Le web et ses usages sociétaux

Table des matières

1. Du Web aux réseaux sociaux....2
    1.1. Web et Internet....2
    1.2. Web 2.0....2
    1.3. Les réseaux sociaux....3
    1.4. Hashtag....4
    1.5. Les matrices....4
    1.6. Evolution des modèles....5
2. Le Cloud....6
    2.1. Qu'est-ce que le Cloud ?....6
    2.2. Les data centers....6
    2.3. Sécurité....7
3. Du bitcoin à la blockchain....8
    3.1. L'argent dématérialisé....8
    3.2. La Blockchain....8
    3.3. La cryptographie....8
    3.4. Les applications de la blockchain....9
    3.5. L'impact écologique....10
Glossaire....10

Internet, Web 2.0, Web mobile, réseaux sociaux, médias sociaux… Ces mots que l'on imagine volontiers interconnectés mais qui ne désignent pas les mêmes dispositifs socio-techniques font désormais partie du vocabulaire courant non seulement des individus et des groupes, mais aussi des sciences humaines et sociales.

1. Du Web aux réseaux sociaux

1.1. Web et Internet

Qu'est-ce que le Web ? Ou plutôt qu'est-ce que le Web n'est pas ?

Et notamment parce que les gens font l'amalgame souvent entre Web et Internet. Le Web, ça n'est pas Internet. Internet, c'est un ensemble de standards e t de technologies qui nous permettent de relier des ordinateurs entre eux et de relier les réseaux entre eux. On peut voir ça un peu comme un réseau routier sur lequel vont transiter différents types de services, de marchandises, de personnes, de véhicules. Sur ce réseau routier, comme on a différents types de marchandises, sur Internet, on va voir différents types d'application.

Le Web, c'est une de ces applications qui va transiter sur ce réseau. Mais on en a d'autres, par exemple, l'email, la téléphonie à travers Internet est un troisième exemple. Il faut bien faire la différence entre cette infrastructure de réseaux reliés entre eux qui est Internet et une des applications au-dessus de cette infrastructure qu'est le Web.

Après le Web, a été développé comme une application au début pour partager de l'information qui date de la fin des années 80, début des années 90 au CERN. L'idée est de relier des documents entre eux pour permettre d'accéder à ces documents même s'ils ne sont pas sur la même machine. Au début, c'est pour des scientifiques et puis cela va s'ouvrir au grand public très rapidement : le Web va devenir un cette toile mondiale.

Le Web en lui-même est à la fois les standards qui permettent de créer cet objet et puis l'objet qui en émerge, la toile mondiale sur laquelle on se balade tous les jours. Dès le début du Web, on a deux facettes :

- une facette documentaire, qui va nous permettre de relier des documents entre eux qui sont sur différentes machines. Mais on a aussi cette idée que différentes personnes vont contribuer à différents documents sur différents serveurs.
- une facette sociale dès le départ puisque ça va permettre une certaine interaction entre les différents contributeurs.

Au début, le Web et est ouvert en écriture, mais très peu utilisent cette possibilité. La plupart des premiers serveurs Web seront juste accédés en lecture. Et il faut attendre le mi lieu des années 90 et la réouverture du Web en écriture notamment avec les wikis pour avoir à ce moment-là, la possibilité de voir tout le monde contribuer. C'est vraiment à ce moment-là qu'on va basculer vers le Web social et toutes les applications sociales que l'on connaît maintenant sur le Web.

1.2. Web 2.0

Les réseaux sociaux prennent vraiment beaucoup de formes différentes, mais on va dire une définition d'un réseau social actuellement comme on l'entend dans les journaux, c'est une application qui va utiliser le s sciences et technologies de l'information, donc le Web, Internet, les mobiles pour mettre en lien des personnes. Elles ont ça en commun.

Après ces différentes applications vont se différencier, par exemple en termes d'usage. Est-ce qu'il s'agit de relier entre eux des CV comme sur LinkedIn ou d'échanger des messages plus ou moins sérieux comme sur Facebook. Elles vont se différencier en type de liens dans le réseau. Par exemple, est-ce que c'est un réseau d'amis ? Est-ce que c'est un réseau professionnel ? Est-ce que

c'est un réseau basé sur les centres d'intérêt ? Elles vont aussi se différencier en termes de moyens d'accès. Est-ce qu'on y accède à travers le Web ou est-ce qu'on y accède à travers un mobile par exemple. Elles vont se différencier en termes de contenus échangés. Par exemple, est-ce qu'on échange des vidéos ? Est-ce qu'on échange des messages courts ? Et donc tous ces aspects vont différencier les différentes applications des réseaux sociaux. Et notamment, on va parler aussi d 'une notion un peu plus particulière qu'on appelle les médias sociaux. C'est-à-dire à partir du moment où ce réseau social permet de produire et d'échanger des contenus, par exemple YouTube est un média social.

