d'enregistrer sur la blockchain une œuvre originale à des fins de protection intellectuelle. Cela aura pour avantage de donner une date certaine à cet enregistrement et de tendre à démontrer, en cas de contestation, que cet œuvre a été enregistrée tel jour par tel personne. **Mais la blockchain à elle seule ne permet pas de certifier que l'auteur de cet enregistrement est bien le propriétaire de l'œuvre et non un contrefacteur.**

Or, si l'authenticité de l'information n'est pas vérifiée avant son enregistrement sur la blockchain, alors, c'est une information fausse voir illicite qui sera enregistrée sur le registre blockchain, et ce, de manière définitive.

Par conséquent, il apparaît important que des tiers de confiance comme des notaires ou encore des prestataires de service de confiance interviennent en amont de l'enregistrement de chaque information sur le registre à des fins d'authentification.

3° La concentration en pool de minage malgré la décentralisation du réseau

Nous avons vu précédemment pour Bitcoin que le travail de minage réalisé par certains nœuds du réseau est si compliqué et coûteux en électricité à réaliser que cela pousse les acteurs à se regrouper en pool de minage.
Cette tendance à la concentration n'est-elle justement pas l'ennemi du système (qui se veut par définition distribué) ? Des pools de minage basés dans un pays comme la Chine ne posent ils pas également un problème en termes de sécurité ? Il n'est pas impensable d'imaginer que la Chine pourrait, pour des raisons politiques ou d'opportunité, couper l'électricité dans les zones de minage, ce qui mettrait potentiellement tout le système Bitcoin en péril.
Un pool de minage, particulièrement influent et dirigé dans l'ombre par une entité secrète, ne pourrait-il pas parvenir aux 51 % nécessaires pour pirater la blockchain (et détourner des fonds de leur destination initiale) ?
Le nombre de nœuds du réseau, le niveau de décentralisation et leur localisation sont des aspects importants de la sécurité informatique de la blockchain. A noter qu'Ethereum travaille actuellement sur un projet tendant précisément à éviter la concentration de mineurs.

4° Les failles potentielles de sécurité aux interfaces de la blockchain

Cet autre aspect est important car il pose plus largement la question de l'interaction de la blockchain avec le monde réel. Si la blockchain est censée offrir un niveau de sécurité informatique très élevé, une modification, un détournement de l'information, juste avant son enregistrement sur la blockchain resterait toutefois possible. Or, l'enjeu d'une cyberattaque, intervenant avant l'entrée de la donnée sur la blockchain, est crucial puisqu'une fois enregistrée, la donnée ne peut plus être modifiée.

5° La fiabilité des données dont a besoin le smart contract pour fonctionner

Pour exécuter les conditions prédéfinies, le smart contract interagit soit avec des données déjà présentes sur la blockchain soit avec des données extérieures à la blockchain.
Dans ce dernier cas, Ethereum propose de recourir à un « **Oracle** », c'est-à-dire à une personne ou une machine désignée dans le smart contract et qui aura pour mission de collecter la donnée située à l'extérieur de la blockchain pour la restituer dans le smart contract et de permettre ainsi l'exécution de l'opération programmée.
Mais comment s'assurer que la donnée collectée à l'extérieur de la blockchain, et devant être enregistrée dans le smart contract, est bien exacte ? Comment être sûr qu'elle n'a pas été corrompue ?
L'Oracle de la blockchain Ethereum n'est-il pas une nouvelle forme de tiers de confiance ?[12]

A l'issue de ces premières analyses, on constate que si la blockchain et le smart contract peuvent en théorie permettre de supprimer des intermédiaires de confiance, ils font néanmoins apparaître d'importantes interrogations et de nouvelles sources d'insécurité, notamment au plan juridique.

[12] Pour en savoir plus sur cette question : https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/

C - UNE BLOCKCHAIN A PERMISSION, CHOIX TECHNOLOGIQUE RETENU POUR LE PROJET BLOCKCAR

L'utilisation d'une blockchain publique, comme Bitcoin ou Ethereum, pose, à notre sens, d'importantes questions, non encore résolues à ce jour, et est source d'insécurité.
C'est pourquoi il nous a semblé plus opportun d'étudier la possibilité de mettre en place une blockchain non pas publique mais à permission, construite par exemple à partir d'Hyperledger, gérée par la Linux Foundation[13].
Hyperledger n'est pas exactement une blockchain. C'est en réalité un « tool kit » (boîte à outils), permettant à des développeurs de construire une blockchain répondant à leurs besoins spécifiques.
Les droits de consultation, d'écriture et de modification du registre peuvent ainsi être paramétrés selon des règles préétablies. Nous ne sommes donc plus sur un système totalement égalitaire, horizontal et transparent comme Bitcoin par exemple.
IBM a lancé une offre "*Blockchain as a service*" développée à partir du code open source Hyperledger (Fabric, version 1.0). Il s'agit d'une sorte de Framework (un cadre applicatif) que les entreprises pourront utiliser, pour créer leur propre réseau blockchain sécurisé, applicable à n'importe quel secteur d'activité. Ce service offrirait la possibilité de choisir, en option, des couches additionnelles de sécurité comme la mise en place de contrôles d'accès, la gestion sécurisée des clés de chiffrement, ou encore la possibilité de coupures en cas de détection d'intrus.
La fondation Linux vient, par ailleurs, de lancer un nouveau projet dénommé « Composer » pour permettre le développement de smart contract à partir d'Hyperledger[14]

Ainsi, il serait possible d'envisager la mise en place, au plan technologique, d'une blockchain à permission construire « sur mesure », afin de l'adapter à un service de covoiturage et, dont les caractéristiques principales pourraient être les suivantes (nous consacrerons plus loin des développements particuliers à certaines de ces caractéristiques) :

- Un réseau distribué ouvert à tous serait mis en place pour permettre d'accueillir le plus grand nombre d'utilisateurs, mais les droits d'accès, de consultation, et de modification du registre seraient préalablement déterminés par une entité[15], selon des règles prédéfinies (voir sur ce point notre proposition : II C 2)
- L'accès au service de covoiturage se ferait grâce à une plateforme web et/ou applicative interfacée avec la blockchain
- La réalisation du service de covoiturage se ferait grâce à la mise en place d'un smart contract permettant l'exécution automatique des réservations, des confirmations, le séquestre des fonds, la libération des fonds, et les remboursements (cf notre essai pratique de smart contract au point I D)
- Les paiements de pair à pair seraient réalisés grâce à la mise en place d'une cryptomonnaie (Nous renvoyons sur ce point au paragraphe II B)
- Tous les acteurs du réseau et du service seraient clairement identifiés (pas d'anonymat) et la localisation géographique des nœuds du réseau serait choisie avec soin (en France, et /ou dans des pays stables et sécurisants au plan du droit et de la sécurité internationale)
- Les règles de vérification des informations par les nœuds seraient prédéfinies et adaptées à un service de covoiturage

[13] Plusieurs acteurs fondateurs participent à son pilotage (notamment IBM, Intel, Cisco, Accenture ou J.P.Morgan). IBM bien que minoritaire au sein du comité de direction, est celui qui contribue le plus à Hyperledger, en particulier sur le code informatique.
[14] Voir à ce sujet l'article de Maryse Gros avec IDG News Service , du 09 Mai 2017 : http://www.lemondeinformatique.fr/actualites/lire-la-fondation-linux-modelise-l-automatisation-de-contrats-sur-blockchain-68140.html
[15] Voir sur cette question, notre proposition : partie I-B

- Le registre blockchain enregistrerait les empreintes (le hash) de clés publiques de signature électronique relatives aux exécutions du service grâce au smart contract, assurant ainsi la traçabilité des opérations
- Le registre n'ayant pas pour vocation de stocker de données en clair, un cloud sécurisé (comme celui d'IBM) hébergerait l'ensemble des informations et documents liés au fonctionnement du service du covoiturage

Avant de poursuivre notre étude et d'aborder la faisabilité juridique du projet BLOCKCAR, il nous a paru intéressant d'exposer, comment pourrait se construire un smart contract pour un service de covoiturage. Cet essai pratique du smart contract nous semble d'autant plus nécessaire qu'il pose des questions juridiques intéressantes pour les juristes et les avocats (comme nous le verrons plus loin – cf II D 2).

