“Internet rêve-t-il d’or électronique ?”

—

La blockchain, moteur de la quatrième révolution industrielle ?

Jules WACQUIER - ECDE - Master Marketing Communication & E-business - Promotion 2020

Table des matières

Introduction

Dans un monde où internet a infiltré toutes les strates de nos sociétés, nous sommes désormais en pleine crise de confiance vis-à-vis de celui-ci. De grands bouleversements sociétaux, économiques et écologiques sont en marche, la guerre de l’information et de l’influence fait rage, et nous, simples humains, avons de plus en plus de mal à suivre.

Notre cerveau est acculé jour après jour, d’un tsunami d’informations, tout s’accélère, et il y ne reste que peu de place pour le temps long. Notre communication, nos méthodes de travails, nos organisations se digitalisent, se rationalisent, se centralisent autour d’acteurs de plus en plus puissants. Nous plaçons la majeure partie de notre vie privée avec ces mêmes acteurs, notre confiance est elle-même centralisée en ce petit nombre d’entités.

Cependant, une technologie promet de nous émanciper de l’obligation de céder aux chants des sirènes avides de données pour profiter d’outils performants et le plus souvent gratuits.

Une technologie distribuée et décentralisée, profitant des infrastructures d’internet pour offrir une confiance non pas dépendante d’acteurs unique, mais décentralisée : la blockchain[1].

La première révolution industrielle à construire les bases de notre société capitaliste et mondialisée, la deuxième a été un catalyseur de ce modèle de société, développant la consommation des ménages et voyant naitre de gigantesques entreprises, enfin, la troisième sonne l’avènement d’internet et les GAFAM. Et si une quatrième révolution était en marche, cachée dans la troisième, s'apprêtent à bouleverser l’ordre établi ?

Dans ce mémoire, nous allons tout d’abord analyser les idéologies, le fonctionnement et les controverses liés à la technologie blockchain. Nous enchainerons sur des études de cas concrets, nous éloignant du focus financier. Enfin, nous terminerons sur les mutations sociétales pouvant découler de l’utilisation massive de cette technologie.

[1] Chaîne de blocs

Origines, fonction et controverses

Dans ce chapitre, nous allons découvrir comment cette technologie a émergé.

Les inventions sont parfois accidentelles, mais les innovations, elles, sont motivées par une idée. Et des idées, il y en a beaucoup à l’origine de cette technologie, laissez-moi tout d’abord vous partager les fondations idéologiques. Je vous présenterai ensuite le fonctionnement de base de cette technologie avec sa première implémentation concrète : le Bitcoin. Enfin, pour clore ce chapitre, je vous présenterai les limites actuelles de la technologie Blockchain telle qu’elle est implémentée aujourd’hui.

Motivations politiques

Si l'on veut comprendre l'essence de la technologie blockchain, il faut tout d'abord se tourner vers ce qui l'a faite émergée, son objectif, et ses inspirations aussi bien idéologiques que politiques. Car au-delà de l’objet technologique complexe, de la spéculation ou du “buzzword” [2], c’est avant tout un changement idéologique.

Échecs du système centralisé

La crise financière issue des subprimes a fait de sérieux dégâts au système financier mondialisé, mettant en évidence les dérives des institutions financières vis-à-vis de leurs investissements de l’épargne des contribuables dans des produits financiers complexes. Les mécanismes de régulations et les agences de notations sont passés à côté de l’émergence de tels produits financiers, conduisant à une intoxication du système et à la faillite ou la nationalisation de certaines banques.

Cette crise a eu un impact sur la confiance du peuple envers les institutions financières. De nombreux épargnants et entreprises ont perdu beaucoup dans cette crise.

Cette crise de confiance du peuple envers les institutions publiques et démocratiques se matérialise dans l’incapacité de ces mêmes institutions à intervenir sur les marchés financiers. De plus en plus centralisé, le pouvoir décisionnel est incapable de répondre aux nouveaux enjeux économiques.

C'est de ce constat d’échec qu'est née la technologie blockchain : puisque le système, économique et politique, intervenant en tant que tiers de confiance dans une économie globalisée, ne remplit pas son contrat de confiance, il faut un système d’échange de valeur automatisé et incorruptible, sans dépendance à un état ou une banque.

C’est en 2008, qu’un mystérieux personnage, Satoshi Nakamoto, publia sur le site bitcoin.org un manifeste : *“Bitcoin: À Peer-to-Peer Electronic Cash System”* , annonçant ce fameux principe d’échange de valeur reposant sur une technologie appelée aujourd’hui blockchain.

Cette idéologie de non-dépendance distillée dans ce document n’est pas apparue du néant, elle prend racine de deux courants de pensée politiques majeurs que sont **le libertarisme et le cryptoanarchisme**.

[2] Mot à la mode

Libertarisme : hors de contrôle d’un état ou des lois

Le libertarisme est un courant politique prônant le droit à la propriété privée sur soi-même ou sur ses acquisitions comme droit inaliénable. Celui-ci repose sur un état dit régalien, se contentant de la police, la justice et l’armée. Il prend sa base sur quatre piliers : la libre disposition de soi, la réparation, **l'appropriation originelle et la juste circulation**.

C'est sur ces deux derniers principes que se repose la blockchain.

L'appropriation originelle est à mettre en parallèle du système de récompense utilisé dans la blockchain. Dans la monnaie numérique Bitcoin par exemple, celui qui va apporter son aide pour la sécurisation du réseau monétaire recevra une récompense créée spécialement pour lui, il en devient le propriétaire originel.

À la manière des chercheurs d’or de la conquête de l’ouest déterrant du minerai d’or de la terre dont ils deviennent propriétaires, on décrit les personnes mettant à disposition leurs machines pour la sécurisation du réseau monétaire comme des “mineurs de Bitcoin”. À chaque transaction validée, le “mineur” à l’origine de cette validation reçoit une récompense : du bitcoin fraichement créé pour lui : **il en est le propriétaire original, libre à lui ensuite d’en faire ce qu’il lui plait.**

La juste circulation est quant à elle garantie par la décentralisation et le consensus de validation d'une transaction. Étant donné que sur le réseau, chaque machine à un droit de réponse égale à une autre machine sur la validité d'une transaction dans la course à la récompense. Contrairement aux échanges monétaires, les échanges sur la blockchain ne connaissent pas de frontières, ce qui garantit la possibilité d’échanger de la valeur sans tenir compte des frontières.

Ces deux valeurs sont les piliers majeurs de la valeur intrinsèque de la Blockchain et son avantage concurrentiel vis-à-vis de la monnaie traditionnelle : une circulation et un système de création monétaire hors de contrôle d’un tiers (état, banque, organisme privé..).

Cryptoanarchisme : “Ni dieu ni maitre” sur internet.

L’anarchisme est un courant de pensée politique prônant l’auto-organisation du système par des citoyens-producteurs. Ce courant de pensée est en contradiction avec la notion de propriété privée du libertarisme. Son évolution contemporaine est le cryptoanarchisme, un courant de pensée défendant l’anonymat, une libre disposition d’internet et une égalité d’accès à l'information.

> *« Un spectre hante le monde moderne, le spectre de la cryptoanarchie. La technologie informatique est sur le point de permettre aux individus et aux groupes de communiquer et d'interagir de manière totalement anonyme. Deux personnes peuvent échanger des messages, faire des affaires et négocier des contrats électroniques sans jamais connaitre le vrai nom ou l'identité légale de l'autre. Les interactions sur les réseaux ne seront pas traçables, grâce à un réacheminement étendu des paquets chiffrés et des boites inviolables qui mettent en œuvre des protocoles cryptographiques avec une assurance presque parfaite contre toute altération. Les réputations seront d'une importance capitale, bien plus importante dans les transactions que les notations de crédit d'aujourd'hui. Ces développements modifieront complètement la nature de la règlementation gouvernementale, la capacité de taxer et de contrôler les interactions économiques, la capacité de garder l'information secrète et même de modifier la nature de la confiance et de la réputation. La technologie de cette révolution - et elle sera surement à la fois une révolution sociale et économique - existe en théorie depuis une décennie. Les méthodes sont basées sur le chiffrement à clé publique, les systèmes de preuve à divulgation nulle de connaissance et divers protocoles logiciels pour l'interaction, l'authentification et la vérification. Jusqu'à présent, l'attention s'est portée sur les conférences universitaires en Europe et aux États-Unis, conférences suivies de près par la National Security Agency. Mais ce n'est que récemment que les réseaux informatiques et les ordinateurs personnels ont atteint une vitesse suffisante pour rendre les idées pratiquement réalisables. Et les dix prochaines années apporteront suffisamment de vitesse supplémentaire pour rendre les idées économiquement réalisables et concrètement imparables. Les réseaux à haut débit, le RNIS, les boitiers inviolables, les cartes à puce, les satellites, les émetteurs en bande Ku, les ordinateurs personnels multi-MIPS et les puces de chiffrement en cours de développement seront quelques-unes des technologies habilitantes. Bien entendu, l'État essaiera de ralentir ou d'arrêter la diffusion de cette technologie, en invoquant les préoccupations de sécurité nationale, l'utilisation de la technologie par les trafiquants de drogue et les fraudeurs fiscaux, et les craintes de désintégration de la société. Beaucoup de ces préoccupations seront valables ; la cryptoanarchie permettra aux secrets nationaux d'être*

librement échangés et permettra le commerce de matériaux illicites et volés. Un marché informatisé anonyme rendra même possibles des marchés odieux d'assassinats et d'extorsion. Divers éléments criminels et étrangers seront des utilisateurs actifs du CryptoNet. Mais cela n'arrêtera pas la propagation de la cryptoanarchie. Tout comme la technologie de l'imprimerie a modifié et réduit le pouvoir des guildes médiévales et la structure du pouvoir social, les méthodes cryptologiques vont fondamentalement modifier la nature des sociétés et l'ingérence du gouvernement dans les transactions économiques. Combinée aux marchés de l'information émergents, la cryptoanarchie créera un marché liquide pour tout ce qui peut être mis en mots et en images. Et juste comme une invention apparemment mineure comme le fil de fer barbelé a rendu possible la clôture de vastes ranchs et fermes, changeant ainsi pour toujours les concepts de terre et de droits de propriété en Occident, la découverte apparemment mineure d'une branche mystérieuse des mathématiques deviendra le coupe-file qui démantèlera les barbelés autour de la propriété intellectuelle. Levez-vous, vous n'avez rien à perdre si ce n'est vos barbelés ! »

— Timothy C. May, Le Manifeste cryptoanarchiste, 1989[3]

Comment ne pas penser à la blockchain en lisant ce manifeste ? Tout y est : anonymat, cryptographie, transfrontalité... C’est assez incroyable de voir que ce manifeste, publié sur une mailing-list Cypherpunk il y a près de trente ans, distille autant de grands principes utilisés aujourd’hui par la blockchain.

L’anonymat est un principe clé de la pensée cryptoanarchiste, reprise par l’anonymat des transactions (sur la blockchain, le nom légal du titulaire d’un compte n’est pas nécessaire, il est remplacé par un identifiant unique appelé clé publique)

Ainsi nous obtenons un système d’échange de valeur anonymisé, autogéré par ces utilisateurs, non dépendant des états et des organismes de régulations.

Le mélange des inspirations cryptoanarchistes et libertariennes est intéressant à observer. La blockchain en plus d’être un objet technique complexe possède également une alchimie politique et idéologique hors du commun. Aussi attaché à la notion de propriété et de libre circulation de la valeur qu'à la notion d’anonymat et d’équité entre ses utilisateurs.

Après avoir fait un focus sur l’idéologie derrière cette technologie, permettez-moi de vous présenter les rouages techniques...

[3] Version originale : https://www.activism.net/cypherpunk/crypto-anarchy.html

Fonctionnement de base

Comment résumer la blockchain en une phrase ? “Internet a digitalisé la communication, la blockchain va digitaliser la confiance” [4].

En écoutant cette phrase, il est facile de voir en quoi internet a digitalisé la communication, il n’y a qu’à voir le succès des réseaux sociaux et le poids financier qu’ils représentent. Mais quid de la “confiance” ?

Dans un échange monétaire basique entre un acheteur et un vendeur, la confiance est matérialisée dans la monnaie dite fiduciaire (pièces et billets de banque), elle offre la garantie au vendeur de pouvoir échanger cette monnaie contre autre chose.

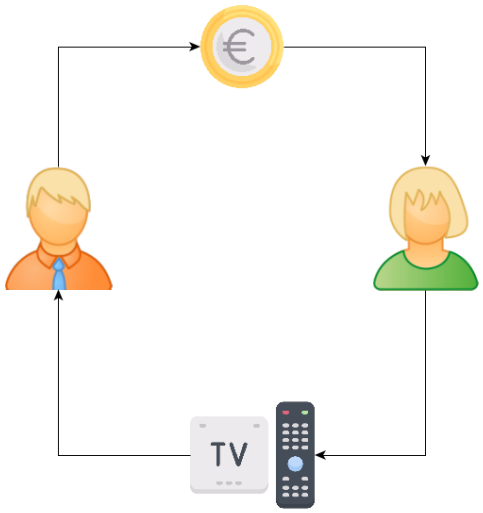

Figure 1 - échange monétaire

Avant l’invention de la banque, l’on fonctionnait exclusivement comme le schéma précédent. Mais avec l'apparition des virements bancaires, des chèques et des cartes de crédit, c’est par elles que passent 90% des transactions.

Voici comment cela fonctionne lors d’un paiement via ces moyens de paiement dit scripturaux, la banque de l’acheteur va certifier à la banque du vendeur que son client à la possibilité d’effectuer cet achat. Elle va ensuite prélever l’argent du compte client pour émettre un bon de dette à la banque du vendeur, celle-ci à la réception de ce bon va créditer le compte de son client avec la somme inscrite sur le bon.

La confiance est matérialisée ici dans ce “bon de dette”. La monnaie est dite scripturale et non fiduciaire, elle n’est donc pas palpable. Cette monnaie virtuelle, c’est

[4] phrase issue d’une interview de Eric Larchevêque, fondateur de Ledger, pour le podcast Vlan!

celle de votre compte en banque, elle peut être retirée à tout moment en monnaie fiduciaire, mais n’existe qu’en tant que “dette”. En clair, si vous avez 2000€ sur votre compte courant, votre banque à une dette de 2000€ envers vous, mais ne stocke pas cette somme au fond d’un coffre-fort.