On peut aussi faire la différence par exemple entre des réseaux sociaux explicites, c'est-à-dire des réseaux sur lequel on va effectivement donner les différents types de liens qu'on a avec les autres personnes, déclarer activement ces liens. Donc par exemple, quand je suis sur LinkedIn, je vais déclarer le lien avec une personne activement. Et puis des réseaux sociaux qu'on peut qualifier d'implicites, c'est-à-dire qu'ils sont calculés par rapport à l'activité de leurs utilisateurs. Par exemple en sciences, on a des applications sociales comme ResearchGate qui permettent aux scientifiques de poster et de maintenir leur bibliographie, l'ensemble des articles qu'ils écrivent. Et à travers cette activité et en regardant par exemple quelles sont leurs co-auteurs, on peut en déduire un réseau social implicite à cette activité.

Autre exemple de différences qu'on peut faire aussi entre ces applications : est-ce qu'elles sont essentiellement liées au Web ? Ou est-ce qu'elles sont essentiellement liées à d'autres plateformes ? Par exemple, une application comme Tumblr est née et est définitivement ancrée sur le Web. Alors que des applications comme WhatsApp ou Snapchat sont nées et elles sont essentiellement utilisées à travers les réseaux mobiles.

Pour conclure, on pourrait dire qu’on a à la fois un tronc commun qui est cette idée que ce sont des applications qui utilisent les nouvelles technologies de l'information pour mettre des liens entre les personnes, pour permettre de créer des liens entre personnes. Et en même temps, elles ont un ensemble de différences à travers leurs usages, les types de contenus, les types de liens qu'elles permettent de créer.

1.3. Les réseaux sociaux

Les réseaux sociaux, ils n'ont pas attendu ni Internet ni même l'informatique pour exister en fait. Cela existe depuis très longtemps, la notion de réseau social, de structures sociales à la fois leur importance ; avoir un réseau, c'est une expression qu'on connaît bien ; et l'étude aussi, en sociologie, l'étude de ces structures date de très longtemps.

Et même en informatique, si on regarde les débuts, cela prédate même Internet :les bulletin boards, un système BBS, ont commencé à être utilisés avant Internet dans les années 70. Après, il y a eut des applications comme Usenet, les newsgroups qui elles aussi, ne vont pas attendre le déploiement complet d'Internet pour être utilisées. Et puis dans la continuation, on va avoir le mail avec les mailing lists. On va voir les IRC pour les chats synchronisés. Donc la communication plutôt synchronisée. Et les forums ou les chat rooms, les salles de discussion commencent très, très tôt en informatique.

Après ce qui va se passer, c'est effectivement non seulement le déploiement d'Internet, mais surtout le déploiement du Web. Et avec le déploiement du Web une bascule dans les années 90 parce que le Web non seulement démocratise l'accès à Internet, il n'y a pas que des technophiles qui accèdent d'un seul coup à cet espace. Mais en plus en même temps, le Web a une transformation et devient social. C'est-à-dire, ce n'est plus une bibliothèque comme on l'a autour de nous ici, mais c'est un

endroit où tout le monde va pouvoir contribuer, écrire. Et donc à la fois grand public et à la fois ouvert à l'écriture et donc on a un espace où on va pouvoir déployer des applications sociales. Au début, assez simple comme Six Degrees pour simplement dire qui était son camarade de classe avant. Et puis petit à petit, des applications comme les wikis, les forums, les blogs qui vont permettre la contribution et donc les médias sociaux.

1.4. Hashtag

Quand on a besoin de représenter ou de modéliser ces réseaux sociaux, en mathématiques, en informatique, dans les sciences du numérique, le premier objet qu'on veut utiliser, le premier type de modèle en fait ce sont des graphes, pour capturer la structure du réseau social. Alors dans un graphe, on trouve des nœuds qui représentent par exemple les personnes, et puis on va trouver des arcs qui représentent les liens entre ces personnes. Et puis à partir de ça, on va très vite voir que ce modèle de graphe va pouvoir s'enrichir, et qu'on va avoir différents types de graphes pour représenter différents types de réseaux sociaux.

Par exemple, si dans un réseau social je peux avoir plusieurs liens avec une personne, par exemple un lien familial et un lien professionnel, alors on va passer du graphe au multigraphe, c'est-à-dire, on va avoir la possibilité de faire des arcs entre 2 mêmes nœuds, plusieurs arcs.