D -ESSAI PRATIQUE D'UN SERVICE DE COVOITURAGE DANS UN SMART CONTRACT

Construire et lire un smart contract suppose de comprendre le fonctionnement du code informatique. Voici, à titre d'exemple, à quoi peut ressembler un smart contract[16] sur Ethereum pour l'exécution d'un jeu simple de type pierre, feuille, ciseau. Pour une personne qui ne sait pas coder, le contenu d'un smart contract peut sembler compliqué à comprendre[17].
Il nous a dès lors paru utile, de voir comment pourrait se traduire un service de covoiturage dans un smart contract, mais dans un langage un peu hybride, à cheval entre le langage informatique et le langage français, afin de permettre sa compréhension par le plus grand nombre.

On rappelle qu'un smart contract est un protocole informatique qui permet de programmer à l'avance l'exécution automatique de conditions prédéfinies. Il fonctionne selon la logique conditionnelle :
si…alors….
Par ailleurs, pour être exécuté, le smart contract obéit à des « fonctions ».
En outre, l'exécution d'un smart contract se fait grâce à du gas (un peu comme le carburant d'une voiture) payé en monnaie virtuelle. Ce gas sert également à récompenser les nœuds du réseau pour la preuve de travail effectuée (cf. l'incitation au consensus déjà exposée sur Bitcoin).
Dans l'hypothèse d'un service de covoiturage, un smart contract pourrait être construit pour automatiser certaines exécutions conditionnées du service.
Par précaution, ce smart contract ne comporterait aucune donnée en clair mais uniquement du code informatique et des données « hashées ». La cryptographie utilisée serait celle décrite au paragraphe consacré à Bitcoin (I A 1).
Les principales fonctions d'un smart contract de covoiturage pourraient se traduire de la manière suivante (l'hypothèse retenue est volontairement la plus simple : celle d'un covoiturage entre un conducteur et un seul passager). L'exécution de chaque fonction serait enregistrée sur la blockchain :

Fonction 1 : Demande de réservation

Cette fonction serait activée depuis la plateforme web du service, interfacée avec la blockchain, par un utilisateur souhaitant réserver un trajet de covoiturage proposé par un conducteur.

Le passager génèrerait grâce à la signature électronique depuis son portefeuille une adresse et réaliserait un paiement à l'adresse du smart contract, d'un certain montant en monnaie virtuelle (par exemple 100 ether), ce montant intégrant à la fois le prix du covoiturage et le coût de

[16] On peut se référer au workshop tenu par Clément Lesaege :
https://gist.github.com/anonymous/c752ca1ec20a32a5bb5501e52bcbf78d
[17] Pour en savoir plus sur la manière de construire un smart contract, on peut lire https://www.ethereum-france.com/ecrire-une-dapp-pour-ethereum-1-smart-contract/

fonctionnement du smart contract (exprimé en gas et représentant l'équivalent de quelques centimes d'euros)[18].

- Si un utilisateur passager activait la fonction réservation en versant le montant de la réservation
- Alors :

→ le smart contract – fonction 1 - serait activé

→ le montant versé pour la réservation serait séquestré sur l'adresse du smart contract

Fonction 2 : Réponse conducteur

Trois variables seraient prévues ici : « acceptation » - « refus » - « non-réponse » du conducteur

- Si le conducteur adressait la variable « refus » depuis son adresse utilisateur
- Alors : les deux actions suivantes seraient automatiquement activées dans le smart contract :

→ le remboursement des fonds séquestrés depuis l'adresse du smart contract vers l'adresse du passager

→ la fin du smart contract

- Si le conducteur adressait la variable « acceptation »
- Alors : l'action suivante serait activée :

→ la réalisation du covoiturage le jour J (J étant le jour fixé pour la réalisation de la prestation de covoiturage)

- Si le conducteur n'activait pas la fonction 2 au bout d'un temps déterminé (J+7 par exemple)
- Alors : la fin automatique du smart contract serait enregistrée

- **Fonction 3 : Annulation**

Plusieurs variables seraient prévues sous cette fonction, pour envisager l'hypothèse d'une annulation éventuelle du trajet par l'un des deux utilisateurs (passager, conducteur) avant le jour J, avec ou sans le respect d'un préavis raisonnable (fixé ici à 2 jours) :

- Si la fonction « annulation » du covoiturage était activée par le passager ou le conducteur avant J-2
- Alors : les deux actions suivantes seraient activées :

→ le remboursement des fonds séquestrés depuis l'adresse du smart contract vers l'adresse du passager

→ la fin du smart contract

- Si la fonction « annulation » du covoiturage était activée par le passager/ ou le conducteur après J-2
- Alors : les deux actions suivantes seraient enregistrées :

→ la libération des fonds séquestrés, depuis l'adresse du smart contract vers l'adresse du conducteur/ou du passager

→ la cotation de l'utilisateur passager/ ou du conducteur serait de 0/5

→ la fin du smart contract

- **Fonction 4 : Evaluation**

Les variables suivantes de cette fonction seraient activées par chaque utilisateur ou par défaut, après la réalisation d'un covoiturage (après J+7) :

- Si l'évaluation était activée par les deux utilisateurs :
- Alors :

→ un avis serait enregistré par chacun concernant l'autre utilisateur : cotation allant de 0 à 5 (la cotation pourrait par exemple garder en mémoire les dernières variables d'évaluation)

→ la fonction 5 serait automatiquement activée.

- Si l'évaluation n'était pas activée par l'un des deux utilisateurs après J+7 :

- Alors :

→ une cotation de 0/5 serait appliquée par défaut à l'utilisateur n'ayant pas activé la Fonction 4
→ la fonction 5 serait automatiquement activée.

Fonction 5 : Fin du smart contract

Les 2 variables de cette fonction seraient les suivantes : « Prestation réalisée » - « Prestation non réalisée ou mal réalisée »
La fonction 5 serait activée soit, après que chaque partie ait activé la fonction 4 soit, par défaut après J+7.

- Si la prestation était réalisée :
- Alors :

→ les fonds séquestrés sur le smart contract seraient envoyés vers l'adresse du conducteur, après déduction du montant d'ether accordé aux nœuds du réseau pour leur participation au protocole de vérification

- Si la prestation n'était pas réalisée ou mal réalisée :

Si l'activation de cette variable était faite par l'un au moins des deux utilisateurs

- Alors :

→les fonds seraient transférés vers une adresse « sinistre »
→ la fin du smart contract serait activée

L'activation de cette dernière variable déclencherait la saisine automatique de l'organe qui serait en charge de la gestion des désaccords ou sinistres (voir sur ce point notre proposition au point II C 2).
Nous pourrions également envisager que ce smart contract communique avec d'autres smart contract comme par exemple :
-le smart contract dédié à la réputation des utilisateurs pour permettre une mise à jour automatique des cotations
-le smart contract dédié aux droits d'accès, de consultation, et de modification du registre (les droits pourraient par exemple être fixés en fonction de la réputation obtenue et d'un nombre minimum de covoiturage réalisé)

Après avoir étudié les aspects technologiques de la blockchain, du smart contract et retenu le cadre qui nous semble le plus adapté pour le projet BLOCKAR, celui d'une blockchain à permission, abordons à présent la faisabilité juridique d'un tel projet.

PARTIE II – UNE BLOCKCHAIN POUR UN SERVICE DE COVOITURAGE : ANALYSE JURIDIQUE

L'objectif de cette seconde partie sera se passer en revue - il s'agit non d'être exhaustif mais avant tout de donner une vue d'ensemble et d'explorer une matière en cours d'évolution - les principales questions juridiques qui peuvent se poser dans le cadre du projet BLOCKCAR.