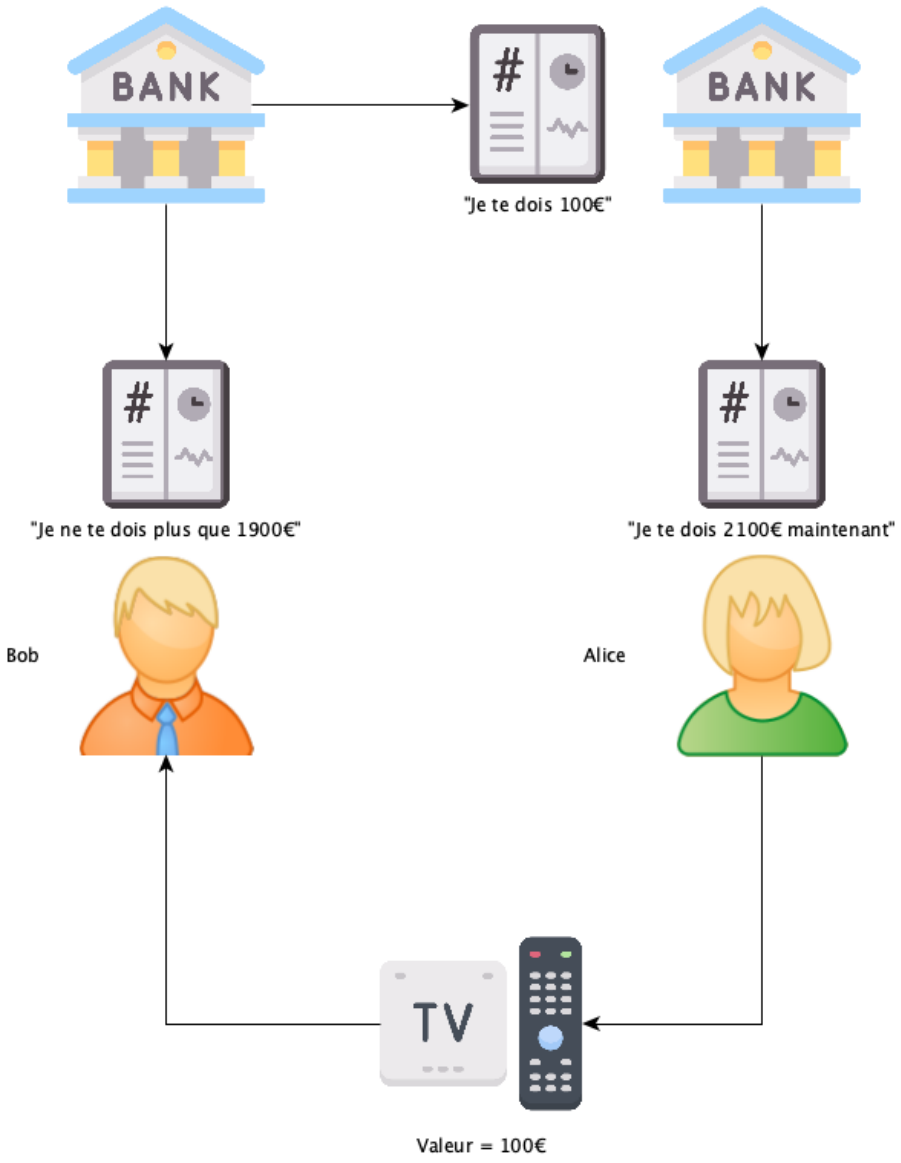

Figure 2 - échange bancaire

Contrairement au modèle précédent, la confiance n’est plus en la monnaie en elle-même, mais envers la promesse de votre banque de vous donner 2000€ quand vous en aurez besoin.

C’est un peu comme si dans le premier exemple, l’acheteur écrivait une reconnaissance de dette en lieu et place de monnaie.

Il faut avoir confiance pour accepter ce système, si l’émetteur de dette n’est pas fiable, il y a un risque de ne pas revoir son argent. Nous devons nous en remettre à ce que l’on appelle un tiers de confiance.

Revenons à la blockchain, celle-ci nous promet un système d’échange sans banque ou tiers de confiance ni monnaie physique. Grâce entre autres à un système sécurisé, numérique, sans tiers de confiance.

Prenons un exemple, la première implémentation de cette technologie : le Bitcoin.

Le Bitcoin (BTC) peut être vulgarisé grâce à deux analogies :

- L’analogie du chercheur d’or utilisé au chapitre précédent
- L’analogie de l’e-mail

L’e-mail est horodaté avec l’heure, l’expéditeur, le destinataire

Le Bitcoin est une chaine de “blocs” de transactions dans lesquels sont inscrits des transactions horodatées avec l’heure, le montant, l’expéditeur et le destinataire.

Chaque utilisateur possède un *portefeuille électronique*[5] possèdent lui-même deux clés uniques, l’une est privée et peut s’assimiler à votre code de carte bleue, l’autre est publique et sert d’identifiant unique pour s’identifier sur la blockchain.

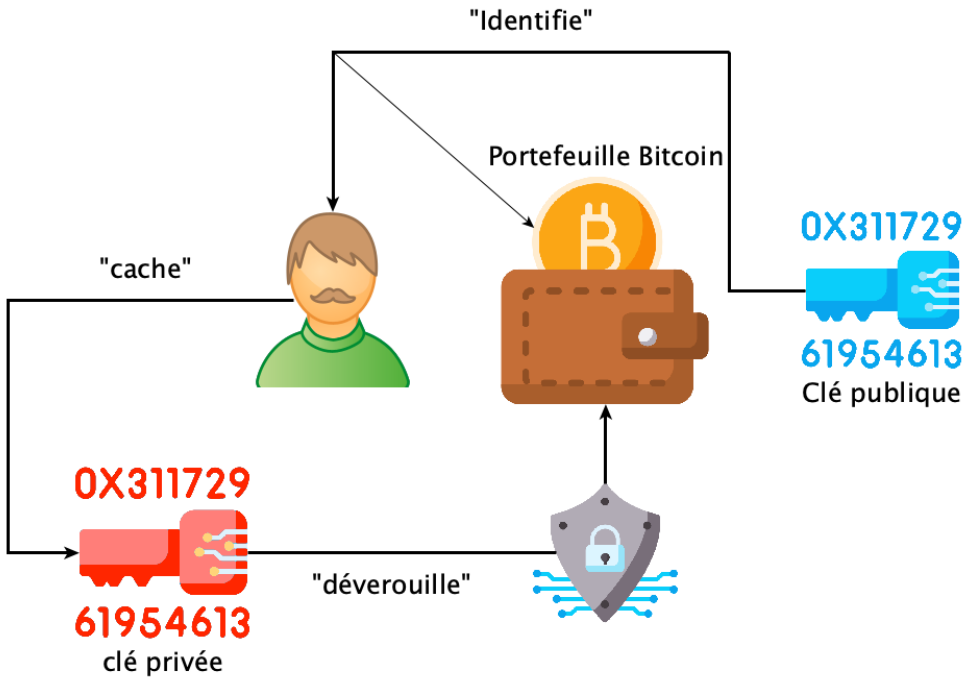

Figure 3 - clé publique, clé privée

[5] Porte-monnaie virtuel

Si l’on reprend notre précédent schéma de transaction monétaire classique, l’acheteur va émettre un ordre de paiement sur le réseau Bitcoin, cet ordre de paiement va être stocké dans un bloc, chaque bloc est ajouté à la suite du bloc de transaction précédent sous 10 minutes par un travail de vérification.

Sur terre il existe une quantité finie d’or, il est de plus en plus dur d’en extraire au fil du temps. Pour le Bitcoin, c’est pareil, il y a une quantité finie de Bitcoins disponible et, au fil des blocs transactions, c’est de plus en plus dur pour les “mineurs” d’obtenir de grosses récompenses. Chaque bloc de transaction est vérifié et validé par les mineurs. Le premier qui arrive à certifier que la transaction est valide, en vérifiant son exactitude ainsi qu’en résolvant le premier un problème mathématique complexe dont le résultat est certifié par 5 autres mineurs, gagne la récompense et ajoute le bloc de transaction à la Blockchain. C’est ce que l’on appelle la preuve de travail.

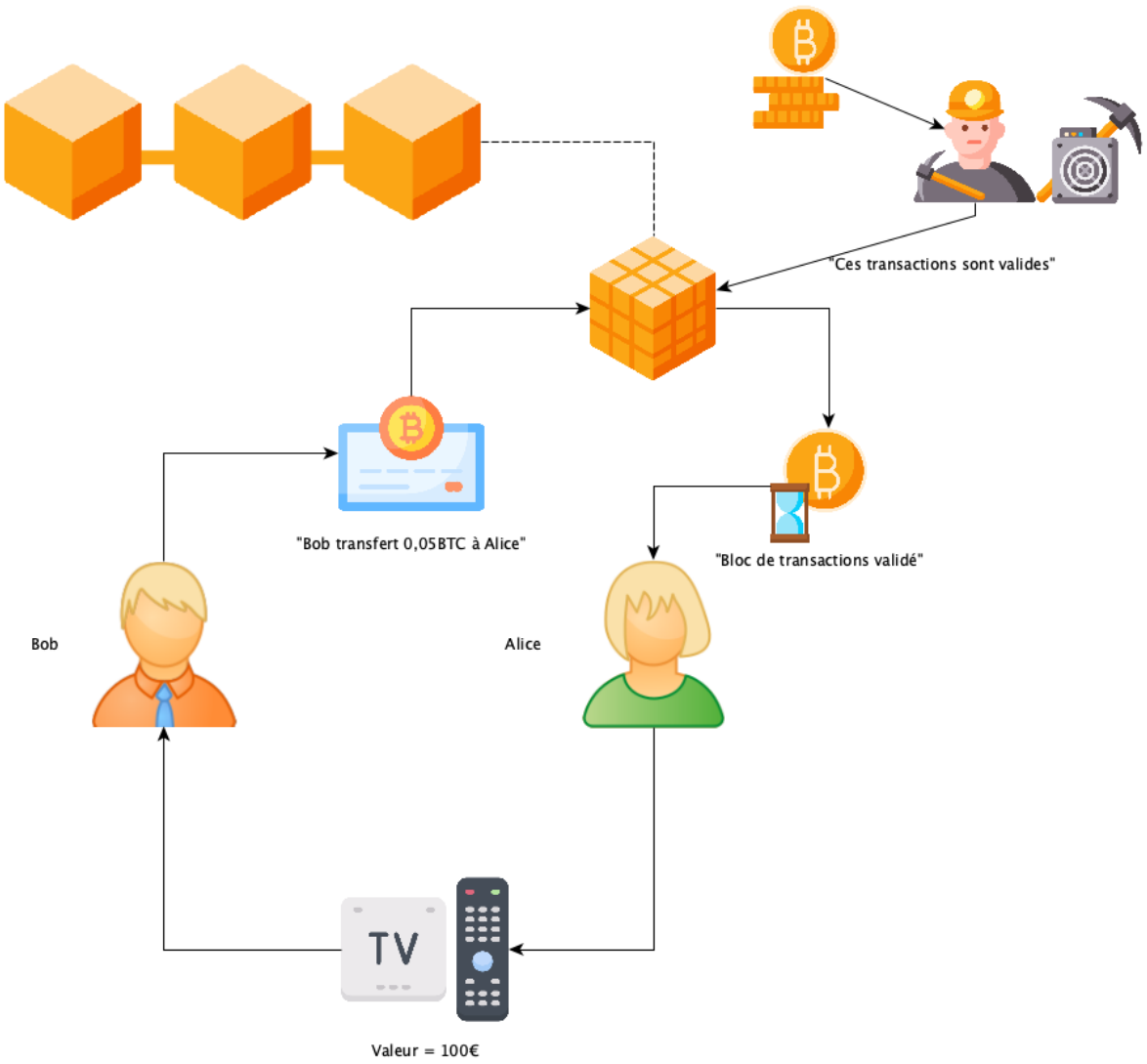

Figure 4 - échange via transaction bitcoin

Tous les “mineurs” connectés au réseau possèdent une copie locale qui est mise à jour par rapport aux différentes validations. Nous avons une propagation de l’information sur tout le réseau de transactions dès qu’un bloc de transactions est validé par 51% du réseau, on peut admettre que la transaction est valide. Il y a donc consensus et l’ensemble du réseau se met à jour avec cette nouvelle liste de transactions valide

tous les 210000 blocs de transaction, on divise la récompense par deux, elle fut d’abord de 50 BTC, puis 25, 12,5 et depuis mai 2020 : 6,25 BTC. Mathématiquement, par diminution successive de la récompense la limite de création monétaire se situe en dessous de 21 millions de bitcoins.

Cette chaine de blocs de transactions peut se matérialiser en un grand livre de compte partagé où chaque utilisateur et mineur peut vérifier l’état de toutes les transactions en temps réel et propager les modifications à tous les acteurs en cas de nouveau bloc.

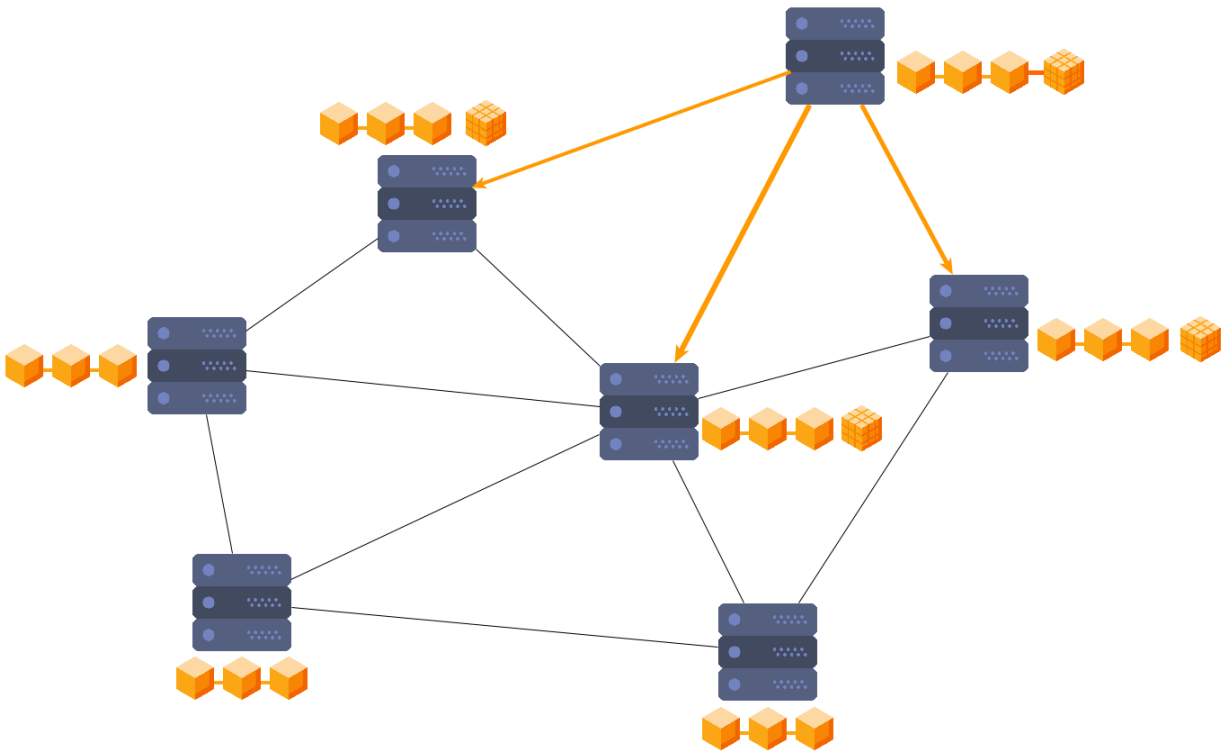

Figure 5 - Nœuds en réseau d'une blockchain

Controverses

Énergie

Le point sensible concernant l'utilisation de la blockchain est surement son impact énergétique. Actuellement, la blockchain Bitcoin consomme en moyenne autant qu'un pays comme l'Autriche chaque année, avec une consommation atteignant en moyenne les 50 TWh par an : **c'est gigantesque.**