Si je m'intéresse par exemple à des réseaux dans lesquels les relations sont orientées, par exemple dans Twitter, la relation dans Twitter, je suis quelqu'un mais la personne n'est pas obligée de me suivre, donc il y a un sens à la relation, alors je vais utiliser des graphes orientés. Alors que pour Facebook, je n'en ai pas besoin parce que la relation par défaut d'amitié elle est symétrique donc je n'ai pas besoin d'orienter mon graphe.

Je vais aussi être amené à regarder s'il y a différents types de liens dans mon réseau, par exemple sur LinkedIn, je peux avoir un lien professionnel, ou d'autres types de liens, et donc on va s'intéresser à des types de graphes qu'on dit "étiquetés", c'est-à-dire qu'on va mettre sur les arcs du graphe différents types de liens. Les graphes, c'est un exemple parmi d'autres, on peut aussi s'intéresser par exemple à représenter des communautés, donc on ne regarde plus vraiment la structure du réseau social, mais on va regarder des groupes à l'intérieur, par exemple des gens qui ont les mêmes centres d'intérêt. Et même d'un point de vue mathématique, là où on utilise des graphes, on pourrait utiliser d'autres structures, comme les matrices.

1.5. Les matrices

Une matrice peut être construite à partir d'un graphe, notamment ce qu'on appelle une matrice d'adjacence, c'est-à-dire que pour chaque arc que j'ai dans mon graphe, pour chaque lien que je vais avoir dans mon réseau social, je vais mettre dans ma matrice un petit 1 pour dire que j'ai une relation.

Par exemple, si je prends une matrice d'adjacence, les colonnes et les lignes ont tous les nœuds de mon réseau, et s'il y a un lien entre 2 nœuds de mon réseau, je vais mettre dans la petite case à l'intersection de la colonne et de la ligne correspondante, pour indiquer que j'ai un petit arc, je mets un 1.

Cela peut être amené à évoluer, par exemple si demain je m'intéresse à des réseaux dans lesquels on met des poids, c'est-à-dire par exemple pour représenter la certitude que j'ai sur une relation ou la force qu'il y a entre la relation de 2 personnes, je vais avoir ce qu'on appelle un graphe pondéré, et de façon symétrique je vais avoir une matrice d'adjacence, où au lieu de mettre des 1 dans cette matrice, je vais mettre des petits poids pour indiquer à quel point la relation est forte. Donc, en

fonction des différents types de réseaux, je vais être a mené à utiliser différents types de modèles, mais aussi en fonction des différents types de traitements que je vais vouloir faire dessus.

1.6. Evolution des modèles

Alors il y a beaucoup d'enjeux scientifiques et techniques en fait avec ces réseaux sociaux, on vient d'en voir une avec la question des modèles, c'est déjà une question scientifique : quel modèle je peux choisir pour représenter, stocker ces données du réseau social ? Comment ce modèle peut être implémenté de façon efficace en machine pour prendre le moins d'espace possible, pour être indexé le plus efficacement possible, pour permettre l'accès le plus efficacement possible ? Mais aussi comment je peux le distribuer sur plusieurs machines lorsqu'il devient trop gros et qu'il ne tient pas sur une machine ? Donc déjà la question du modèle, de la représentation, du stockage et de la gestion de ces données pose des questions scientifiques et techniques.

Après, en informatique, il y a toujours ces deux aspects, la structure de données et l'algorithme, et donc se pose aussi la question du traitement que je faire sur ces données, et là les traitements peuvent être extrêmement complexes. Ils sont difficiles à deux titres, d'une part parce qu'on peut avoir de très gros volumes de données, on a des réseaux sociaux qui ont des milliards de relations à l'intérieur, donc d'une part parce qu'il y a cette taille, et d'autre part parce que le traitement en lui-même qu'on va vouloir faire dessus va être compliqué.

Un traitement qu'on veut faire assez classiquement dans un réseau social, c'est de trouver le plus court chemin qui existe entre deux personnes, pour savoir comment elles sont reliées. Et donc, chercher ce plus court chemin, c'est déjà un traitement qui peut prendre du temps parce qu'il faut regarder tous les chemins qui existent, parmi ceux-là, regarder ceux qui relient bien les deux nœuds qui nous intéressent, et puis après choisir le plus petit à l'intérieur, donc c'est déjà compliqué.