Après avoir fixé le cadre juridique de l'étude (**A-**), nous aborderons la possible désintermédiation bancaire (**B-**) puis la gouvernance du système : l'absence d'administration humaine du service, à l'instar de l'expression souvent utilisée « Code is Law[19] » est-elle possible au plan juridique ? (**C-**). Nous analyserons ensuite la force juridique des opérations réalisées dans un smart contract et des informations enregistrées sur la blockchain (**D-**) avant de terminer notre étude par la question de la protection des données personnelles des utilisateurs du service (**E-**).

A – QUEL CADRE JURIDIQUE APPLICABLE POUR LA BLOCKCHAIN ?

La blockchain interroge, tout d'abord, quant au droit applicable. Est-ce bien le droit français et la compétence des juges français qui s'appliqueraient en cas de défaillance causant un préjudice à un utilisateur français ?
Le réseau décentralisé d'une blockchain, comportant des nœuds et des mineurs présents dans différents pays ne constituerait-il pas l'élément d'extranéité qui impose alors de faire application des règles de droit international privé et de droit européen (c'est-à-dire lorsqu'au moins deux systèmes juridiques sont concernés) ?

Pour la présente étude, nous raisonnerons en droit français et n'aborderons pas les règles de droit international privé et européen (qui mériteraient un article à part entière).

La blockchain n'a pas, à ce jour, de cadre juridique spécifique en droit français. Elle n'est pas interdite mais n'est pas non plus reconnue juridiquement[20].
A noter cependant la démarche du gouvernement français au printemps 2016, sous l'impulsion d'Emmanuel Macron, consistant à expérimenter la blockchain dans un domaine particulier ; celui des bons de caisses, par l'adoption d'une Ordonnance le 28 avril 2016, laquelle autorise l'inscription des émissions et cessions de minibons, sur un « *dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations* ».
Si le texte de l'Ordonnance ne fait pas expressément référence à la blockchain, le rapport au Président de la République relatif à cette ordonnance la mentionne explicitement[21].
La Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, la lutte contre la corruption et la modernisation de la vie économique a habilité le gouvernement à prendre par voie d'ordonnance, dans le délai de 12 mois, les mesures nécessaires pour adapter le droit applicable aux titres financiers et aux valeurs mobilières afin de permettre la représentation et la transmission, au moyen d'un dispositif d'enregistrement électronique partagé, des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers.

[19] L'expression aurait été inventée par le juriste américain Lawrence Lessing
[20] Cette technologie n'est pas encore reconnue par l'ANSSI (l'Agence Nationale de la sécurité des systèmes d'information).
[21] Voir le rapport au Président de la République relatif à l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse - JO n°0101 du 29 avril 2016 texte n° 15

Précisons que le gouvernement[22] a lancé une consultation publique sur la blockchain, toujours dans le domaine des titres financiers, afin de recueillir les avis des parties prenantes intéressées et de définir les principes ainsi que le niveau de règlementation à retenir[23].
Ainsi, une clarification des règles de la blockchain, dans le domaine particulier des titres financiers, devrait intervenir prochainement.
Dans l'intervalle, il conviendra de raisonner selon les règles de droit françaises actuellement en vigueur.

B - LA DESINTERMEDIATION BANCAIRE D'UN SERVICE DE COVOITURAGE

Nous avons vu que la blockchain Bitcoin fonctionnait sans aucun intermédiaire bancaire, les utilisateurs du service utilisant, pour se rémunérer directement entre eux, une monnaie virtuelle appelée bitcoin, basée sur la cryptographie : une cryptomonnaie.
Quelle valeur juridique peut-on donner à ce type de monnaie ?
La reconnaissance juridique des monnaies virtuelles fait aujourd'hui débat en France.
Si ces monnaies ne font pas l'objet d'une interdiction formelle, elles n'ont toutefois pas de reconnaissance légale. Le bitcoin et l'ether ne sont pas au sens du droit français, considérées comme des monnaies.
Selon l'article L111-1 du Code monétaire et financier, la seule monnaie française est l'euro.
Il ne s'agirait pas non plus de monnaie électronique au sens de l'article L315-1 du Code monétaire et financier qui énonce que : « *la monnaie électronique est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement définies à l'article L. 133-3 et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* ».
En effet, une monnaie électronique suppose qu'au préalable les unités incorporées au titre soient bien de la monnaie, ce qui n'est pas le cas d'une cryptomonnaie.
C'est ainsi que la quasi-totalité des auteurs refuse la qualification de monnaie à une cryptomonnaie, retenant ainsi une interprétation purement littérale des textes et, une vision étatique de la monnaie.

Il convient de relever que, dans un arrêt en date du 22 octobre 2015, la Cour de justice de l'Union européenne a jugé que le bitcoin constitue un moyen de paiement contractuel (CJUE, 22 oct. 2015, aff. C-264/14, Skatteverket c/ David Hedqvist).

Par conséquent, si tous les utilisateurs d'une blockchain sont contractuellement d'accord pour se rémunérer en bitcoin, cela devient juridiquement possible. L'effet libératoire du paiement en bitcoin est contractuel et non pas légal.
Il n'est toutefois pas possible d'imposer un paiement en bitcoin en dehors de la communauté d'utilisateurs.

Relevons toutefois, la position intéressante du Professeur Nicolas MATHEY qui considère que ce qui caractérise véritablement une monnaie, ça n'est pas le fait qu'elle émane de l'Etat ou bien qu'elle ait cours légal, mais c'est en réalité l'acceptation par une communauté d'un bien comme moyen de se libérer d'une dette.
C'est selon lui « *la reconnaissance du pouvoir libératoire attaché au transfert d'un bien matériel ou immatériel qui devrait être le critère déterminant de la qualification de monnaie* ».
Il ajoute que : « d*ans la mesure où la monnaie est une institution sociale, il faut encore qu'une communauté, dont la taille peut être très variable, accepte généralement le paiement au moyen de*

[22] Le ministère de l'Économie et des Finances a lancé le 23 mars 2017 une consultation publique sur l'utilisation de la blockchain pour certains titres financiers (les minibons) et sur l'opportunité de légiférer : http://www.tresor.economie.gouv.fr/16101_consultation-publique-ordonnance-blockchain-applicable-a-certains-titres-financiers
[23] Pour consulter la synthèse des résultats de cette consultation : https://www.tresor.economie.gouv.fr/Articles/2017/08/31/synthese-de-la-consultation-publique-sur-la-transmission-de-certains-titres-financiers-au-moyen-de-la-technologie-blockchain

ce bien. Cela suppose que chacun accepte par ce moyen le paiement des dettes parce qu'il sait, ou, à vrai dire, parce qu'il croit, que d'autres accepteront à leur tour qu'il se libère de sa propre dette à leur égard par ce même moyen »[24].

C'est d'ailleurs dans cet esprit d'évolution que sont apparues en France, avec la Loi n° 2014-856 du 31 juillet 2014 relative à l'économie sociale et solidaire, les **monnaies locales complémentaires**, qui peuvent être émises et gérées par des personnes mentionnées à l'article 1er de cette loi (Article L311-5 du Code monétaire et financier). Contrairement à la cryptomonnaie, dont la confiance ne repose que sur la technologie, ces monnaies locales sont reconnues en France car fondées sur une économie locale, structurée par un système d'échange de biens et de services, à but non-lucratif, générant ainsi la confiance des autorités publiques et de la population.
Nous nous sommes interrogés, dans le cadre du projet BLOCKCAR, pour savoir s'il ne serait pas possible d'adosser une cryptomonnaie à une monnaie locale complémentaire légalement reconnue (voir sur ce point notre proposition au point II C 2).