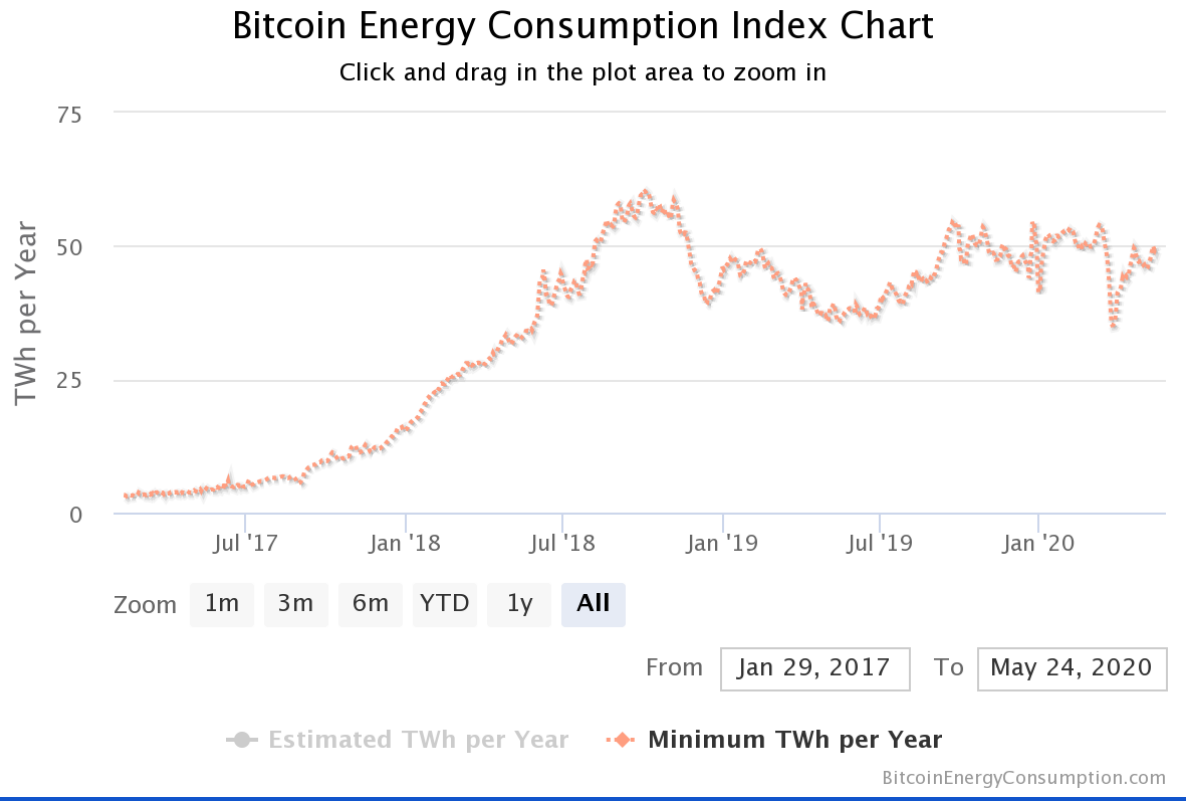

Figure 6 - consommation annuelle du Bitcoin

On estime également l’empreinte carbone de la blockchain à 28 Mt CO2 par an, **c'est presque autant qu'un pays comme la Syrie.**

Étant donné que la procédure de vérification des transactions du réseau repose sur l'utilisation de puissance de calcul, donc d'énergie, afin de mettre en concurrence les mineurs chargés de la sécurisation du réseau, il n'est pas étonnant de constater cette croissance de la consommation.

Plus le temps passe, plus il y a de bitcoins en circulation, plus il y a de transactions à gérer, plus il est devenu complexe de vérifier les transactions, plus il faut de puissance pour miner les blocs de transactions, plus il faut d'énergie.

En l'état, la blockchain Bitcoin n'est pas viable à long terme au niveau écologique, sa consommation va croitre avec le nombre de transactions, en corrélation avec la complexité de son système de sécurisation : la preuve de travail.

Des solutions sont néanmoins envisageables pour atténuer ce problème, par exemple l'utilisation d'énergie dite "fatale", les surplus générés par les énergies renouvelables comme l'éolien, le solaire ou l’hydroélectrique.

Hydro-Québec, producteur d’énergie canadien, a par exemple proposé des “offres” à tarifs réduits pour les potentiels “mineurs” lorsque les barrages hydroélectriques produisent un surplus d’énergie par rapport aux besoins de l’industrie et de la population.[6]

Mais la solution idéale serait de passer d'un modèle "preuve de travail" à un modèle basé sur la "preuve d'enjeux". La sécurisation des données n'est plus basée sur la compétition de puces de silicium consommant une quantité astronomique d'énergie, mais sur le tirage au sort des acteurs chargés de vérifier les transactions.

La preuve d'enjeux

Au lieu de résoudre un problème mathématique complexe avant tout le monde, le réseau de transaction tire au sort un “mineur”, ou plutôt ici un “forgeron”, chargé de valider une transaction. L’on dit que le bloc de transaction n’est pas “miné” via de la puissance de calcul, mais juste “forgé” sur la blockchain par le forgeron tirer au hasard.

La sélection du forgeron se joue sur les critères suivants :

- **La mise de départ** : chaque forgeron va “miser” une somme pour participer à la course au forgeage du bloc de transaction sur la Blockchain. Cette mise est verrouillée tant que le forgeron est dans la course. Plus la mise est importante, plus le forgeron aura de chance d’être sélectionné.

- **Le temps d’attente** : Plus le forgeron aura passé de temps dans la file d’attente avec sa mise, plus ses chances augmentent également.

- **La réputation** : Si un forgeron forge un bloc contenant des transactions frauduleuses, celui-ci perd tout ou partie de sa mise.

La rémunération du forgeron est issue des frais de transactions contenus dans le bloc. Ici, la puissance de calcul n’est plus utilisée en compétition, mais en coopération.

[6] Source : https://www.hydroquebec.com/chaines-de-blocs/

Chacun est également libre de participer au forgeage, sans avoir besoin de bêtes de calculs pour pouvoir gagner de la récompense. L’impact écologique est considérable puisque le réseau n’a plus besoin d’autant de puissance pour fonctionner.

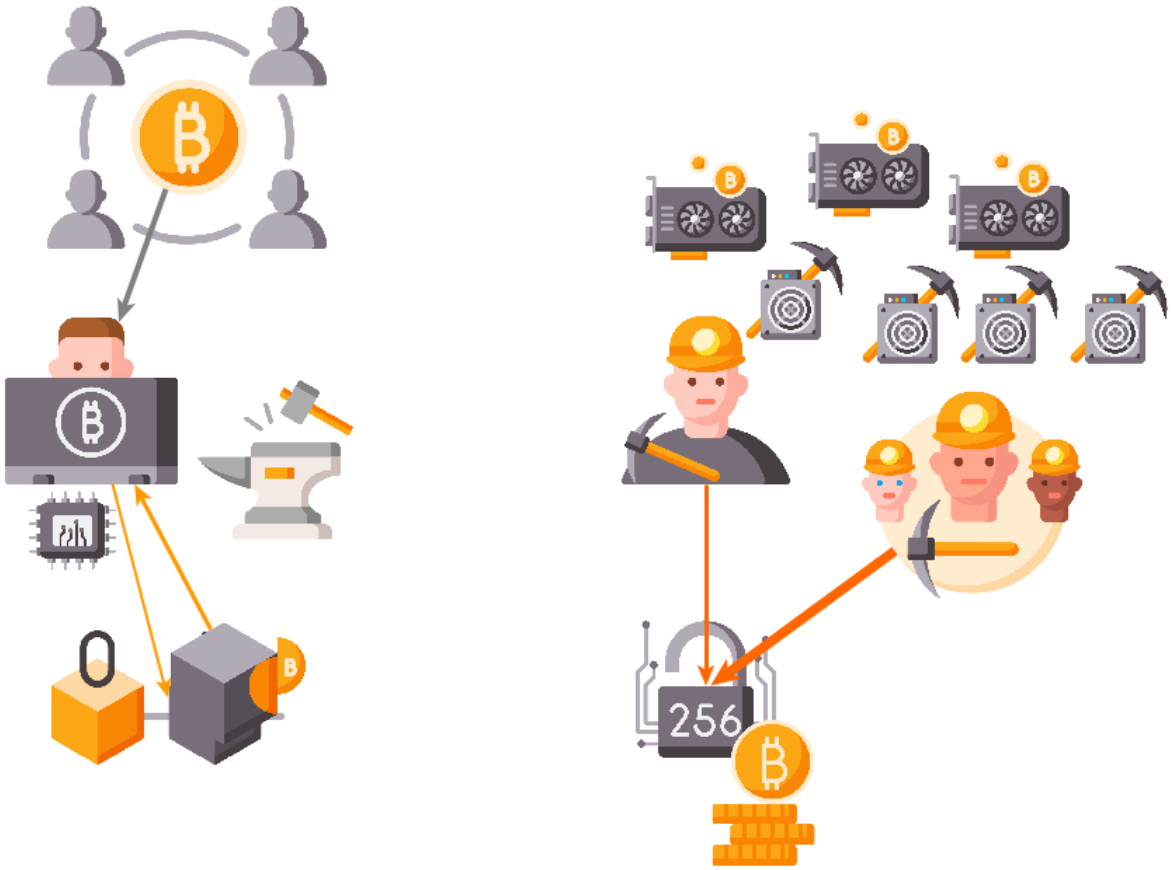

Figure 7 - Proof of stake VS Proof of work

Hors des frontières et des législations

Un autre frein à la régulation de la blockchain, et non des moindres, est le bras de fer entre une vision reposant sur une création monétaire maitrisée par l'état, utilisée dans une zone monétaire et un cadre défini par la loi versus une création monétaire régie par un algorithme, sans frontière et sans cadre juridiques.

Cette "dérégulation" de la monnaie, sans personnes morales ou physiques derrière les transactions, permet à des organisations criminelles de faire transiter des fonds en toute discrétion. Malgré des transactions publiques de tous, la blockchain utilise des identifiants anonymes, propre à chaque compte, appelé clé publique.

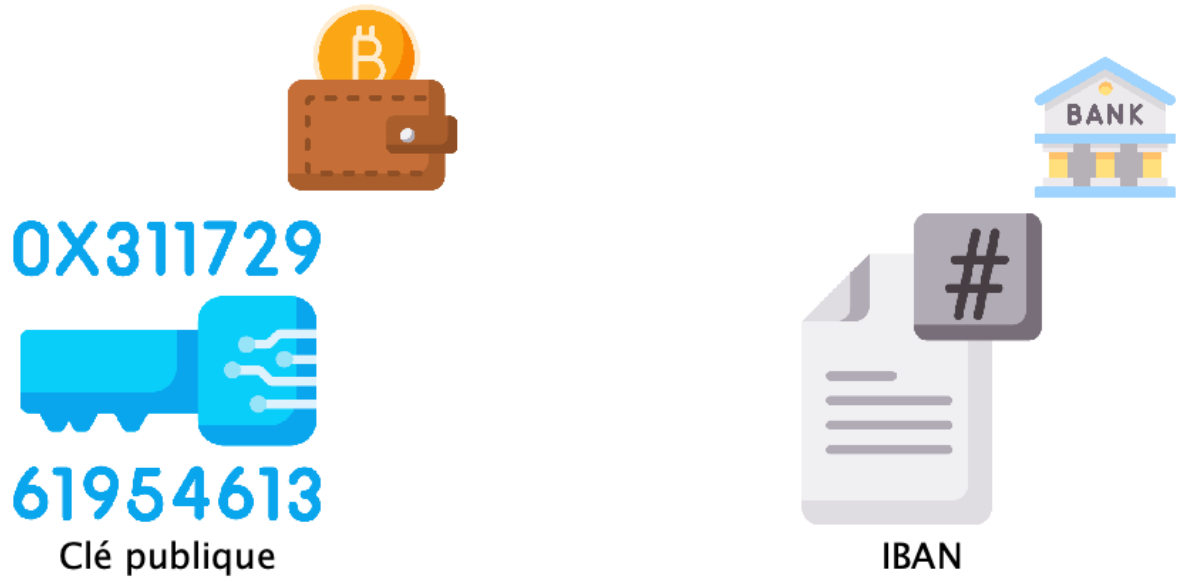

Figure 8 - clé publique VS IBAN

Les seules informations disponibles avec la blockchain étant donc la liste des différentes transactions soit la liste des clés publiques, leurs historiques de transaction et par conséquent leur solde. Mais en revanche, il est impossible de savoir l’identité légale d’un propriétaire de compte.

La blockchain permet également de contourner les embargos, le Venezuela à par exemple créer le "Pétro", une monnaie adossée aux réserves de pétrole et minerais du pays, permettant de lever des fonds via une émission de cette crypto monnaie en dehors du pays.

La nouveauté de cette technologie et la non-régularisation stricte de ses cas d’usages dans de nombreux pays forment donc une sorte de zone grise législative sur son champ d’action. Il est à noter que malgré cela, le fait que les transactions restent à vie dans une blockchain forme une preuve indestructible lors d’une utilisation de cette

technologie à des fins illégales... Il suffit en effet aux services de police d'associer votre matériel informatique à votre clé publique pour vous identifier ainsi que l’ensemble de votre historique de transaction !

Escroquerie et opacité

La blockchain est également perçue par certaines personnes comme une pyramide de Ponzi géante. Le fait d’investir de l’énergie, des marchandises, voir même de l’agent contre une monnaie aux cours parfois fortement volatiles et dont la valeur est extrêmement difficile à déterminer. Avec un système de création monétaire et de sécurisation des transactions complexe, mais surtout sans aucun cadre juridique ni législatif d’un état, cela peut paraitre un pari risqué. Le fait également que c’est une technologie nouvelle, en émergence et complètement digitalisée, accentue les suspicions.

Prenons le cas de Onecoin, une cryptomonnaie promettant sur le papier une véritable révolution financière. Jugez plutôt :

- Arthur investi dans Onecoin à hauteur de 150€, il achète une "formation" et reçoit alors le titre de "commercial indépendant".
- Arthur va alors convaincre Béatrice d'investir 100€ dans onecoin. Béatrice va recevoir 1000 onecoins, et Arthur va alors toucher un "Bonus".
- Au bout de 9 "Bonus", Arthur va convaincre sa dixième victime, Kate, d'investir dans onecoin, mais cette fois-ci, Les "Bonus" d'Arthur sont transformés par la société Onecoin en nouvelle "formation".
- Arthur obtient le droit d'empocher directement les 100€ de Kate. Une fois Athur payé, Onecoin envoi "1000" OneCoin à Kate.

Les 10 victimes d'Arthur constituent un nouvel étage de la pyramide et n'ont d'autre choix que de convaincre elles aussi 10 nouvelles personnes d'investir pour récupérer leur argent.

Figure 9 - "onecoin - the bitcoin killer"

Je n’ai pas la prétention de pouvoir être sûr que de grandes blockchains comme Bitcoin ne soient pas en réalité une vaste escroquerie, mais une chose est sure : techniquement, Bitcoin fonctionne, Onecoin n’était cependant qu’une simple feuille Excel sans aucune véritable “blockchain” derrière…

En effet, aucune infrastructure n’était implémentée, aucun livre blanc technique, juste un simple site web avec une base de données de “clients”.

OneCoin est aujourd'hui interdit dans de nombreux pays, et sa créatrice, Dr Ruja Ignatova, est actuellement en fuite depuis plus de deux ans.

Onecoin à réussi à amasser près de 4 milliards de dollars. La valeur des Bitcoins en circulation avoisine en 2020 les 100 milliards de dollars.