Mais en plus, dans les réseaux sociaux, on va s'intéresser par exemple à trouver les personnes les plus centrales dans le réseau, pour voir qui sont les gens les plus influents par exemple dans le réseau. Pour faire ça, il y a une métrique qu'on appelle la centralité d'intermédiarité, cette métrique, quand on la calcule, consiste à regarder le nombre de fois où une personne est sur un plus court chemin entre deux autres nœuds, donc en fait on regarde à quel point elle est intermédiaire, à quel point on passe par elle pour relier les autres. On voit qu'on va être obligé de calculer plein de plus courts chemins pour chacun des nœuds pour voir quels sont ceux qui sont le plus souvent sur des plus courts chemins.

On voit là qu'on augmente encore la complexité. Donc si on met ensemble le fait qu'on a des gros volumes de données et le fait que les calculs qu'on va faire dessus sont complexes, et bien on voit que très rapidement, on va se poser des questions d'optimisation du calcul, voire même d'approximation de calcul pour avoir des résultats qui ne sont pas tout à fait exacts, mais suffisamment bons et suffisamment tôt.

Plein d'autres questions se posent d'un point de vue technologique, par exemple, ces graphes sont amenés à changer dans le temps, les réseaux sociaux évoluent, on crée ou on enlève des nouvelles relations, donc comment est-ce que je gère ces changements ? Comment je les représente ? Comment je les analyse ? Autant de questions sur la temporalité du graphe, ou encore, ces graphes vont avoir des contenus qui vont transiter sur eux, on a parlé de médias sociaux, donc je vais échanger, non seulement du texte, mais des images, du son, etc., comment je traite ces contenus ? Comment je peux les analyser ? En regard du réseau social, on regarde la structure pour avoir des indicateurs, savoir qui est intéressé par quel sujet, par exemple dans le réseau social. Et puis toutes ces questions elles sont effectivement très liées aux technologies et aux sciences du numérique mais

c'est en fait c'est une problématique pluridisciplinaire puisqu'on a des enjeux juridiques, politiques et sociétaux qui se posent à travers ces réseaux sociaux. On pourrait dire que c'est juste ment parce que ces réseaux sont sociaux en fait, qu'ils posent des questions interdisciplinaires et qu'ils interrogent toutes nos disciplines.

2. Le Cloud

2.1. Qu'est-ce que le Cloud ?

Il faut revenir à ce que c'est que l'informatique. Qu'est-ce que c'est que l'informatique ? Ce sont des données dans une mémoire, sur un disque peut-être, et c'est aussi des calculs, et ces calculs se réalisent dans des processeurs. Alors, vous avez peut-être l'habitude de votre ordinateur personnel, cet ordinateur personnel c'est quoi ? C'est des mémoires, un disque, et puis c'est aussi un processeur, et tout ça calcule, et vous avez tout ça chez vous.

Le Cloud, c'est de vous dire : "plutôt que d'avoir ça chez moi, je vais transporter toute une partie de ce travail ailleurs, ailleurs dans les nuages". Ça veut dire quoi dans les nuages ? Ça veut dire dans un data center, probablement à l'autre bout du monde, je ne sais pas dans quel pays. Alors le mot Cloud vient d'une image, la représentation du réseau, d'Internet, c'est un nuage. Et donc à partir du moment où on va mettre ses calculs, ses données sur Internet, on va les mettre dans les nuages et donc on va parler de calculs dans les nuages. En fait, ce n'est pas du tout des nuages, c'est quelque chose de bien physique, c'est des ordinateurs, c'est des disques. C'est juste qu'ils ne sont pas situés chez vous, mais quelque part dans le monde, vous ne savez même pas où.

2.2. Les data centers

Pour bien comprendre le Cloud, il faut bien comprendre ce qui a permis sa réalisation. C'est d'abord et principalement des réseaux hyper rapides, des réseaux qui connectent votre entreprise ou votre maison avec ces data centers qui sont situés un peu partout, donc des réseaux rapides.

Deuxièmement, les coûts des machines et les coûts des disques, et les coûts du stockage qui sont devenus vraiment plus marginaux, qui ont diminué de façon considérable.

Alors à partir de ce moment-là, ça devient possible de construire, de concentrer dans des centres toute une quantité de processeurs, de stockage, etc., et de déporter ailleurs toute cette infrastructure. Donc le Cloud, c'est d'abord une infrastructure bien physique avec des réseaux bien physiques, des machines bien physiques, des disque s, des stockages considérables. La difficulté technique quand on parle du Cloud, c'est de faire marcher ces gigantesques entrepôts de données, ces gigantesques entrepôts d'ordinateurs. Prenons juste deux problèmes, les problèmes peut-être les plus critiques :

- Premier problème, tous ces ordinateurs, dégagent de la chaleur. Cela demande en permanence d'être climatisé, et donc il y a eu des progrès considérables en climatisation qui ont été réalisés dans ces data centers.
- Deuxième chose, c'est du matériel qui tombe en panne, c'est des logiciels qui tombent en panne, donc vous pouvez être certains que quand vous prenez un ordinateur, au bout d'un certain temps statistiquement, il va avoir une panne, matérielle ou logicielle.