C - LA GOUVERNANCE DU SYSTEME

Un service de covoiturage fonctionnant uniquement à partir d'un smart contract et d'une blockchain, sans aucun intermédiaire qui gouverne, administre le système, peut-il juridiquement s'envisager aujourd'hui en France ? Cette hypothèse semble à notre sens difficilement imaginable, à moins peut-être d'envisager que la gouvernance du système soit, elle-même, distribuée sur la blockchain.
Nous verrons que cela ne fonctionne pas et qu'une administration du système reste nécessaire. Nous proposerons une solution en ce sens pour le projet BLOCKCHAR.

1° The Code is Law. L'expérience malheureuse de The DAO

C'est sur un modèle de gouvernance autonome distribuée (DAO : Decentralized Autonomous organization) que les start-up Zooz et Slock.it travaillent actuellement.
Il s'agit du modèle le plus avancé du protocole blokchain d'Ethereum : automatiser grâce à un « super » smart contract la gouvernance d'une organisation, de manière distribuée, transparente et égalitaire.
La première DAO lancée par Slock.it sur Ethereum s'appelle « The DAO » et a fait couler beaucoup d'encre. Cette organisation décentralisée porte un 1er cas d'usage : une plateforme de crowfunding dont les règles de fonctionnement sont fixées dans un smart contract.
Son objet : collecter des fonds pour investir dans des projets divers. The DAO collectera près de 150 millions de dollars (soit la plus importante levée de fonds en crowfunding jamais réalisée) jusqu'au 17 juin 2016, date à laquelle, un pirate informatique parvient à détourner 3 millions d'ether (l'équivalent de 50 millions de dollars) contenus dans un smart contract. Après vérification, le réseau s'aperçoit que la faille ne provient pas de la blockchain en elle-même mais d'un bug dans le code informatique du smart contract.
La confiance dans le code informatique, sur laquelle l'organisation entière reposait jusque-là, s'effondre en un instant. Après des débats intenses entre ceux qui estimaient qu'il fallait respecter la philosophie de la blockchain (code is law) et, donc laisser partir le pirate avec les fonds, et ceux qui considéraient, au contraire, qu'il fallait intervenir pour casser la chaîne de blocs (par un fork)

[24] Article du Professeur Nicolas MATHEY de l'université Paris Descartes, Sorbonne Paris Cité : « La nature juridique des monnaies alternatives à l'épreuve du paiement » - Revue de Droit bancaire et financier n° 6, Novembre 2016, dossier
Voir également la décision rendue par la CJUE le 22 octobre 2015 considérant que bitcoin était bien une devise, au même titre que les devises traditionnelles et que l'échange de différents moyens de paiement ne pouvait donner lieu à TVA.

et permettre ainsi aux investisseurs de récupérer leurs fonds, le fork est finalement décidé à la majorité des nœuds et mineurs[25].
La communauté blockchain a pris conscience de l'absolue nécessité de renforcer la sécurité et la fiabilité du code informatique des smart contract (par des auditeurs de code notamment), étant rappelé qu'un code n'est en tout état de cause jamais infaillible.

Analyse juridique de The DAO
On comprend que le registre d'une blockchain publique n'est pas aussi immuable que certains l'affirment puisqu'un fork de la chaine de blocks, entraînant la suppression de toutes les informations enregistrées jusque-là, est possible s'il est décidé par la majorité du réseau (ou par une minorité influente).
Cet épisode pose également la question de la reconnaissance en droit d'une telle entité dépourvue de toute personnalité juridique et de sa responsabilité dans un cas comme celui-ci.

Comment qualifier juridiquement une telle organisation ? Si cette affaire n'a pas donné lieu à un contentieux, selon Thibault Verbiest[26], Avocat, un juge aurait probablement considéré The DAO comme une société créée de fait, soumise au même régime juridique que la société en participation et, relevant des articles 1871 et suivants du Code civil. Ainsi s'il avait fallu indemniser des victimes de The DAO, un juge aurait pu, sur ce fondement, éventuellement retenir la responsabilité illimitée et personnelle de ses associés fondateurs, à condition toutefois que ces derniers aient pu être identifiés, ce qui n'est pas le cas de The DAO (blockchain publique).

L'exemple de The DAO nous amène à envisager, pour le projet BLOCKCAR, une solution de gouvernance plus sécurisante au plan juridique, qu'une gouvernance autonome distribuée.

2° Proposition de régulation du service de covoiturage par une Société Coopérative d'Intérêt Collectif (SCIC)

Le service de covoiturage étant, par nature, un service à utilité sociale et solidaire, nous pourrions envisager de constituer une coopérative, relevant du régime juridique de la **Loi n° 47-1775 du 10 septembre 1947 sur la coopération, et de la** Loi n° 2014-856 du 31 juillet 2014 **relative à l'économie sociale et solidaire (ESS).**

Pourquoi une coopérative ?
On peut, tout d'abord, remarquer que les principes fondateurs de l'ESS ressemblent assez à ceux de la blockchain (tout au moins la blockchain publique) :
la volonté de développer un projet grâce à la collaboration d'une communauté d'acteurs et consacrant le principe d'égalité de droits entre les membres.
Une coopérative de type SCIC (d'intérêt collectif) semblerait, en outre, bien adapté à l'objet par nature social et collaboratif d'un service de covoiturage.
Une société coopérative d'intérêt collectif **pourrait ainsi être créée, sous la forme d'une société commerciale, dont l'objet** social serait la fourniture d'un service de covoiturage en France, à des fins d'utilité sociale.
Le but poursuivi serait ainsi l'intérêt de la collectivité des utilisateurs du service et non la distribution de bénéfices à destination d'un ou plusieurs acteurs isolés.
Le statut de SCIC pourrait également permettre à la SCIC de bénéficier de subventions publiques, au visa de l'article 15 de la loi du 31 juillet 2014, dès lors qu'elle porterait une innovation sociale grâce à la blockchain.

[25] Pour en savoir plus sur The DAO, voir l'article rédigé par l'avocat Simon Polrot « The DAO : Post Mortem » : https://www.ethereum-france.com/the-dao-post-mortem/
[26] Article de Thibault Verbiest : « Technologies de registre distribué (blockchain) : premières pistes de régulation

Enfin, la SCIC pourrait émettre et gérer une monnaie locale complémentaire, conformément à l'article 16 de la loi. Une cryptomonnaie pourrait ainsi être utilisée par la SCIC dans un cadre légal, sécurisant pour ses utilisateurs et permettant la désintermédiation bancaire.

Fonctionnement de la coopérative portant le service de covoiturage

Une gouvernance démocratique, définie par des membres fondateurs et actée dans des statuts, fixerait les règles de fonctionnement de la coopérative, mais également de la blockchain, du smart contract, établirait les conditions d'utilisation du service, d'adhésion à la structure (identification obligatoire, nombre minimum de covoiturage réalisé, réputation), de perte de la qualité d'adhérent, ainsi que les droits et contribution de ses adhérents.
Le service serait accessible aux utilisateurs grâce à un site internet relié à la blockchain.
Chaque utilisateur du service pourrait, par principe, devenir adhérent de la coopérative.

Conformément aux principes qui gouvernent une coopérative, chaque adhérent de la coopérative serait associé et disposerait d'une voix lors de l'assemblée générale (selon le principe égalitaire : une personne = une voix).
La SCIC pourrait également accueillir dans son capital social, des tiers non sociétaires (dans la limite légale de 20 % de son chiffre d'affaires). Les collectivités territoriales, leurs groupements et les établissements publics territoriaux pourraient également détenir ensemble jusqu'à 50 % du capital.
Cette coopérative devrait toutefois obtenir l'agrément « entreprise solidaire d'utilité sociale » par le préfet dans les conditions de l'article 11 de la loi du 31 juillet 2014.