Cas d'usages pratiques

La Blockchain n’est pas seulement un objet technologique servant exclusivement l’échange de valeur sur internet, comme toute technologie, c’est avant tout un outil.

Sa nature programmable lui permet de se transformer pour prendre plusieurs formes.

Nous connaissons bien la Blockchain Bitcoin, une sorte d’échange d’or numérique en ligne, mais d’autres Blockchains existent, des Blockchains qui ont muté pour répondre à de nouveaux besoins.

Dans ce chapitre, je vous présente trois cas d’usages alternatifs à la blockchain Bitcoin.

Contrats intelligents et assurance.

Tout comme l’univers bancaire, où les banques ne s’échangent pas uniquement de la monnaie, mais aussi des contrats, des titres, des produits financiers ou des polices d’assurance. Nous pouvons également échanger plus que de la monnaie sur la Blockchain, ou plutôt devrions nous dire les blockchains.

En effet, Bitcoin n’est que la première implémentation de cette technologie, une sorte de première version, conçue exclusivement pour échanger de la monnaie électronique prenant pour modèle de référence l’or.

Mais l’avantage d’une monnaie électronique, dont le système et les règles de transactions sont basés sur un algorithme, c’est justement de pouvoir faire évoluer le code source.

C’est ce qu’a tenté de réaliser Vitalik Buterin en 2011, qui a l’idée de modifier Bitcoin afin de le rendre plus léger et orienté vers l’économie réelle et la création logicielle. Cette nouvelle blockchain nait en 2015 sous le nom d’Etherium.

L’idée est de fournir une blockchain fonctionnant sur le même principe que Bitcoin, le minage de bloc de transaction. À la différence que les mécanismes de créations monétaires sont simplifiés : après une émission initiale de 50 millions d'Éthers (la monnaie de la Blockchain Etherium), chaque “transaction” minée rapporte en moyenne 3 Éthers au mineur.

Un Ether : la monnaie d'Etherium

Figure 10 - Représentation de l’Ether

Mais le véritable avantage de cette Blockchain, c’est qu’elle est “programmable”. Il est donc possible de créer des applications utilisant cette blockchain comme plateforme de vérification et de financement. Il est ainsi possible de mettre en place des contrats intelligents, des programmes s'exécutant sous certaines conditions.

Ces contrats, une fois signés numériquement, ne peuvent plus être modifiés et s'exécutent automatiquement si les conditions définies dans celui-ci sont validées par

des “oracles”. Ces oracles sont des programmes faisant office de capteurs à ces contrats intelligents, dès que ces oracles avertissent que certaines conditions sont réunies, les contrats s'exécutent automatiquement.

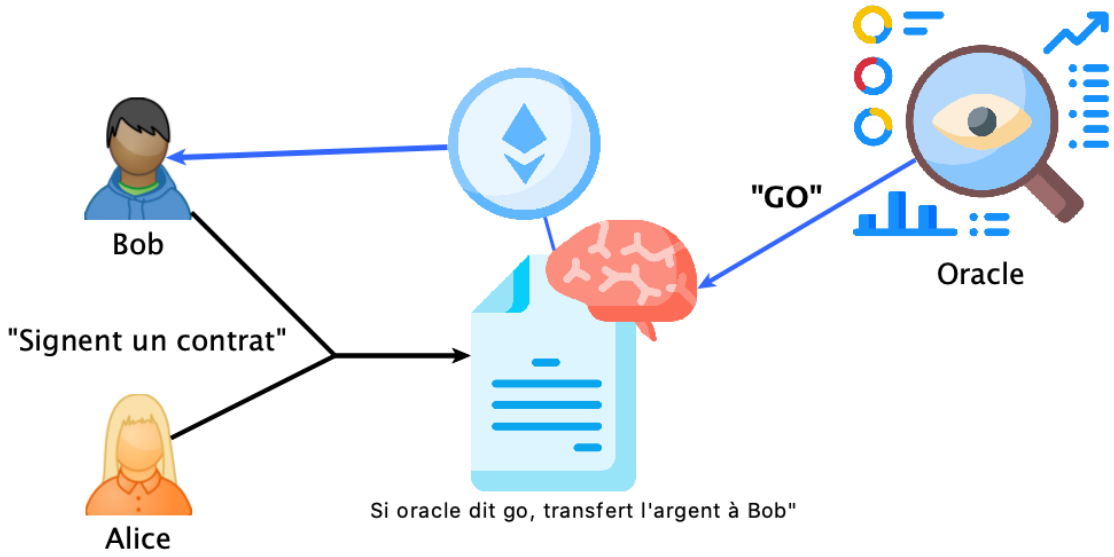

Figure 11 - fonctionnement d'un smart contract

Prenons l’exemple d’un agriculteur ayant souscrit un contrat contre la canicule. Celui-ci a souscrit une assurance via un contrat intelligent via son assurance et verse l’équivalent de 1 Éther (environ 180€) par an pour ces 10 hectares de champs.

Ce contrat intelligent est programmé pour s'exécuter et verser 25 Éthers (environ 4600€) si la température moyenne relevée par la sonde locale et météo France dépasse les 40°C sans précipitation pendant plus de 10 jours et si la souscription annuelle à bien été versée sur le contrat.

Ainsi, l’agriculteur est automatiquement remboursé par la plateforme en cas de sinistre.

Mais l’agriculture n’est pas le seul cas d’utilisation de ces contrats intelligents, l’on peut également imaginer son application dans des domaines de la vie de tous les jours : par exemple, une assurance “Connexion” souscrit avec votre fournisseur internet via un contrat intelligent qui s'exécute en cas de coupure de service pour vous rembourser les périodes où vous n’avez pas pu profiter de votre connexion internet de façon stable et optimale.

Et si il existait une assurance pour les transports en commun, qui vous rembourse automatiquement, et ce sans la moindre démarche de votre part, si votre bus, train ou avion a du retard ou est annulée ?

C’est ce qu’a fait la société Axa avec Fizzy, la première assurance utilisant les contrats intelligents pour rembourser automatiquement les souscripteurs si leur avion a plus de deux heures de retard.

Son utilisation est simple, il suffit de s’inscrire sur le service, de rentrer son numéro de vol, de payer et le service vous envoie une confirmation de prise en charge. En cas de retard de plus de deux heures sur votre vol, vous êtes indemnisé automatiquement par le système, sans intervention humaine

Alice veut souscrire à une assurance. Elle s'inscrit sur le service et Fizzy va récupérer son numéro de vol, ses informations bancaires et lui générer un couple clé public / clé privé. Alice n'a pas accès aux détails, elle a juste une police d'assurance valide. Un contrat est donc créé entre Alice et Axa, celui-ci s'exécutera si l'oracle (un programme surveillant les horaires des vols) détecte un retard. Imaginons que le vol d'Alice à plus de 2h de retard, le contrat intelligent va interroger l'oracle et va s'exécuter pour envoyer la somme convenue sur le compte Éther créer lors de l'inscription d'Alice sur le service. Alice va ensuite être payée en euro par Axa qui soldera son compte Éther.

Fizzy nécessite tout de même un cout de fonctionnement dont le prix est fixé par le réseau etherium, une sorte de cout d'exécution payé par celui qui dépose le contrat intelligent sur la blockchain. Chaque clôture de contrat intelligent doit être exécutée dans l'Etherium Virtual Machine.

L'Etherium Virtual machine peut être comparé à une poissonnerie. Les parents *-les créateurs des contrats intelligents* - donnent aux enfants - *les contrats* - un billet de 100€ avec une somme maximale à ne pas dépasser pour l'achat d'un kilo de poisson *- la commission nécessaire à L'EVM pour fonctionner autrement appelée **'gas limit'*** - .

Imaginez donc une fille d'enfants attendant tranquillement chacun leur tour pour l'achat d'un ou plusieurs poissons.

Dans la glace, 1kg de Saumon à 25€, 1 kg de Homard à 60€ et 1 kg de Cendre à 15€.

Si notre enfant à une limite de 30€, et que nous voulons qu'il achète du saumon, il va acheter du saumon et nous le rapporte si et seulement si le kilo de saumon est strictement inférieur à 30€, et à la suite de son achat il nous donnera la monnaie. Si nous voulons tout de même du saumon et que celui-ci passe au-dessus des 30€, il va nous falloir rehausser la limite fixée à notre enfant.

Un Gas est donc assimilable une décomposition plus petite de l'Éther (le billet de 100€ de l'exemple), c'est plus à proprement parler une limite plutôt qu'une commission fixe. Pour fixer la limite d'une transaction, nous pouvons nous aider du site ETH Gas Station qui nous indiquera le cout moyen d’une transaction.

Celui-ci nous permet de savoir en temps réel le cout d'une exécution de contrat dans l'EVM. Il existe trois types de couts différents :

- Fast : pour une file d'attente inférieure à 2 minutes
- Standard : pour une file d'attente inférieure à 5 minutes
- Safe Low : pour une file d'attente inférieure à 30 minutes.

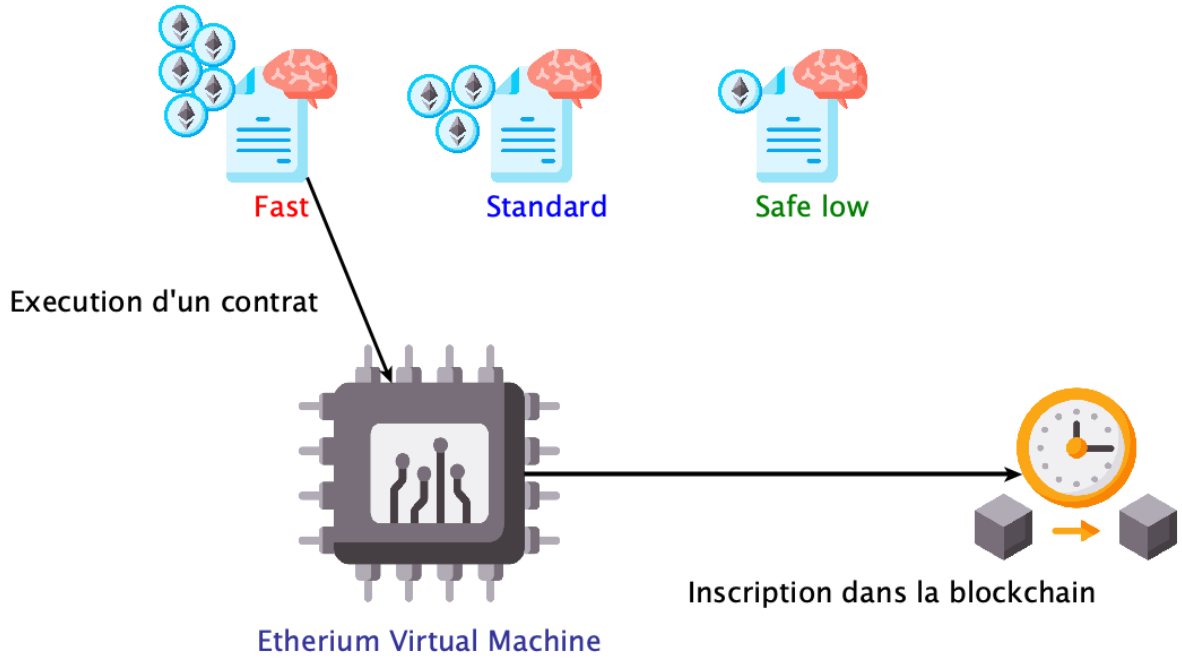

Figure 12 = Fonctionnement de l'Etherium Virtual Machine

Ce choix va conditionner la position de votre contrat dans la file, pour Fizzy, tout dépend si le contrat doit s'exécuter et donc rembourser le client immédiatement, sous 5 minutes, ou si la durée n’a pas d’importance.

Fizzy repose donc sur cette logique de contrat intelligent. Enfin reposait sur cette logique puisque le service expérimental a fermé fin 2019.

La raison de cette fermeture n'est pas explicitée, mais nous pouvons imaginer plusieurs cas de figure :

- Le service reposant sur des commissions, les couts sont assez élevés pour Axa en cas de retard effectif, d'où peut-être une faible rentabilité (R&D + cout de fonctionnement).
- Les questionnements sécuritaires autour du basculement de la blockchain Etherium sur un modèle de vérification des contrats basé sur la preuve d'enjeu

(en remplacement de la preuve de travail dont nous avons parlé précédemment), on remit en question la fiabilité du service.

- Manque d'utilisateurs du service.

Quoi qu'il en soit, nous resterons à l'affut d'une prochaine initiative dans le milieu de l'assurance. Mais l'assurance étant parfois un produit complexe, la rigidité des contrats inscrits sur la blockchain peut effrayer en cas d'erreur, car le contrat, pour rappel est irrévocable une fois déposer sur celle-ci.

De plus les « oracles», ces supercapteurs chargés de fournir aux contrats les données relatives à l'exécution ou non du contrat (dans le cas de Fizzy, c'est le protocole de surveillance du trafic aérien "Automatic dependent surveillance – broadcast") doivent être supposés "de confiance" et incorruptible pour garantir une juste exécution des contrats.

En résumé, pour garantir une assurance paramétrique de qualité, il faut :

- Des "oracles" surs et incorruptibles nous fournissant des données justes et de qualités
- Des contrats bien écrits, prenant en compte tous les cas d'utilisations possibles de nos clients (d'où l'importance de commencer par quelque chose de "simple" à dématérialiser)
- Une infrastructure blockchain résiliente de confiance : comme Etherium.

Traçabilité et sécurité alimentaire

Le grand avantage de la blockchain réside en sa capacité à offrir à ces utilisateurs une parfaite transparence entre les différentes transactions sur le réseau. Tout le monde peut à tout moment consulter l’historique des transactions dans le réseau et obtenir l’historique d’échange d’un “token” comme Bitcoin, c’est comme si, à partir du numéro de série d’un billet de banque, nous pouvons identifier via un identifiant unique, tous les précédents porteurs de celui-ci.

Figure 13 - un billet de 500€ avec son numéro de série

Imaginons maintenant que ce registre de transaction publique ne serve plus à faire transiter de la monnaie, mais des certificats, des documents dont on pourrait identifier chaque modification via un identifiant unique.

C’est ce qu’a mis en place IBM via une nouvelle blockchain “FoodTrust”. Son objectif principal est de sécuriser la traçabilité alimentaire et de prévenir automatiquement les risques sanitaires. En un scan sur un produit alimentaire en rayon, l’on doit pouvoir identifier tout son parcours, du champ jusqu’au magasin.

Pour ce faire, IBM va utiliser la blockchain comme “historique global” partagé entre tous les utilisateurs du service.

Chaque utilisateur va se voir attribuer un identifiant unique et une clé privée pour utiliser le service.

Ensuite chaque acteur va pouvoir effectuer six différentes actions :

- **Création :** indiquant la création d’un objet.

  Par exemple une récolte de pommes. Pierre l’agriculteur va enregistrer un document sur la blockchain IBM détaillant les caractéristiques de son produit,

son lieu et date de récolte par exemple.

- **Agrégation :** indique le regroupement d’objets.

  Par exemple Pierre va conditionner 1000 pommes dans une palette direction la coopérative, chez Paul à 40 kilomètres d’ici.

- **Désagrégation :** indique le démantèlement d’objet en objet plus petit.

  Pierre va séparer la palette de 1000 pommes en cartons de 100 pommes chacun et en vendre 3 à Jacques, un industriel fabricant de la compote.

- **Transformation :** indique la transformation d’un produit.

  Jacques va transformer les objets “pommes” en “Compote de pomme Jacques&Co”

- **Observation :** indique une observation sur un produit.

  Le frère de Jacques, tenant le magasin, scanne un lot de compote avant sa mise en rayon.

- **Suppression :** indique la suppression d’un objet.

  Au vu du scan du gérant du magasin, la chaine du froid n’a pas été respectée entre son départ de l’usine Jacques&Co et sa mise en rayon, il lance une alerte pour avertir les autres utilisateurs du service et le produit est détruit.

À la manière d'Amazon avec leurs Amazon Web Services, IBM va fournir aux professionnels de l'agroalimentaire une myriade d'outils pour interconnecter leurs infrastructures existantes avec cette Blockchain et suivre en temps réel l'état de tel ou tel produit :

- **Traçabilité :** Assurer le traçage de la localisation et de l’état des produits alimentaires en amont comme en aval de la chaine logistique. À la manière d'une frise chronologique, on peut identifier si nos produits sont à l'étape ferme, stockage, usine de traitement, distributeur, ou en magasin.

- **Certifications :** Garantir la fiabilité et la gestion responsable des produits grâce à l’accès instantané aux fichiers et documents de certifications des produits au format numérique. À chaque scan ou check point, on peut visualiser ces documents.

- **Indicateur de fraicheur :** Accéder en temps réel aux données de la chaine logistique et améliorer la fraicheur et la durée de conservation des produits grâce à des indicateurs précis, une sorte de Google Analytics de la Supply Chain (Chaine d'approvisionnement) avec toutes les données et un moteur d'analyse des risques)

- **Un système d'importation** : l'on peut importer ses données directement depuis une simple feuille Excel, jusqu'à un import de base de données existante, IBM fournit tous les outils nécessaires à la bonne importation des données dans leurs systèmes.

En plus de cette suite d’outils, un système d'attributs pour veiller à la sécurisation des données contenu dans la blockchain. Il est ainsi possible de classifier les données suivant quatre niveaux de sécurité :

- **Ouvert** : Les documents sont publics à tous les utilisateurs de la blockchain IBM Food Trust.

- **Privé** : Les documents sont uniquement visibles par l’organisation qui les a publiés sur la Blockchain

- **Restreint** : Les documents sont partagés avec la liste des organisations listée dans le document.

- **Lié** : Les documents sont uniquement partagés lors d’un échange de produits entre deux organisations différentes (lors d’une vente par exemple)

Nous avons ici un outil très complet, respectant la norme “GS1 EPICS” (Electronic Product Code Information Services), utilisant la Blockchain de façon à stocker le la donnée et non purement de la valeur fiduciaire ou un contrat déclenchant un échange de valeurs.

Cette Blockchain contrôlée par IBM n'est certes pas totalement transparente vis-à-vis du modèle de gouvernance, mais permet aux différents acteurs présents en son sein d'interagir et d'évoluer dans un milieu de confiance. Il est dans l'intérêt de tous que les données renseignées ici soient les plus sures possible.

C'est un bel exemple d'une utilisation de la Blockchain en temps qu'outil plutôt que de moyen de spéculation au service de la sécurité alimentaire.

Mais ce mécanisme de traçabilité assisté par la blockchain ne s'arrête pas à l’alimentaire, mais pourrait également séduire l’industrie automobile ou le marché de l’art. Imaginons un système de certification universel permettant de tracer les oeuvres

d’art et de justifier de leur authenticité en cas d’achat ou de ventes. Ou encore une carte grise numérique 2.0, contenant les différentes informations d’une carte grise, mais aussi, l’historique des contrôles techniques, la police d'assurance et le carnet d’entretien du véhicule.

Mécanisme de tokenisation et entrepreneuriat

Lorsqu’une société veut se lancer en bourse, elle émet des actions sur le marché public via ce que l’on appelle une IPO pour *initial public offering*. Lors de cet évènement, la société va émettre sur le marché des actions à un prix défini.

Par exemple l’entreprise Facebook a en 2012 introduit la société en bourse via une IPO, celle-ci a distribué 421 millions d’actions à 38$, ce qui a permis à Facebook d’amasser environ 16 milliards de dollars. En échange une partie de la société est détenue par les propriétaires de ces actions à travers un titre de propriété.

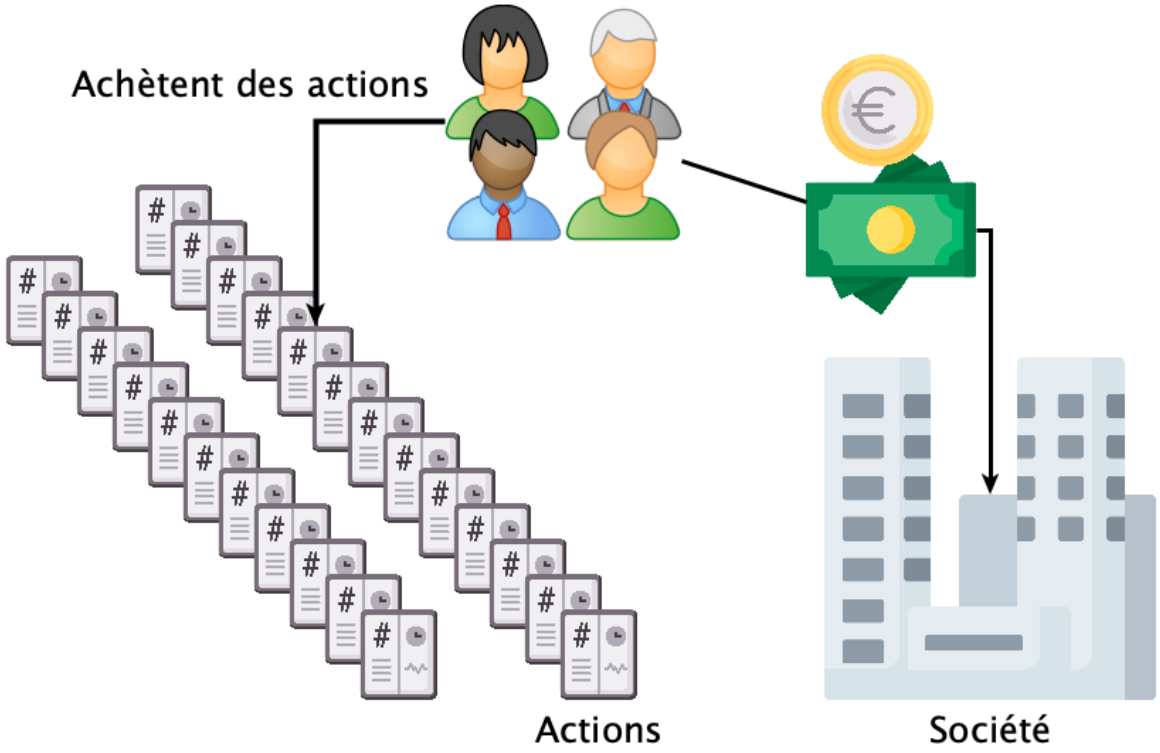

Figure 14 - Actionnariat dans une société classique

La blockchain repose sur un mécanisme de tokenisation. En sécurité informatique, il s'agit de remplacer un élément critique par un équivalent qui, sorti du système n'a aucune valeur, un "token" ou jeton en français. Ce procédé a pour but d’anonymiser les données transmises.

Exemple : je tape un mot de passe dans mon navigateur pour me connecter à un service "toto1234", ce mot de passe va être "haché" dans une fonction mathématique pour donner un token, en occurrence ici une suite de caractère de taille fixe : "8a1eb5a4df96a2f9a9984a6f61d9357d4c5abe70" . Ce token est ensuite envoyé sur

le serveur qui comparera le token, une empreinte du mot de passe avant de donner ou non l'accès au service.

Imaginons maintenant une entreprise souhaitant lancer un service de partage de fichier en ligne. Ce service proposera d’héberger “au juste prix”, les données de ses clients sans avoir accès à celle-ci. Mais avec l’achat du matériel, la main d’oeuvre et les frais de gestion & marketing, l’entreprise a besoin de 10 millions de dollars afin de pouvoir lancer celui-ci.

Elle décide donc de créer un crypto actif “FIL”, reposant sur Etherium afin de pouvoir financer son service. Il faut donc voir ce nouveau crypto actif “FIL” comme un “token” ou jeton dont la valeur de base est définie par rapport à l'Éther. Un peu comme la valeur d’une action d’une société définie en dollars.

Figure 15 - 1 Ether s'échange contre 10000 "FIL"

À la manière d’une IPO, la société va émettre sur le marché 50 milliards de FIL échangeables contre de l’ETH. La particularité du FIL étant de vous autoriser à héberger 1Go de donnée pour 1 an, et ce pour l’équivalent de 1 FIL soit, lors de son émission sur le marché des crypto actifs : 2 cents.

L’entreprise se prépare à ce que l’on nomme une *“initial coin offering”* ou ICO. Elle va donc mettre en ventes ces FIL et pour chaque achat de ce nouveau token, le prix du FIL va monter, pour chaque vente, il va baisser, exactement comme ce qu’il se passe en bourse. À la différence que les possesseurs de FIL vont pouvoir au choix, revendre leurs FIL au prix du marché contre de l’ETH (le prix du FIL baisse), ou utiliser leurs FIL pour utiliser le service de la société. Dans ce cas les FIL sont de retour dans les mains de la société et elle peut les mettre en vente de nouveau contre de ETH.

Si la société à besoin de cash, elle va vendre une partie de l’ETH récolté pour couvrir ses frais. C’est ensuite à elle de juger si elle souhait à nouveau injecter des FIL dans

le circuit au risque de faire baisser sa valeur, mais couvrir plus d’utilisateurs et faire des économies d’échelles ou au contraire les détruire après utilisation pour contrôler la valeur de ceux-ci.

Ce système permet à l’entreprise de stabiliser les prix de son service en fonction des

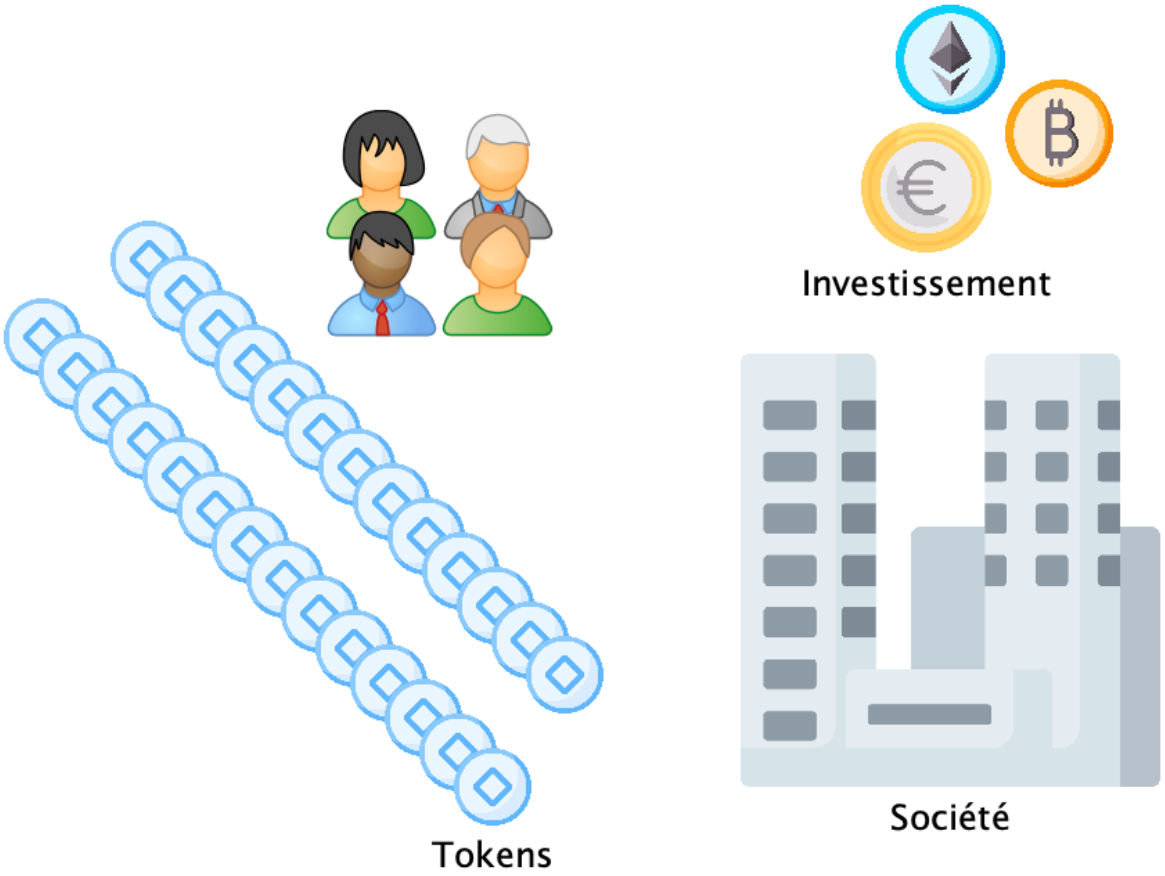

Figure 16 - Principe d'une ICO

couts réels au fil du temps. Mais c’est surtout un formidable outil de financement participatif permettant à n’importe quelle personne possédant de l’ETH ou un autre token, comme le Bitcoin, d’investir facilement dans un projet lui semble prometteur, et le plus souvent avec quelques centimes.

C’est une nouvelle manière de penser le financement de projets, 100% numérique, permettant à tous de participer, via ces “token”, à la création de certains projets innovants. En revanche il faut être vigilant vis-à-vis de ceux-ci, car aucune garantie n’est applicable en cas d'émission d’actifs toxiques sans aucune valeur en échange d'Éther ou de Bitcoin... Moralité, il faut faire attention à ce que l’on “achète”.

Mutations sociétales

Imaginez devoir expliquer en quoi Facebook, TripAdvisor, Uber ou AirBnB va bouleverser les mentalités et la société d’ici une vingtaine d’années dans les années 2000, dix ans seulement après la mise en service du premier serveur web et la naissance d’internet.

La Blockchain est née en 2008 et malgré les innovations présentées précédemment, il est encore trop tôt pour parler de révolution industrielle. La Blockchain n’ayant pas encore infiltré toutes les strates de nos vies comme internet.

Nous pouvons cependant détailler les champs des possibles offerts par cette technologie. À travers cet ultime chapitre, je vais me prêter à un exercice difficile, utilisant le passé et le présent pour dessiner l’avenir, à travers trois visions de sociétés rendues possibles par la Blockchain.

Une société décentralisée et participative.

Aujourd’hui, la technologie et les moyens de production se centralisent. Nous observons la mise en place de gigantesque monopole, au fil des fusions à plusieurs milliards de dollars. L’oligopole, cauchemar absolu du libéralisme, où la libre concurrence n'existe plus, pourrait ainsi devenir réalité.

La Blockchain permet de distiller les ressources et la technologie à travers le monde. Sa puissance augmente avec le nombre d’utilisateurs qui met à sa disposition ses infrastructures informatiques.

Cette vision repose sur un Web décentralisé, sortant de la logique “client-serveur”, avec une vision plus participative du réseau, ou chaque acteur peut contribuer à son bon fonctionnement avec ses propres moyens.