Essai de projection
L'objectif recherché par la coopérative serait d'être, par principe, ouverte à tous et que tous les utilisateurs du service de covoiturage (passagers et conducteurs) deviennent, par un système d'incitation (on reprendrait ici la logique de l'incitation d'une blockchain), adhérents de la structure et contribuent ensuite, par tous moyens, à la bonne réalisation du service de covoiturage.
L'incitation à devenir adhérent pourrait par exemple consister pour un passager, en une prise en charge par la coopérative d'une partie de l'indemnité devant être verser à un conducteur, et destinée à compenser les frais d'essence, de péage, d'assurance, d'entretien du véhicule[27].
Les adhérents de la coopérative pourraient ensuite devenir membres de différents collèges constitués au sein de la coopérative (on peut imaginer plusieurs collèges possibles, tels que le collège des fondateurs, le collège des mineurs, le collège du smart contract auditeur de code, le collège des oracles, le collège de gestion des sinistres, etc).
Certains adhérents pourraient devenir des nœuds du réseau (héberger le registre), participer au protocole de vérification des informations à enregistrer sur la blockchain.
La coopérative pourrait aussi choisir de faire appel à des oracles (des tiers professionnels extérieurs à la coopérative dont la mission consisterait à recueillir certaines informations à l'extérieur de la blockchain). Ces professionnels pourraient également être des prestataires de service de confiance qualifiés, au sens du règlement eIDAS[28].
Enfin, la coopérative pourrait demander à l'ANSSI (l'Agence National de Sécurité des Systèmes d'Information) de certifier la blockchain BLOCKCAR utilisée pour réaliser le service de covoiturage ou bien de qualifier le service dans son ensemble (trois niveaux de qualification sont possibles : élémentaire, standard et renforcé permettant de résister à des attaques de niveau croissant). La certification ou la qualification permettrait d'attester d'un certain niveau de sécurité et de confiance dans la technologie ou dans le service.

[27] Le conducteur, non-professionnel du transport, ne peut légalement réaliser de bénéfice à partir de l'activité de covoiturage. Ainsi, il ne peut percevoir du passager, qu'une indemnité destinée à compenser les frais d'essence, de péage, d'assurance, d'entretien du véhicule, etc, calculée conformément au barème fiscal des frais kilométriques.
[28] Le *Règlement « eIDAS »* n°910/2014 du 23 juillet 2014 a pour objet d'accroître la confiance dans les transactions électroniques au sein du marché intérieur.

Responsabilité de la coopérative
La coopérative, dotée de la personnalité morale, propriétaire de la blockchain ainsi que du service de covoiturage, pourrait engager sa responsabilité juridique et indemniser, le cas échéant, un utilisateur victime d'une défaillance du service (ex : une faille dans un smart contract).

D - QUELLE SECURITE JURIDIQUE POUR LES OPERATIONS REALISEES DANS UN SMART CONTRACT ET ENREGISTREES SUR LA BLOCKCHAIN ?

Sous ce titre, nous tenterons de répondre aux trois questions juridiques suivantes :

- Quelle qualification juridique donnée au smart contract ? Est-il réellement une simple modalité d'exécution d'un contrat ou bien peut-il être un contrat au sens du code civil ?
- Le code informatique d'un smart contract ne devrait-il pas être validé par des juristes ?
- Quelle force probante peut être donnée à l'enregistrement d'une information sur la blockchain ? ou dit autrement, cet enregistrement permet-il de prouver l'information, la bonne exécution de l'opération du smart contract ?

1° La qualification juridique du smart contract

Rappelons, tout d'abord, ce qu'est avant tout un smart contract : un programme informatique qui permet de déclencher l'exécution automatique d'actions, dès la survenance de conditions prédéfinies.
Dans le silence des textes et de la jurisprudence, une question se pose : quelle qualification juridique donner à ce type de programme ? Peut-il s'agir d'un contrat, au sens juridique du terme ?
Il convient à notre sens de distinguer deux hypothèses :

- **Cas où le smart contrat ne peut pas être un contrat**

La première hypothèse envisagée est celle où deux parties concluent un contrat juridique à l'extérieur de la blockchain et décident de recourir à un smart contract pour automatiser l'exécution d'une ou plusieurs conditions de ce contrat (le paiement à réception d'un produit par exemple), puis d'enregistrer ce smart contract et son exécution dans une blockchain.
Dans cette hypothèse, le smart contract n'est qu'une modalité technique d'exécution du contrat juridique. Il a pour objet d'automatiser l'exécution, d'augmenter la force exécutoire du contrat juridique, et donc éviter d'éventuelles inexécutions (ex : dès réception de la marchandise, l'acheteur paye automatiquement, grâce au smart contract, la somme due au vendeur, par libération des fonds séquestrés).

- **Cas où le smart contract pourrait être un contrat**

Il s'agit d'envisager ici l'hypothèse où il n'y aurait pas de contrat conclu à l'extérieur. Certains auteurs se sont interrogés sur le sujet[29]. Toutefois, sur la base des principes actuels du Code civil, qualifier de contrat un smart contract paraît difficile à retenir. Rappelons les principes de droit :

Formation
Le premier principe est qu'un contrat se forme, sauf exception (contrats solennels et réels) par le seul échange des consentements des parties (article 1109 du Code civil).
Le contrat est donc un accord de volontés, et plus précisément, la rencontre entre une offre et une acceptation, par lesquelles les parties manifestent leur volonté de s'engager (articles 1110 et 1113

[29]Jérôme Giusti, Avocat : « Les « smart contract » sont-ils des contrats ? » le 27 mai 2016 – blog : https://jeromegiustiblog.wordpress.com/2016/05/27/les-smart-contracts-sont-ils-des-contrats/

du Code civil). L'article 1102 précise que chacun est libre de déterminer le contenu et la forme de ce contrat dans les limites fixées par la loi.
Ainsi, des parties pourraient, en principe, librement décider qu'un smart contract, tant dans sa forme que son contenu (rédigé en code), serait le contrat.

Négociation
Le Code civil prévoit cependant que les contrats doivent être négociés de bonne foi (article 1104). L'exigence de négociation d'un contrat paraît incompatible avec un smart contract. En effet, un smart contract ne peut que programmer des évènements prédéfinis à exécuter. Il ne laisse aucune place à la négociation, à moins d'envisager le cas où les parties négocieraient librement le programme du smart contract, c'est-à-dire les conditions et exécutions, ce qui semble difficile à imaginer.
Le smart contract serait alors un contrat d'adhésion, c'est-à-dire, selon l'article 1110 du code civil, un contrat dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance par l'une des parties.
Si le législateur reconnaît la validité juridique des contrats d'adhésion, une limite importante a récemment été consacrée par la Réforme du Droit des obligations (Ordonnance du 10 février 2016) : toute clause qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite.
Par conséquent, le smart contract ne devrait comporter aucune condition créant un déséquilibre significatif entre les droits et obligations des parties, à peine de nullité.

Eléments essentiels du contrat
De plus, les textes civils précisent que l'offre de contrat doit comprendre les éléments essentiels du contrat envisagé. Un smart contract devrait ainsi retranscrire cette offre et, donc tous les éléments essentiels du contrat envisagé, à moins que l'offre contractuelle ne s'exprime sur un autre support relié électroniquement au smart contract (un site internet par exemple).
Au demeurant, on voit mal comment un smart contract pourrait retranscrire les mentions légales obligatoires que doivent comporter les contrats conclus entre professionnels et consommateurs (même si cela est en théorie possible puisque le smart contract peut contenir des données en clair).

Intelligibilité
Se pose également la question de la compréhension du langage informatique du smart contract par les utilisateurs. Le législateur exige que le consentement des parties soit éclairé et non empreint d'erreur, dol ou violence.
Comment des parties, profanes en code informatique, pourraient-elles donner un consentement éclairé, non entaché d'erreur ? Une exacte traduction du code du smart contract en langage français dans le smart contract ou avant la conclusion, semblerait nécessaire.

Manifestation de volonté
Enfin, un smart contract en tant que contrat supposerait que les parties aient pu manifester leur volonté de s'engager. Selon l'article 1113 du Code civil, cette volonté peut résulter d'une déclaration ou d'un comportement non équivoque de son auteur.
Mais comment cette volonté peut-elle se manifester si l'exécution d'un smart contract se déclenche sans intervention humaine ? Peut-être par un opt-in à partir d'un site internet relié au smart contract ?
La manifestation de volonté des parties pourrait aussi s'exprimer grâce au moyen cryptographique asymétrique utilisé par exemple sur Bitcoin (signature électronique par clé privée et clé publique)[30] ;

En matière de commerce électronique, la loi exige que le consommateur ait eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation. L'auteur de l'offre doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée. On voit ainsi mal, pour ces contrats particulièrement règlementés, comment un smart contract pourrait traduire le respect de ces obligations légales.

Clauses contractuelles
La richesse des clauses contractuelles pouvant exister ne peut, selon nous, être retranscrite dans un smart contract.

Nullité
Enfin, si le contrat est le smart contract et si ce dernier est enregistré sur le registre immuable de la blockchain, comment assurer son effacement rétroactif en cas de nullité prononcée par un juge ?

Ainsi, qualifier le smart contract de contrat ne semble pas évident.

Dans le cadre du projet BLOCKCAR, nous retiendrions la première hypothèse : le smart contract comme moyen d'exécuter certaines dispositions du contrat de covoiturage passé entre deux utilisateurs et conclu à l'extérieur de la blockchain.
Ce contrat ainsi que le contrat d'utilisation du service entre l'utilisateur et BLOCKCAR seraient conclus à partir du site internet de la coopérative par la mise en place d'opt-in (une case à cocher obligatoirement par l'utilisateur avant toute réservation d'un trajet de covoiturage).

2° La validation du code informatique du smart contract

Nous avons pu constater, en essayant de traduire un service de covoiturage dans un smart contract, que l'exercice n'est pas simple. Construire un smart contract nécessite de savoir écrire du code informatique mais pas uniquement.
A notre sens, la mise en place systématique de testeurs, d'auditeurs de code semble indispensable afin d'éviter que ne se reproduise l'affaire The DAO. Rappelons que, plus le smart contract est complexe, plus les risques de bug sont grands.
Nous irons même plus loin, la place du juriste ou de l'avocat sachant lire et écrire le code informatique, nous semble justifiée afin de s'assurer d'une part, que les évènements programmés dans le smart contract sont conformes aux règles de droit et contrats en vigueur, et, d'autre part qu'ils sont respectueux de la volonté et des droits des utilisateurs (que le code est la retranscription exacte et fidèle d'une décision humaine). D'ailleurs, tout ne peut pas, à notre avis, être codé dans un smart contract, comme par exemple ce qui relève de l'appréciation subjective de l'une des parties ou encore les cas de force majeure. Le juriste devrait également être le garant de l'exacte retranscription du langage français en langage informatique.
Dans notre cas d'usage, le ou les smart contract serai(en)t rédigés par des développeurs et juristes confirmés, puis testés et audités avant d'être mis en application. Le collège smart contract de la coopérative serait en charge de piloter cette partie du service.

3° La force probante de l'enregistrement d'une information sur la blockchain

La blockchain pourrait avoir un autre intérêt que celui de permettre l'automatisation d'exécutions conditionnelles dans un smart contract ; elle pourrait prouver l'existence d'une information, la réalisation d'une opération, à un instant précis, par l'enregistrement sur le registre de son empreinte cryptographique.

Rappelons qu'en principe, c'est l'empreinte d'une information (le hash), et non le document en tant que tel, qui est enregistré sur la blockchain. L'acte original qui sous-tend l'information (comme par exemple, un contrat) sera quant à lui être conservé à l'extérieur de la blockchain, dans des conditions permettant de garantir sa conservation et son intégrité (archivage à valeur probatoire). Un lien logique sera également assuré entre l'empreinte enregistrée sur la blockchain et l'acte original conservé électroniquement (ce lien pourrait consister en l'apposition du hash sur le document original).
L'enregistrement de l'information sera horodaté sur la blockchain, lui conférant date certaine.

En cas de contestation devant un juge, un utilisateur pourrait-il valablement invoquer la preuve du paiement enregistré sur une blockchain ?
Cette preuve d'enregistrement serait-elle recevable en justice ? et si oui, quelle valeur probante un juge pourrait-il donner à cette information ?

Absence de règles spécifiques
L'Ordonnance du 28 avril 2016 relative aux minibons qui expérimente la blockchain fait référence à « *un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations* ».
L'Ordonnance renvoie toutefois à un décret pris en Conseil d'Etat pour fixer les conditions de sécurité de ce dispositif. Ce décret n'ayant pas encore été adopté, il n'est pas possible en l'état, de connaître les conditions juridiques qui permettront d'établir l'authentification des opérations enregistrées sur une blockchain et leur valeur probatoire. En l'absence de règles propres à la blockchain, il convient de raisonner à partir des règles de preuve actuellement en vigueur.

Droit commun de la preuve
Rappelons, tout d'abord, le principe de droit selon lequel, hors le cas où la loi en dispose autrement, la preuve d'un acte juridique peut être apportée par tout moyen lorsqu'il ne dépasse pas 1 500 €.
Cette règle pourrait être invoquée par l'utilisateur pour démontrer le paiement d'un trajet de covoiturage (puisque le montant serait inférieur au seuil).
Mais si la valeur de l'acte était supérieure à 1 500 €, il faudrait alors le prouver par un écrit[31] (sauf en matière commerciale où la preuve se fait par tout moyen).

Définition d'un écrit
Le Code civil définit l'écrit comme une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support (article 1365 du Code civil).
Une empreinte cryptographique, un smart contract constituent dès lors, au sens juridique, des écrits et, plus exactement, des écrits électroniques.
Précisons que le législateur a consacré le principe de neutralité technologique entre un écrit papier et un écrit électronique, principe qui pourrait être invoqué par l'utilisateur.
Mais pour avoir une force probante convaincante devant un juge, cet écrit électronique doit être signé électroniquement.

A quelles conditions un écrit électronique peut-il avoir la même force probante qu'un écrit papier signé ?
S'agissant des écrits signés (les écrits parfaits), le principe d'équivalence ne joue parfaitement qu'à la condition suivante : « *l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* » (article 1366 du code civil).

[31] Exception à l'exception : en cas d'impossibilité matérielle ou morale de se procurer un écrit, Il peut être suppléé à l'écrit par l'aveu judiciaire, le serment décisoire ou un commencement de preuve par écrit corroboré par un autre moyen de preuve (article 1361 C. civ.)

Le Code civil précise ensuite à l'article 1367 que lorsque la signature d'un écrit est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.

Le Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique (remplaçant le Décret du 30 mars 2001 suite à l'entrée en vigueur du Règlement Européen Eidas du 23 juillet 2014[32]) pose les conditions permettant de qualifier un procédé technique d'identification comme étant « fiable ». Si ces conditions sont remplies, l'écrit électronique est alors présumé avoir la même force probante qu'un écrit papier signé de manière manuscrite.
Cependant, si le procédé de la signature électronique ne remplit pas les conditions de fiabilité posées par le Décret, l'écrit électronique n'en est pas pour autant irrecevable en justice. Il est admissible mais ne bénéficie pas de la présomption d'équivalence (il constitue alors un simple commencement de preuve par écrit).

A ce jour, il nous semble que seule une signature électronique basée sur la technique de la cryptographie asymétrique (clé privée / clé publique) pourrait permettre de se prévaloir de la présomption de fiabilité posée par l'article 1367 du Code civil. Cette signature doit toutefois être accompagnée d'un certificat électronique qualifié : un document électronique qui atteste du lien entre les données de vérification de signature électronique et le signataire du document. Ce certificat est délivré par un intermédiaire : un prestataire de service de certification.
Le certificat électronique permet d'établir le lien entre le signataire d'un acte et la clé publique que ce dernier utilise pour crypter l'acte.