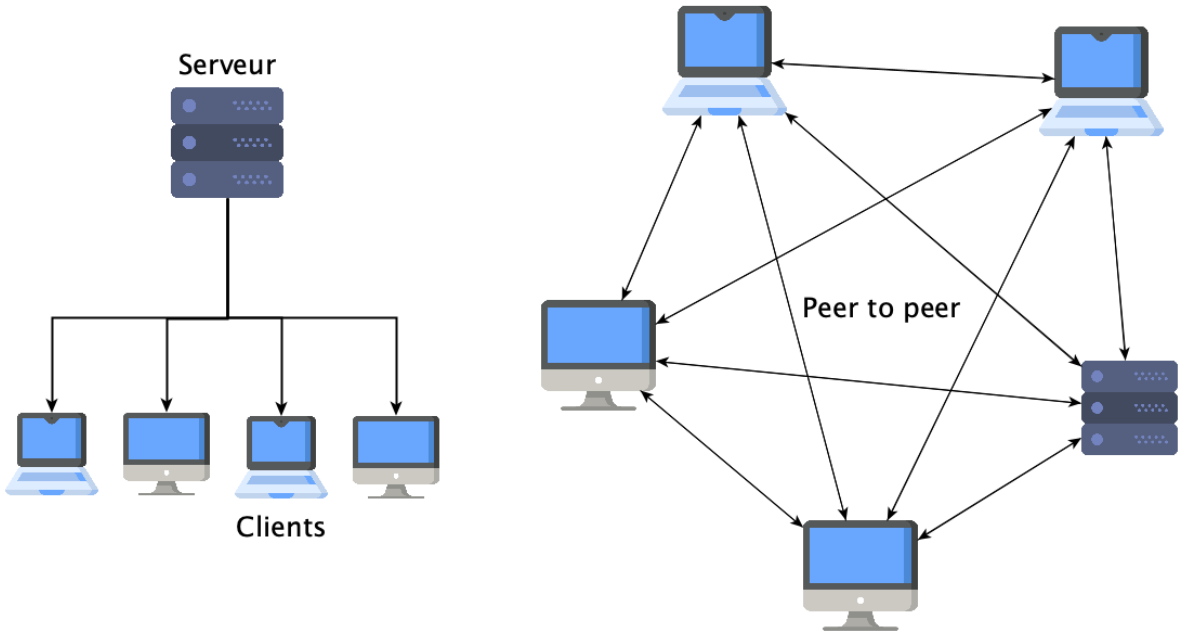

Figure 17 - Modèle client-serveur VS pairs à pairs

Dans ce mode de penser les réseaux, les infrastructures sont partagées avec tous. Avant la technologie blockchain, la plupart des tentatives de rendre le web décentralisé, était complexe, dû à la difficulté d’effectuer une juste rétribution des membres du réseau. La plupart des échanges peer-to-peer[7] étant destinés à des projets open source gratuits ou à de l’échange de fichiers piratés.

[7] Pairs à pairs

Mais avec les nouveaux outils mis en place par la blockchain, comme l’échange de valeur, les contrats intelligents ou la tokenisation. Le web décentralisé peut maintenant se doter d’outils permettant sa généralisation.

Prenons une plateforme d’hébergement vidéo comme Netflix, un abonnement mensuel est payé par l’utilisateur pour profiter du service et les droits de diffusions sont payés par la plateforme pour une durée de diffusion limitée. La plateforme peut ensuite produire ses contenus originaux afin de renforcer son offre et faire grossir ses infrastructures.

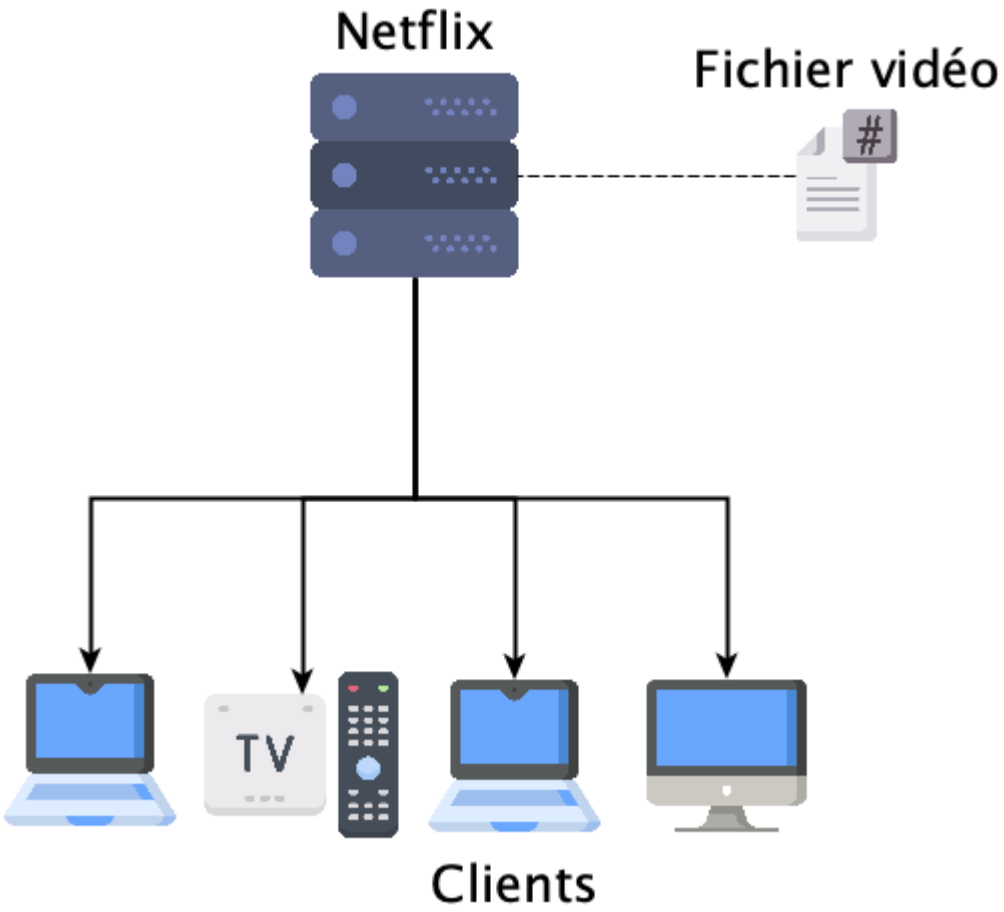

Figure 18 - Fonctionnement de Netflix

Or, imaginons une plateforme de vidéo “VidTrip”, où les créateurs vendent les droits d’accès directement au consommateur, et où les utilisateurs ayant acheté une œuvre sont récompensés en “tokens” pour héberger et distribuer l’œuvre sur le réseau. Ces “tokens” pouvant servir ainsi à acheter de nouvelles œuvres et participer ainsi à la création de nouveaux contenus.

Ici la blockchain permet à tous de publier du contenu sur internet et de garantir un droit d’auteur aux créateurs de contenu. L’utilisateur peut ici au choix, alloué plus ou moins de ressources à l'hébergement du service, ou de dépenser plus ou moins d’argent dans le service. De son côté la plateforme va prendre une commission sur les transactions sur les œuvres, et va récompenser les utilisateurs mettant à profit leurs infrastructures en œuvre à moindre prix.

L’avantage face à Netflix, c’est que les utilisateurs de VidTrip peuvent participer à l’hébergement du service et ainsi consommer des œuvres moins chers, et ce, sans limite de temps. De plus, il n’y a aucune dépendance à un serveur central, les œuvres peuvent sont à de multiples endroits de la planète. Un utilisateur pourrait ainsi héberger un film lu depuis la machine de son voisin de palier, et être récompensé pour ça. Plus besoin d'immenses centres de données consommant d’immenses quantités d’énergie.

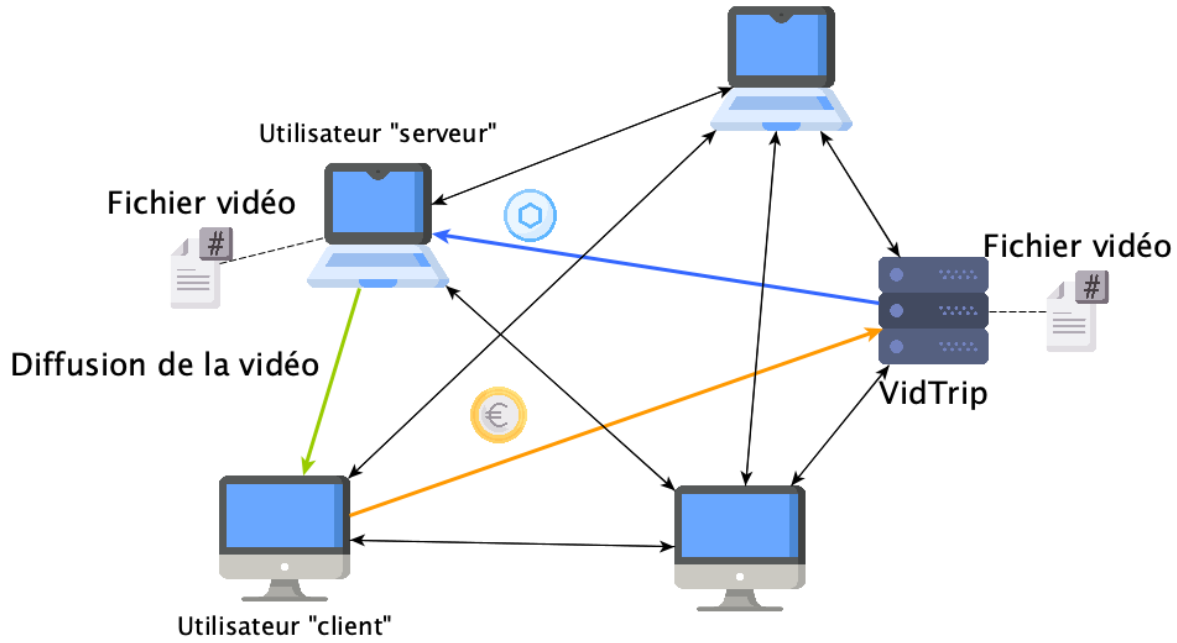

Figure 19 - Fonctionnement de la plateforme VidTrip

Ce modèle n’est pas exclusif à la vidéo, mais est déclinable pour la musique, les livres, les jeux-vidéos ou les logiciels par exemple. On assistera ainsi à une plateforme d’échange d’œuvres numérisées, où chacun participe à son échelle à la sauvegarde et la libre circulation de celles-ci, mais également à la création de nouvelles œuvres en rétribuant les auteurs.

Les droits d’auteurs étant directement inclus dans le prix de distribution, lorsque les films sont coproduits, les différents pourcentages de rétributions attribuer à différents acteurs peuvent directement être “programmé” dans la blockchain.

Ainsi, à chaque vente, une nouvelle entrée s’effectue dans la blockchain exécutant l’ordre de versement pour chacun des acteurs.

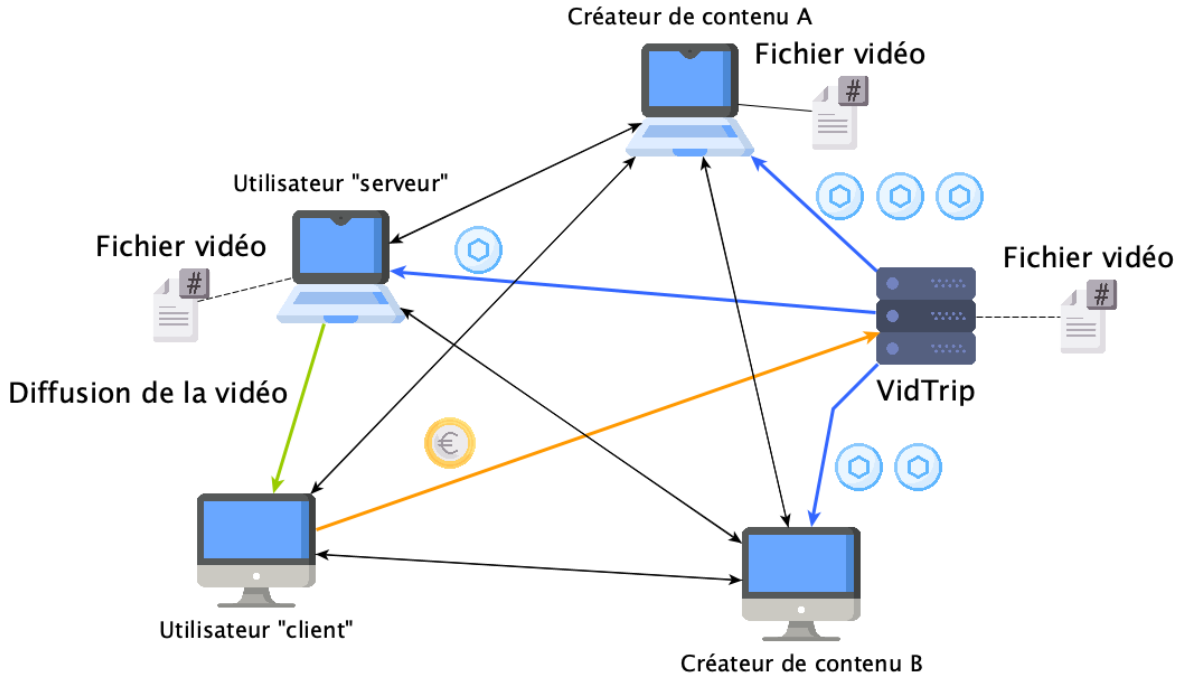

Figure 20 - Répartition des royalties à la suite de l'achat par un utilisateur

Il est aussi possible de mettre en place sur la plateforme des outils anti-plagiat, analysant les contenus, et signant chaque œuvre via un certificat lié aux fichiers. Ce certificat étant sur la blockchain, il devient infalsifiable et permet de s’assurer que la paternité d’une œuvre sera bel et bien respectée.

Ces règles inscrites dans la blockchain permettent donc en résumé de concevoir des règles de distribution, une répartition automatique des royalties et un droit de vote entre les différents acteurs afin de voter l’évolution ou la mise à jour d’une œuvre.

Ce système permet aux œuvres cocréées d'évoluer si une majorité de ses propriétaires le souhaitent. Par exemple, si un livre électronique publié sur la plateforme comporte une erreur et si les propriétaires de l’œuvre souhaitent effectuer une modification, celle-ci sera publiée en lieu et place de la précédente et toutes les personnes ayant achetée cette œuvre recevront la mise à jour.

Cette plateforme, sans la technologie blockchain ne peut pas exister, il faut impérativement un transfert “fluide” de valeur pour récompenser immédiatement chaque acteur de la chaine de distribution. Plus les utilisateurs et les créateurs seront nombreux, plus le système fonctionnera bien commercialement. Plus les utilisateurs augmenteront, plus les créateurs seront récompensés, et plus la qualité du service augmentera. Plus les créateurs augmentent, plus les prix sont en concurrence, et plus le service devient attractif par rapport à l’offre pour les utilisateurs. C’est un cercle vertueux.

Ce qui est intéressant, c’est de voir à quel point le rapport de force change. Avec le trio producteur de contenus - Netflix - utilisateurs, ce sont les utilisateurs qui “subissent” les choix de Netflix en termes de catalogue, celui-ci doit quant à lui négocier avec les producteurs des droits de diffusions. Le pouvoir est entre les mains de Netflix et des producteurs ici.