Force probante de l'écrit électronique signé par la technique de cryptographie asymétrique, et dont l'empreinte est enregistrée sur la blockchain
Rappelons que la cryptographie utilisée sur la blockchain est précisément une cryptographie asymétrique (signature électronique et hachage).
Par conséquent, la présomption de fiabilité d'une information enregistrée sur la blockchain pourrait être invoquée devant un juge, si la cryptographique de signature électronique utilisée est dite « qualifiée » et si le dispositif de vérification de signature électronique repose sur un certificat électronique qualifié, au sens du Décret de 2017 et du Règlement Eidas.

Dans le cadre du projet BLOCKCAR, l'enregistrement horodatée sur la blockchain dans les conditions que nous venons de voir, pourrait faciliter la preuve de l'exécution des opérations du service de covoiturage et donc, dans une certaine mesure, réduire le contentieux existant entre les utilisateurs.

E - LA PROTECTION DES DONNEES PERSONNELLES DES UTILISATEURS

Une règlementation française et européenne particulière s'applique aux traitements automatisés de données à caractère personnel, contenues ou appelées à figurer dans des fichiers (Loi Informatique et libertés n° 78-17 du 6 janvier 1978 et Règlement n°2016/679 du Parlement européen et du Conseil entré en application le 25 mai 2018 « RGDP »).
La question se pose dès lors de savoir si des données personnelles peuvent être enregistrées sur le registre de la blockchain et, si tel est le cas, d'analyser les conséquences possibles au plan juridique.

[32] Le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

Définition de la donnée personnelle
Rappelons tout d'abord la définition d'une donnée personnelle : toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

La CNIL a publié le 24 septembre 2018 ses premières réflexions et analyses sur la blockchain :
L'autorité de contrôle précise que deux types de données personnelles peuvent être enregistrées sur une blockchain :
-l'identifiant des participants et des mineurs : chaque participant/mineur dispose d'une clé publique, ce qui permet d'assurer l'identification de l'émetteur et du destinataire d'une transaction ;
-des données complémentaires, inscrites dans une transaction (ex : diplôme, titre de propriété). Si ces données sont relatives à des personnes physiques, éventuellement autres que les participants, directement ou indirectement identifiables, il s'agit de données à caractère personnel.

La qualification des acteurs d'une blockchain
Selon la CNIL, le modèle décentralisé de gouvernance des données de la technologie blockchain et la multiplicité des acteurs intervenant dans le traitement de la donnée complexifient la définition des rôles de chacun.
C'est ainsi que dans de nombreux cas, le participant personne morale ou agissant dans un cadre professionnel (la personne qui décide de l'enregistrement d'une donnée sur la Blockchain) sera considéré comme un responsable de traitement dans la mesure où il décide de la finalité et des moyens du traitement de données.
Ex : le notaire qui enregistre le titre de propriété de son client dans une blockchain.
Le mineur, qui se limite à valider les transactions que lui soumettent les participants et n'intervenant pas sur l'objet de ces transactions, ne sera, quant à lui, pas qualifié de responsable de traitement.
Il pourra toutefois, dans certains cas, être qualifié de sous-traitant des données personnelles : lorsqu'il vérifie que la transaction respecte des critères techniques (par exemple un format et une certaine taille maximale, et que le participant est en capacité, vis-à-vis de la chaîne, d'effectuer sa transaction).
S'agissant des smart contract, le concepteur de l'algorithme pourra être un simple fournisseur de solution ou, lorsqu'il participe au traitement, être qualifié de sous-traitant ou de responsable de traitement en fonction de son rôle dans la détermination des finalités.
Lorsqu'un groupe d'organismes décident de mettre en œuvre un traitement sur une blockchain pour une finalité commune, il conviendra de définir en amont qui sera le responsable de traitement (qui prend les décisions). A défaut tous les membres du groupe seront qualifiés de responsables de traitement.

Incompatibilité potentielle entre blockchain et certains principes du RGPD ?
On peut s'interroger sur la comptabilité de certaines blockchain avec deux grands principes prévus par le RGPD.

-Le Règlement européen consacre le principe d'interdiction de **transfert de données personnelles en dehors de l'Union Européenne** (UE), à moins que le pays ou le destinataire n'assure un niveau de protection suffisant. Un tel transfert hors de l'UE nécessiterait, par ailleurs, le consentement express de la personne concernée.

L'enregistrement quasi-simultané du registre par les nœuds du réseau d'une blockchain publique, situés aux quatre coins de la planète est-il compatible avec ce principe de non-transfert des données personnelles en dehors de l'Union Européen ?

-Un second principe important est prévu par le RGPD : celui du **droit à l'oubli.** Chaque personne a le droit de demander l'effacement de ses données s'il dispose d'un motif légitime.
Comment concilier ce principe de droit à l'oubli avec l'une des caractéristiques majeures de la blockchain à savoir : l'intangibilité du registre ?
Il est techniquement impossible de faire droit à la demande d'effacement de la personne concernée lorsque des données sont inscrites dans la blockchain.

La CNIL invite les acteurs à s'interroger dès le départ, avant la conception du système, sur l'opportunité de recourir à une blockchain pour la mise en œuvre de traitement de données personnelles et s'il ne vaut pas mieux opter pour une autre technologie.
Les acteurs devront aussi s'interroger sur le type de blockchain à utiliser : publique, à permission, ou privée, ce choix pouvant impacter significativement, à la hausse ou à la baisse, les risques sur les droits et les libertés des personnes. La CNIL invite les acteurs à privilégier lorsque cela est possible, les blockchains à permission.

Enfin, il convient de noter que la réalisation d'une analyse d'impact et l'obtention d'une autorisation de la CNIL peuvent dans certains cas s'avérer obligatoires.

Dans le cadre du projet BLOCKCAR, et par mesure de sécurité, la coopérative réaliserait avant tout traitement, une analyse d'impact afin d'analyser la nécessité et la proportionnalité du système projeté et solliciterait, au besoin, une autorisation de la CNIL.
Elle veillerait, en tout état de cause, à ce qu'aucune donnée personnelle ne figure en clair sur le registre de la blockchain et dans le smart contract.
Seules des données nécessaires (minimisation) et ayant fait l'objet d'un engagement cryptographique seraient enregistrées.
Le niveau de décentralisation du réseau serait européen.
La qualification des acteurs serait clairement définie (qui est responsable de traitement et qui est sous-traitant) et des contrats écrits précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD seraient conclus avec chaque sous-traitant.
Enfin, une politique d'utilisation des données personnelles serait rédigée par la coopérative et communiquée à chaque nouvel utilisateur avant toute collecte de ses données, afin de recueillir son accord express et préalable, avant tout traitement.

CONCLUSION

Il semble donc possible de désintermédier, au plan technologique, un service de covoiturage grâce à une blockchain et un smart contract.

La blockchain et le smart contract pourraient permettre :

-de supprimer certains intermédiaires
-d'automatiser et d'enregistrer l'exécution de services
-d'augmenter le niveau de confiance des utilisateurs, au plan de la sécurité informatique

Toutefois, la désintermédiation ne saurait être totale (l'exemple de The DAO le démontre). Le maintien d'une gouvernance et de tiers de confiance nous semble indispensable.
Le recours aux prestataires de services de confiance qualifiés pourrait être intéressant. L'intervention de l'avocat et du juriste semble aussi tout à fait pertinente.
Il est par ailleurs probable que de nouveaux tiers de confiance, d'un genre nouveau, fassent leur apparition. L'Oracle d'Ethereum en est un parfait exemple.

Cette étude montre également les nombreuses questions juridiques qui se posent dans le cadre d'un projet blockchain : le droit applicable, la monnaie virtuelle utilisée, la gouvernance, l'automatisation des services par le smart contract, la responsabilité, la force probante des informations enregistrées, la protection des données personnelles. D'autres questions juridiques se posent encore, comme celle de la vérification de l'identité des utilisateurs d'une blockchain (comme vérifier que l'utilisateur A est bien Monsieur A ?)[33]. Chacune de ces questions mériterait une étude à part entière, d'autant plus délicate que le droit est ici en cours d'évolution.
L'Etat français et les instances européennes montrent un intérêt très net, à l'égard de cette nouvelle technologie, qu'ils semblent vouloir expérimenter avant probablement de l'encadrer.
Si aujourd'hui, la plupart des projets blockchain ne sont pas encore matures, certains devraient émerger dans les années à venir. Il sera alors intéressant de les étudier au plan juridique afin d'affiner l'analyse juridique.

A ce stade et, en l'absence de reconnaissance légale de la technologie, de jurisprudence établie, le travail d'analyse sur la blockchain et le smart contract est certes, très intéressant, mais ne peut être qu'exploratoire.

NUMETIK AVOCATS
Elise Guilhaudis

33 Sur cette question, on peut se référer aux critères d'évaluation de la conformité au règlement eIDAS , fixés par l'ANSSI le 3 janvier 2017. Des solutions numériques commencent également à émerger. Voir pour exemple : https://www.dhimyotis.com/products.php

Bibliographie

-La blockchain décryptée, Chronique d'une révolution – Blockchain France – mai 2016
-Série trimestrielle Réalité Industrielle des Annales des Mines : « Blockchain et smart contract : des technologies de la confiance » d'août 2017 publié avec le soutien de l'Institut Mines-Télécom
-Henri d'Agrain « *Le protocole Blockchain et ses usages* » Note de synthèse rédigée en janvier 2016 par le Délégué Général du CIGREF et ancien Directeur Général du Centre des Hautes Etudes du Cyberespace
-Hubert de Vauplane, Avocat « La Blockchain et la loi » RTDF n°1 2016 Chronique Digitalisation et Droit financier
-Table ronde EDHEC « Blockchain et smart contract : enjeux technologiques, juridiques et business – cahiers de droit de l'entreprise n°2 – mars-avril 2017
-Thibault Verbiest « Technologie de registre distribué (blockchain) : premières pistes de régulation » - Revue Lamy Droit de l'Immatériel n°129 du 1er août 2016
-Nicolas Mathey « La nature juridique des monnaies alternatives à l'épreuve du paiement » Professeur à l'université Paris Descartes, Sorbonne Paris Cité - Revue de Droit bancaire et financier n° 6, Novembre 2016, dossier
- Célia ZOLYNSKI « Fintech - Blockchain et smart contract : premiers regards sur une technologie disruptive » Revue de Droit bancaire et financier n° 1, Janvier 2017, dossier 4
-Yaël Cohen-Hadria, Avocate « Blockchain : révolution ou évolution ? La pratique qui bouscule les habitudes et l'univers juridique » - Dalloz IP/IT 2016 p.537
-Yves Moreau et Chloé Dornbierer « Enjeux de la technologie de blockchain » - Recueil Dalloz 2016 p.1856
-Thiebald Cremers « La blockchain et les titres financier : retour vers le futur" Issu de Bulletin Joly Bourse - 01/06/2016 - n° 06 - page 271
-Isabelle Renard, Avocat : « Fonctionnement de la Blockchain – Compatibilité avec un environnement réglementé : que peut-on et que doit-on réglementer dans une Blockchain ? Revue de Droit bancaire et financier n° 1, Janvier 2017, dossier 3
-Sébastien Drillon, Avocat : « La révolution Blockchain - La redéfinition des tiers de confiance » RTD Com. 2016 p.893
-Olivier Hielle : « La technologie Blockchain : une révolution aux nombreux problèmes juridiques » - Dalloz actualité 31 mai 2016
-Pierre Storrer, Avocat : « Pour la reconnaissance du KYC digital » - Chronique Digitalisation et droit financier - RTDF N° 2 - 2016
-Xavier Delpech « Le régime juridique des bons de caisse modernisé » Dalloz actualité 10 mai 2016

Webographie

-Gautier Marin-Dagannaud, du 3 juin 2016 « Bitcoin, première implémentation de la blockchain » - Site Ethereum France : https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/
-Jérôme Giusti, Avocat : « Les « smart contract » sont-ils des contrats ? » le 27 mai 2016 – blog : https://jeromegiustiblog.wordpress.com/2016/05/27/les-smart-contracts-sont-ils-des-contrats/
-Simon Polrot, Avocat « The DAO : Post Mortem » du 24 janvier 2017 - Site de Ethereum France: https://www.ethereum-france.com/the-dao-post-mortem/
-Félix Tréguer du 19 septembre 2012 : « Vers un contrat social du cyberespace ? » We the Net : https://www.wethenet.eu/2012/09/vers-un-contrat-social-pour-le-cyberespace/
-Le Raconteur : https://www.raconteur.net/business/the-future-of-blockchain-in-8-charts - Article du 27 juin 2016
-« L'adoption massive de la blockchain est prévue pour 2025 » du site l'Usine Digitale: http://www.usine-digitale.fr/article/l-adoption-massive-de-la-blockchain-est-prevue-pour-2025.N399357 - Article du 27 juin 2016 : Article d'Hubert de Vauplane, Avocat du 15 octobre 2016 – compte LinkedIn : « les applications pratiques de la blockchain » : https://fr.linkedin.com/pulse/les-applications-pratiques-de-la-blockchain-hubert-de-vauplane
-Simon Polrot Avocat, du 13 septembre 2016 : « Les Oracles, lien entre la blockchain et le monde » - Site Ethereum France : https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/
-Simon Polrot Avocat, du 23 septembre 2016 : « Déconstruction du terme smart contract » - Site Ethereum France : https://www.ethereum-france.com/deconstruction-du-terme-smart-contract/
-Le White Paper (Livre Blanc) d'Ethereum : la description originale du projet Ethereum écrite par Vitalik Buterin : traduction française – Site d'Ethereum France: https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/
-Simon Polrot Avocat du 14 février 2016 « Qu'est-ce qu'Ethereum ? » Site de Ethereum France : https://www.ethereum-france.com/quest-ce-que-lethereum/
-Maryse Gros avec IDG News Service, du 09 Mai 2017 – Site de le Monde informatique : http://www.lemondeinformatique.fr/actualites/lire-la-fondation-linux-modelise-l-automatisation-de-contrats-sur-blockchain-68140.html
-Clément Lesaege - Workshop tenu sur le site GitHubGist : https://gist.github.com/anonymous/c752ca1ec20a32a5bb5501e52bcbf78d
-Sébastien Castiel du 25 mai 2016 « Construire un smart contract » Site d'Ethereum France : https://www.ethereum-france.com/ecrire-une-dapp-pour-ethereum-1-smart-contract/

Textes

-Règlement Européen « eIDAS » n°910/2014 du 23 juillet 2014 a pour objet d'accroître la confiance dans les transactions électroniques au sein du marché intérieur
-Règlement n°2016/679 du Parlement européen et du Conseil entré en vigueur le 27 avril 2016 « RGDP ».

-Code civil : articles 1104 – 1010 – 1013 – 13-65 à 1367 - 1871
-Loi Informatique et libertés n° 78-17 du 6 janvier 1978
-Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse - JO n°0101 du 29 avril 2016
-Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique

Jurisprudence :
-Arrêt de la Cour de cassation : 1ère ch. civ. 3 novembre 2016, N° de pourvoi: 15-22595
-Arrêt CJUE du 13 mai 2014 aff C 131/12 Google Spain SL Google Inc c/Agencia Espanola de Proteccion de Datos
-Arrêt CJUE le 22 octobre 2015 aff C-264/14 Skatteverket c/ David Hedqvist