Tandis que sur le modèle de notre exemple “VidTrip”, la plateforme établie les règles du jeu et un équilibre se créer entre les utilisateurs, tantôt hébergeur pour la plateforme qu’investisseur dans les œuvres des producteurs, et ces mêmes producteurs de contenus profitant du marché à leurs dispositions pour engranger des gains que d’une infrastructure fiable, décentralisée et résiliente.

La blockchain étant le “cadre”, la règle du jeu inviolable, dans lequel les différents acteurs interagissent et échangent de la valeur ou des services, sans intermédiaires.

Une société démocratique et désincarnée.

La blockchain étant une plateforme regroupant de nombreux outils tels que les contrats intelligents, des méthodes de certifications, un système d’échange monétaire. Avec ces outils, nous pourrions très bien construire une entité, décentralisée, régie par des statuts programmés dans des contrats intelligents, possédants des actionnaires choisis grâce à une ICO. Lors des assemblées générales de cette entité, les décisions seraient votées en dépensant des “token” pour ou contre certaines décisions. Nous aurions ici, une version décentralisée de nos sociétés anonymes…

Ce nouvel organisme numérique et décentralisé se nomme DAO pour *Decentralized Autonomous Organization*[8]. Ces nouveaux organismes décentralisés évoluent en autonomie sur internet, dématérialisé de tout carcan étatique ou physique, permettent d’offrir un nouveau modèle de gouvernance 100% en ligne.

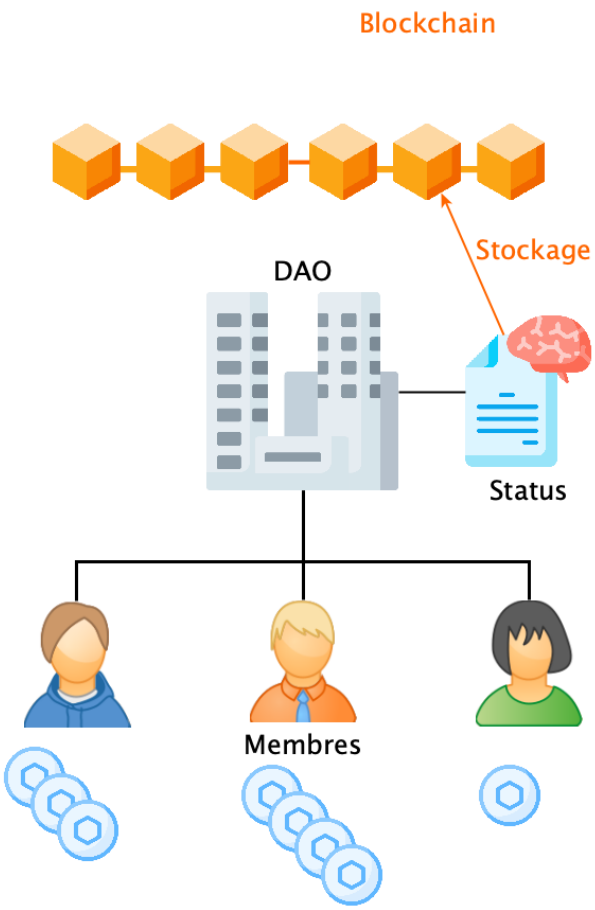

Figure 21 - Exemple de DAO

[8] Organisation autonome décentralisée.

Une entreprise proposant un produit se reposant sur une infrastructure numérique peut ainsi utiliser les mécanismes et outils offerts par la blockchain pour réorganiser sa gouvernance.

Ces DAO, sont des regroupements de personnes, dont les intérêts économiques, politiques et sociétaux convergent autour d’un projet commun. Inspiré de la mouvance “open source”, ce nouveau système de gouvernance met en place un système de vote horizontal et décentralisé, basé sur les mécanismes de tokenisations de la blockchain.

Prenons l’exemple de notre société de vidéo à la demande VidTrip. Typiquement, les actionnaires de la société seraient remplacés par des propriétaires de tokens. Pour rappel, il y a globalement deux façons d’obtenir des tokens :

- Participer à la plateforme en mettant à disposition ses infrastructures et/ou son expertise. Puis être récompensé en token fraichement créé par la plateforme pour son service rendu.
- Acheter des tokens sur le marché en échange de monnaie fiat ou d’autres crypto actifs (Bitcoin, Éther, etc…)

En termes de gouvernance, pour les DAO, le processus de décision n’est pas démocratique (un individu, une voix), mais méritocratique.

Dans les tokens d’une DAO, il est inscrit leurs provenances via l’historique des transactions qui leur est associé. Pour chaque individu, il est facile de noter le pourcentage de tokens fraichement créer par la participation d’un individu par rapport à des tokens acheter sur le marché de l'occasion.

Ainsi pour voter les décisions sur l’évolution de la plateforme “VidTrip”, notre DAO d’exemple, il faut prendre en compte le nombre de “token” d’un individu et le ratio neuf/occasion de ceux-ci pour accorder plus ou moins de poids à ses avantages ou son pouvoir décisionnel sur l’organisation.

$$R = \frac{Total\ tokens\ "neufs"}{Total\ tokens\ "occasions"}$$

Dans ce système de DAO, l’économie est circulaire et en vase clôt, les systèmes de récompenses et de rétribution sont indexés sur le token et le seul moyen de convertir cette valeur virtuelle en monnaie fiat est de vendre son pouvoir de décision sur le marché.

Ce système de gouvernance plus fluide et dynamique permet à la DAO de croitre et de se développer grâce à ses plus actifs contributeurs, en équilibrant le pouvoir

décisionnel entre les investisseurs et les producteurs de ressources, à valeur de token égale, les contributeurs engagés étant prioritaires vis-à-vis des spéculateurs.

Dans ce modèle, il est également intéressant de noter que chaque membre, en échange d’une “mise”, peut soumettre une proposition aux votes d’actionnaires de la DAO. Pour chaque vote, le votant investi un nombre de tokens notés ci-dessous x, le poids de son vote est noté V(x) :

$$V(x) = R \times x$$

Une fois la proposition soumise, les votants investissent un % de leurs tokens et indique leur accord ou désaccord dans le projet. Après le calcul du ratio neuf/occasion de chaque contributeur les % de pour et contre sont calculés. Une fois le vote terminé, la somme “investie” dans le vote est utilisée pour acter le vote.

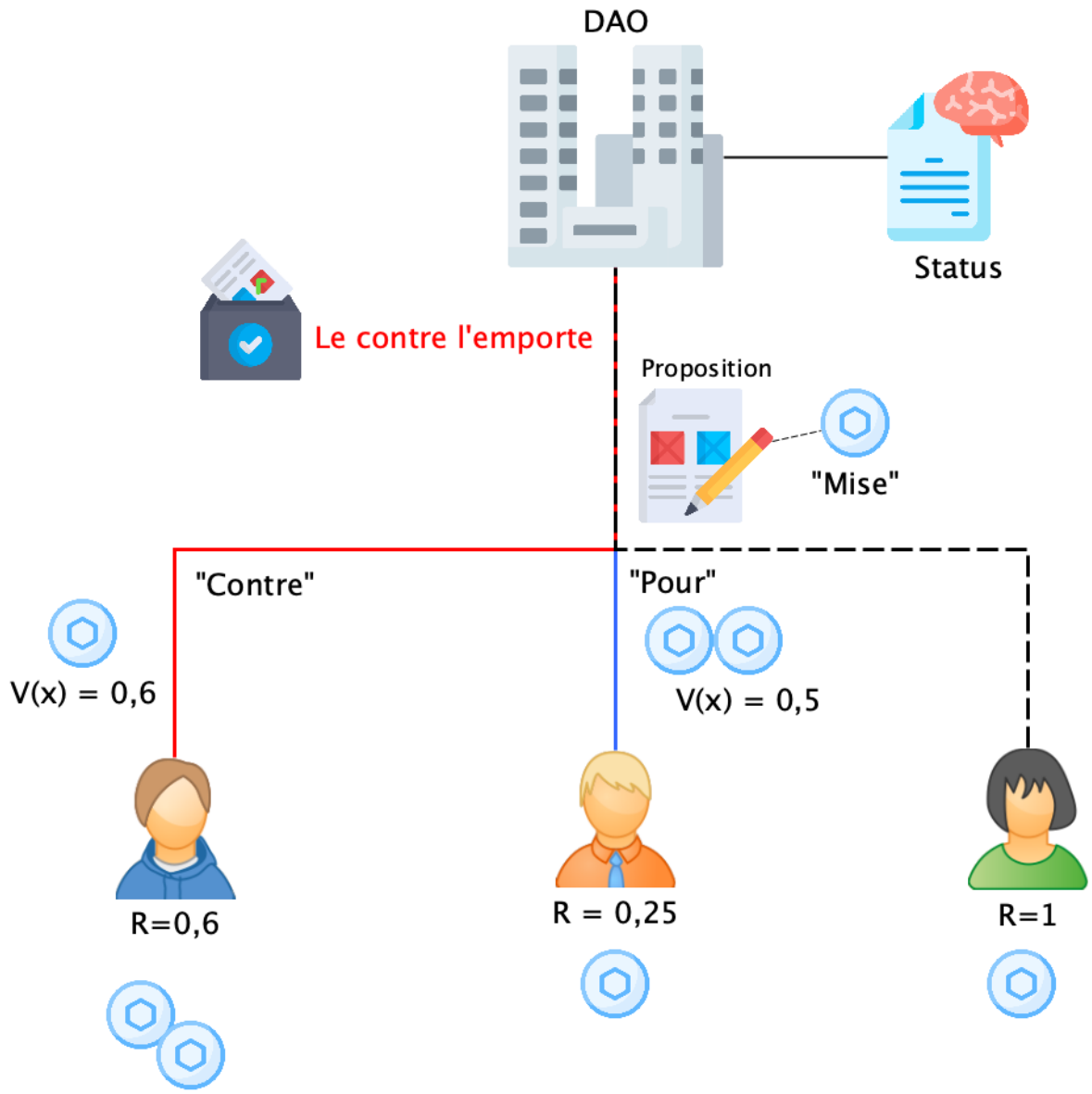

Figure 22 - Un vote dans une DAO

Ces décisions étant inscrites dans la blockchain et propagées sur son ensemble nous avons également une parfaite traçabilité et contrôle de ces votes.

Avec la blockchain comme support, les DAO repensent la création de valeur avec un focus sur la production et la décentralisation du pouvoir. Elles instaurent un équilibre entre l’investissement et la contribution rendant les règles de gouvernances plus méritocratiques. Elles sont une évolution de nos entreprises classiques, disruptives et numériques.

Mais ce modèle de gouvernance ne s’arrête pas aux sociétés privées, mais pourrait bien entendu s’étendre au milieu associatif ou même étatique.

Imaginons un état, mettant en place une blockchain rendant possible la mise en place d’initiatives populaires en ligne. Les tokens utilisés pour ce vote pourraient avoir deux sources différentes :

- Les fonctionnaires de l’état, ou tout citoyen mettant à disposition leur énergie et leur travail pour son bon fonctionnement seraient récompensés par des tokens “neuf” créés pour eux.
- Les citoyens pourront alors échanger les tokens contre de la monnaie fiat via les impôts, l’investissement dans l’état ou l’achat direct envers les propriétaires de ce token.

Enfin, chaque citoyen pourrait alors voter des lois ou investir ces tokens dans des projets nationaux ou locaux.

De plus, afin de garantir un équilibre entre les personnes les plus engagées et les simples spéculateurs, le même ratio neuf/occasion sera appliqué aux votations.

La traçabilité serait garantie par la parfaite lisibilité des votes dans la blockchain et l'incorruptibilité du système. Ce système méritocratique permettrait également de mettre en avant les citoyens s'investissent dans l’état en leur accordant une plus grande voix. Mais l’inverse est également vrai, si une minorité profite de ce pouvoir aux dépens des autres, la majorité peut choisir d’investir plus pour contrer un vote.

Une société technocratique et rigide.

Dans cette ultime partie, nous allons aborder une réalité qu’il ne faut pas oublier quand on parle de technologie innovante : aucune invention scientifique ou technique n’est neutre. Une technologie reste avant tout un outil utilisé par l’homme pour accomplir un objectif, qu’il soit moral ou non…

La blockchain ne faisant pas exception, il faut rester vigilant sur son utilisation.

Pour rappel, tout ce qui est inscrit dans une blockchain y est inscrit pour “toujours”, il est impossible de modifier ou de supprimer une entrée. En d’autres mots, si vous effectuez une transaction, il est impossible de l'annuler une fois l’ordre envoyé, il n’y a pas de droit à l’erreur ni de “remboursement automatique” possible en cas d’erreur.

C’est également valable pour les contrats intelligents, celui-ci s'exécutera automatiquement une fois que vous l’aurez numériquement signé. Aucune des parties signataires ou quelconques autres entités ne pourra annuler celui-ci.

De manière générale, une fois une action effectuée et authentifiée par une signature électronique, il est impossible de revenir en arrière.

En cas d’usurpation de votre clé privée, utilisée pour “signer” vos actions sur la blockchain, il n’y a aucun recours. Le pirate peut agir en votre nom et utiliser vos cryptoactifs comme bon lui semble.

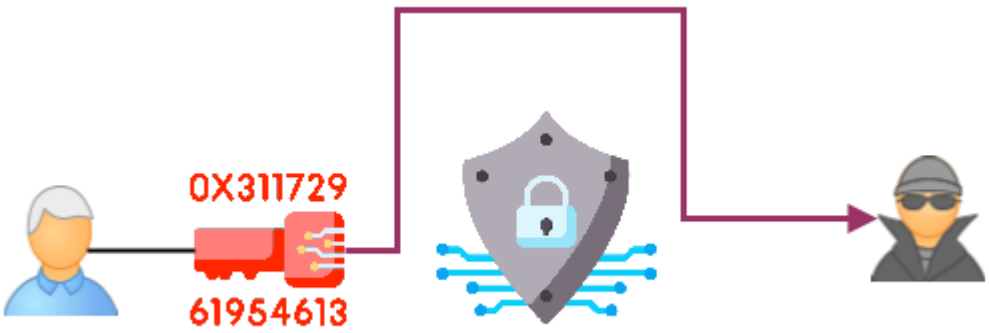

Figure 23 - Usurpation d'identité

On note ici que cette technologie, supprimant les intermédiaires et les entités tierces, supprime de facto toutes actions ou intervention humaines dans ce système. Seul l’algorithme est garant des lois du système et si celui-ci est soumis à un dilemme : être libre de tout contrôle “humain” et garantir une sécurité maximale, en limitant au maximum les vulnérabilités, ou être moins extrême, en mettant en place des mécanismes d’interventions dans la gouvernance en cas d'extrême urgence.

Etherium a par exemple été soumis à ce cas de figure le 17 juin 2016, à la suite d’un gigantesque piratage d’une organisation décentralisée, “the DAO”.

En une journée, le pirate a pu transférer depuis le contrat intelligent de cette organisation l’équivalent de 3 millions de tokens, soit près 50 millions de dollars, sur un de ses propres contrats intelligents. À l’issue de 35 jours suivants, le piratage, les fonds seront envoyés de ce contrat intelligent jusqu’aux comptes du pirate.

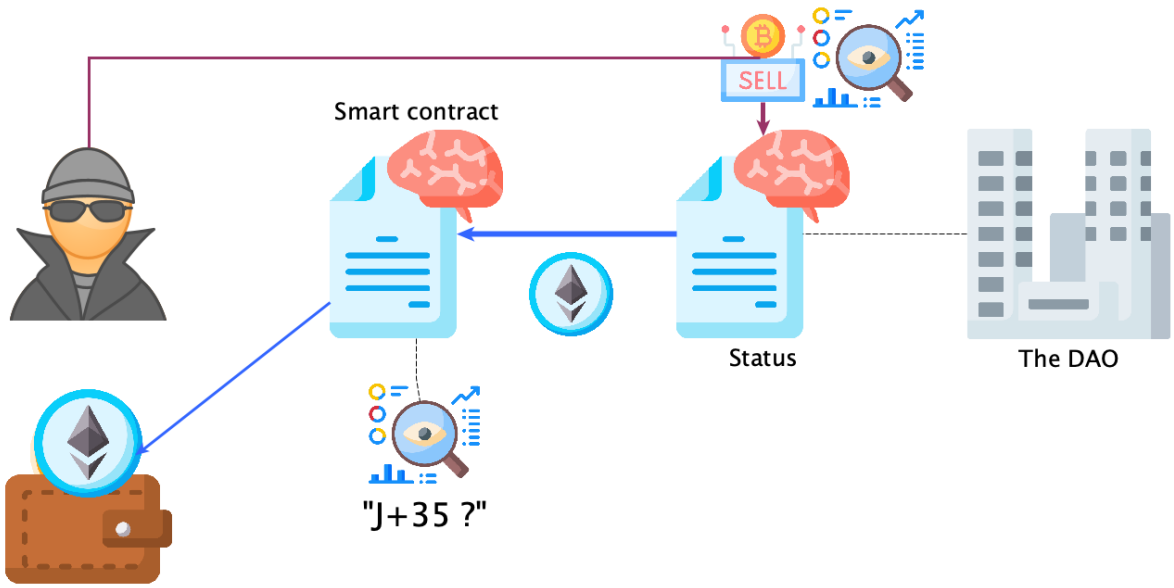

Figure 24 - Piratage de "the DAO"

Durant les 35 jours suivants, ce piratage, l’ensemble des programmeurs derrière la blockchain Etherium et l’ensemble de la communauté ont dû choisir entre respecter l’immuabilité de la blockchain, et donc ne rien changer et laisser le pirate user librement de ces tokens, ou bien exceptionnellement, “effacer” les transactions suspectes et rembourser les personnes ayant investi dans “the DAO”. La communauté a finalement décidé, en majorité, de rembourser les personnes ayant été lésées.

Le 23 juillet, jour J ou le contrat intelligent devait arriver à son terme, Etherium se déchire en deux avec d’un côté, Etherium Classic (ETC), et de l’autre Etherium (ETH). Etherium classic étant une blockchain immuable, dans laquelle le code fait loi, et qu’aucun retour en arrière n’est possible. L’autre, Etherium, une version de la blockchain originelle où le piratage n’a pas eu lieu et tous les utilisateurs ont pu récupérer leurs argents.

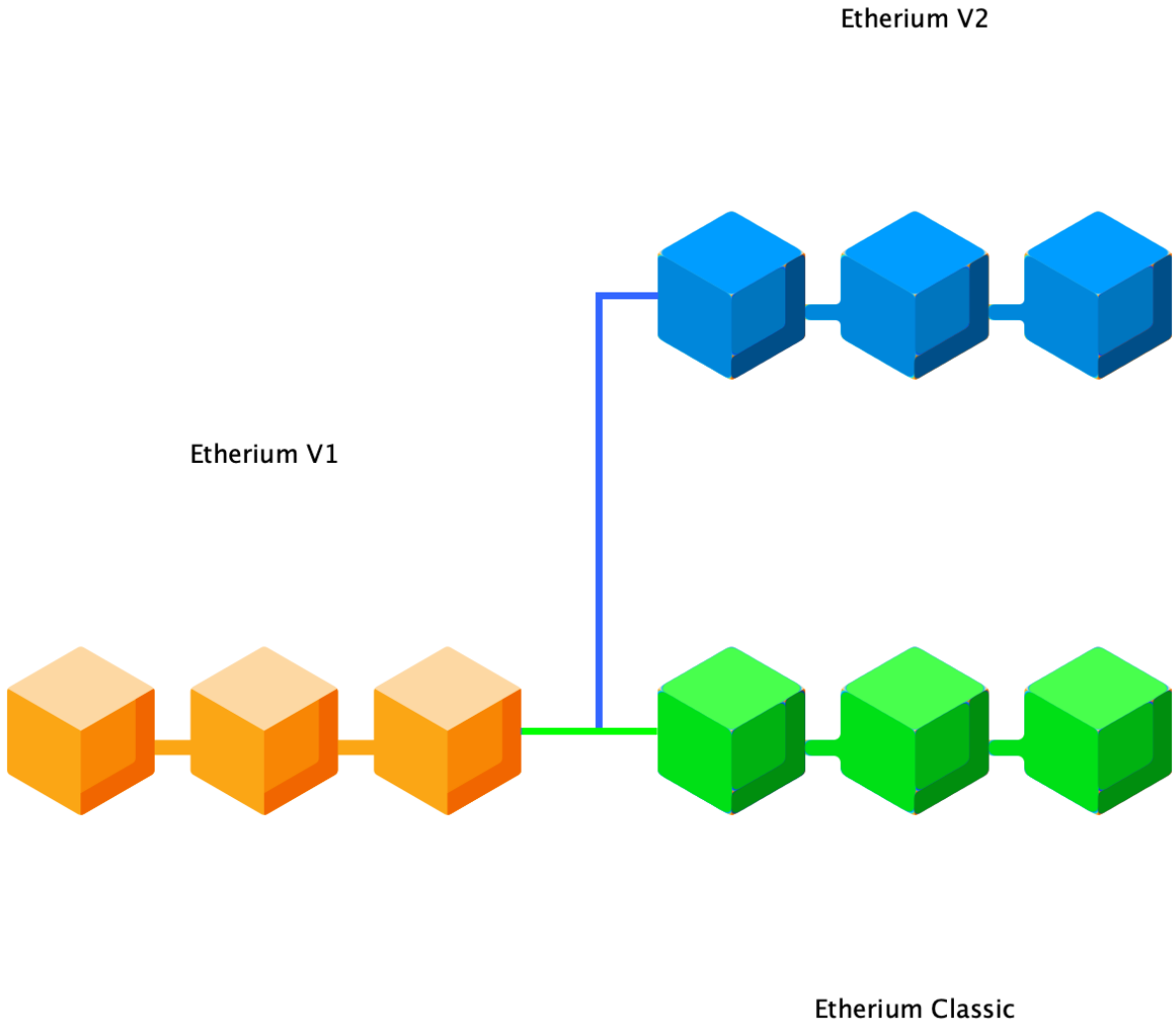

Figure 25 - Fork de la blockchain Etherium en juillet 2016

Pour plus de sécurité, l’on doit faire intervenir la majorité des acteurs pour mettre en place le moindre changement dans l’organisation. Et les personnes en contradictions avec la majorité peuvent tout à fait décider d’effectuer une bifurcation (plus communément appelé “fork”). Afin de faire vivre leur vision en parallèle avec celle de la majorité.

La multiplicité des acteurs et utilisateurs de la blockchain participe à la complexité de gouvernance et à la difficulté d’établir un consensus clair. On ne peut établir aussi rapidement et efficacement des décisions que sur un modèle de gouvernance classique. Mais cette multiplicité d’acteurs et la complexité du processus de validation sont le prix de la sécurité.

Par ailleurs, le piratage n’est pas payant sur la blockchain, puisque l’ensemble des transactions étant connus par tous, il est très facile d'identifier si un compte stocke des tokens précédemment piratés, aussi l’on pourrait imaginer un registre, une sorte de

liste noire, où serait stocké les numéros de compte frauduleux ou ayant accepté des tokens frauduleux et choisir de ne pas accepter les tokens qui en émane.

Mais si le pirate décide de passer à la vitesse supérieure et décide d’attaquer un à un différents noeuds où sont sauvegardées les copies de la blockchain ?

La validation des transactions s’effectuant par consensus majoritaire, il faudrait qu’un utilisateur maitrise plus de 51% des nœuds de transactions où sont stockées les copies de la blockchain pour pouvoir réécrire l'ensemble des transactions et règles d’échange à sa guise.

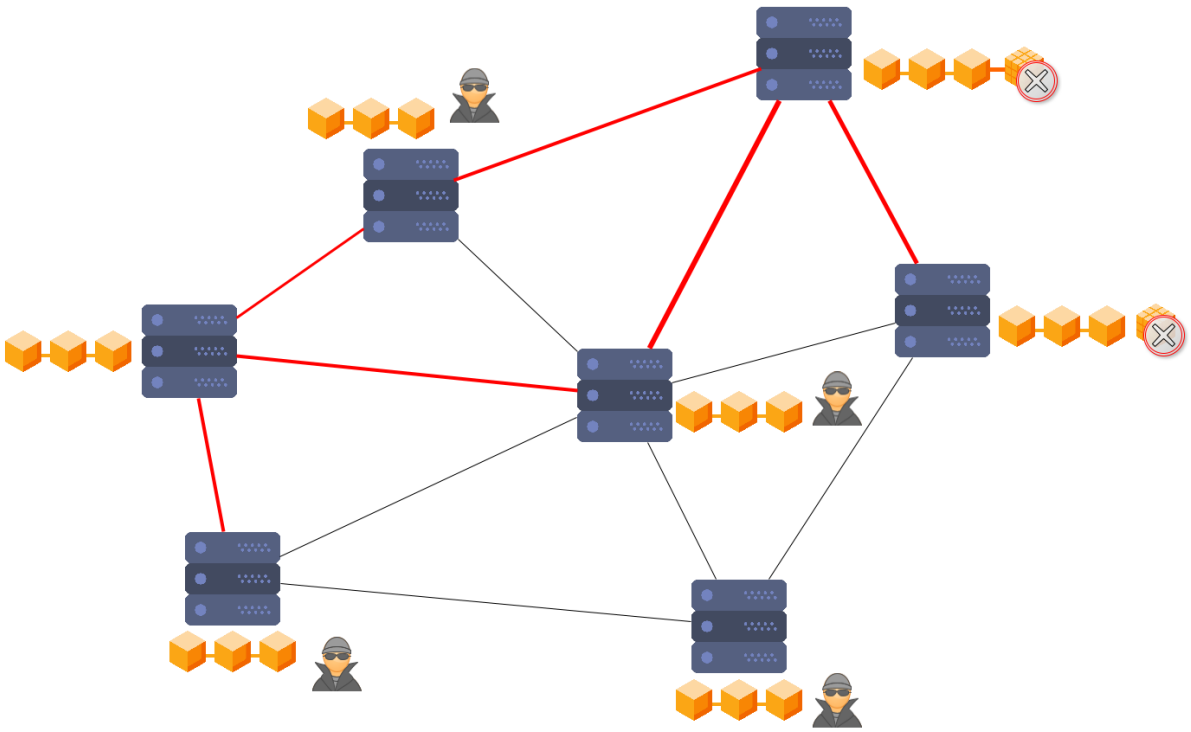

Figure 26 - Attaque dite des "51%"

Mais en faisant cela, celui-ci fera perdre instantanément toute confiance en cette blockchain, poussant ces utilisateurs à effectuer un “fork” vers une version plus stable et équitable. Cette blockchain piratée devenant ainsi sans aucune valeur.

Si la rigueur apparente de cette technologie peut effrayer, il est intéressant de noter que deux visions sont concurrentes et s’opposent au sein de la blockchain. D’un côté la vision d’une blockchain “outil logiciel”, étant avant tout implémenté pour servir à l'innovation. Et de l’autre, un objet technologique idéalisé, au-dessus de toute intervention humaine, véritable esprit synthétique et décentralisé, hors de contrôle.

En réalité, je pense qu’elle est un peu des deux : elle est avant tout un outil d’avenir, permettant de créer des applications décentralisées tournées vers l’avenir, mais également un outil solide à la gouvernance complexe.

Cet équilibre, demeurant fragile, est nécessaire, il ne faut pas que l’un prenne le dessus sur l’autre pour que la généralisation de cette technologie se poursuive.

Conclusion

La blockchain est résolument une technologie singulière, extrêmement complexe et difficile à appréhender pour les néophytes. Mais avant tout, c’est un concept, reposant sur des technologies préexistantes. Une boite à outil, pour construire l'innovation.

En offrant un cadre et une myriade d’outils à tout un chacun sur internet, elle permet la dématérialisation de valeur et des règles de gouvernances tout en garantissant un mécanisme de sécurisation fiable, algorithmiquement sûr, où chaque acteur peut participer et commencer à créer de la valeur.

Aujourd’hui, sa résilience n’en est pas moins éprouvée. C’est en partie grâce à la recherche, aux évolutions et à la croissance toujours plus constante de ses usagers que la blockchain se transforme et évolue, prenant des formes et applications multiples, pour devenir toujours plus élaborée et résistante.

Mais c’est surtout ces applications dans les domaines politiques, économiques et sociétaux qui font d’elle une véritable révolution disruptive : nouveaux systèmes de gouvernances participatives et méritocratiques, entreprises décentralisées dont les ressources servent la création de valeur, assurance automatisée, certification des matières premières et traçabilité des marchandises, les champs d’applications sont multiples et la majorité des usages restent encore à découvrir…

Mais au-delà des applications, c’est une nouvelle idéologie qui émerge, centrée sur la liberté et l’émancipation de l’individu face aux limites d’un système centralisé. Via la blockchain chacun est libre de mettre à profit son temps, ses infrastructures, son argent, ses compétences et d’obtenir sa part de pouvoir sur le système global, cristallisé ici, en “token”.

Internet a digitalisé nos moyens de communication, la blockchain est quant à elle en train de digitaliser nos systèmes d’échange de valeurs et de gouvernance.

Mais pour que cette digitalisation réussisse, le pouvoir doit également être réparti sur l’ensemble des acteurs et utilisateurs d’internet. Et c’est bien ici que se joue cette révolution, dans la décentralisation.

C’est un bouleversement sociétal qui va voir émerger de nouveaux acteurs, capables sans doute de mettre fin à l'hégémonie de la centralisation des pouvoirs politiques, économiques et sociétaux. Des acteurs inarrêtables, dirigés et alimentés par les actions d’une multitude de citoyens, surpassant en nombres et en ressources GAFAM, partis politiques, ou banques.

La question ne serait donc pas de savoir si la blockchain amènera à une quatrième révolution industrielle, celle-ci est déjà en marche. Mais plutôt quand la blockchain et son idéal de pouvoir décentralisé deviendront incontournables dans notre vie à tous ?

Bibliographie et webographie

Blockchain et cryptomonnaies - Primavera De Filippi

Blockchain pour l’énergie - Karim Beddiar & Fabien Imbault

Blockchain, la révolution de la confiance - Laurent Leloup

Livre blanc Bitcoin - Satoshi Nakamoto

Livre blanc Etherium - Vitalik Buterin

Article sur le piratage de "the DAO" - Vitalik Buterin

fizzy by AXA: Etherium Smart Contract in details - Alexandre CLEMENT

IBM Foodtrust website

Cryptoqueen: How this woman scammed the world, then vanished - BBC

Table des figures