Quand vous mettez un million d'ordinateurs au même endroit, un million de processeurs dans un même entrepôt, la probabilité d'avoir des pannes est considérable. Et il faut arriver à développer de la technique pour être capable de continuer à fonctionner et de ne pas être obligé de tout arrêter parce qu'il y a une panne. Donc votre application qui tourne, peut-être qu'elle tourne sur un

ordinateur qui va tomber en panne. Et bien vous n'allez même pas vous en rendre compte, parce que peut-être que vous allez attendre une ou deux secondes, mais elle va continuer à s'exécuter sur un autre ordinateur, ou sur un autre disque.

2.3. Sécurité

Quand vous mettez vos informations sur le Cloud, le premier avantage que vous avez, c'est une garantie de sûreté, ces informations ne disparaîtront pas parce qu'elles sont probablement répliquées dans plusieurs endroits, peut-être sur plusieurs data centers, en tout cas sur plusieurs machines. Même si une machine ou un disque tombe en panne, vous allez quand même récupérer vos données. Chez vous, tout peut se passer, votre ordinateur peut tomber en panne, votre maison peut brûler. Là, il y a une espèce de garantie de protection de vos données, protection aussi contre les intrusions, ce n'est pas garanti à 100 %, mais on va imaginer qu'ils savent quand même mieux se protéger contre les attaques des pirates que vous.

La deuxième chose pour une entreprise, c'est de pouvoir faire des économies de gestion. Pour une entreprise c'est compliqué, il faut acheter des ordinateurs, il faut avoir des ingénieurs système qui gèrent tout ça et ce n'est pas leur business. Si vous êtes une entreprise dans les travaux publics, ce n'est pas votre métier de faire tourner des ordinateurs. En les déportant sur le Cloud, vous externalisez d'une certaine façon votre informatique, et vous autorisez d'autres personnes, des ingénieurs système qui ne sont même pas de chez vous, de les gérer.

Les désavantages, c'est que d'une certaine façon, vous perdez un petit peu le contrôle de ce que vous êtes en train de faire et il y a quand même quelques points négatifs, le premier étant d'abord les problèmes écologiques qu'il génère, puisque quand vous mettez vos données extrêmement loin de chez vous, vous allez avoir des gaspillages d'électricité pour aller les chercher, pour les ramener chez vous.

Il y a aussi une philosophie un petit peu sous-jacente du Cloud d'hyper-centralisation. On centralise les calculs, on centralise les données. À l'arrivée, ce que vous avez, c'est que vous avez quelques entreprises qui vont par exemple posséder toutes les données personnelles de tous les individus dans le monde dans des énormes data centers.

C'est un petit peu à l'opposé d'une philosophie qui est plutôt au départ par exemple de l'Internet, qui était une philosophie d'acentralisation, de localisation au maximum des choses. L'acentralisation a énormément d'avantages, elle vous rend plus autonome, elle fait des économies d'électricité aussi. Et donc d'une certaine façon, la concentration de tous les calculs dans ces data centers n'est pas que positive.

On pourrait imaginer des Clouds beaucoup plus décentralisés, beaucoup plus individualisés, c'est-à-dire toutes nos puissances de calcul. Les ordinateurs que vous avez chez vous, par exemple votre boîte télé, c'est un ordinateur et toutes ces choses-là, et c'est ces ordinateurs-là qui pourraient se mettre ensemble pour faire un Cloud, un calcul dans les nuages. Cela a beaucoup d'avantages. Prenons juste la vidéo. Plutôt que d'aller chercher un film, la vidéo que vous voulez voir ce soir à l'autre bout du monde, et du coup avoir des coûts considérables en énergie, vous pourriez peut-être trouver cette vidéo sur votre Cloud régional ou local, chez un de vos voisins qui ne sait même peut-être pas qu'il va vous servir ce film, mais d'une certaine façon, vous allez faire des économies considérables en énergie et peut-être récupérer cet esprit originel du Web.

3. Du bitcoin à la blockchain

3.1. L'argent dématérialisé

Est-ce que l'argent peut exister sous la forme numérique ? C'est une question à laquelle on peut répondre de plusieurs façons. Tout le monde sait que ce qui se passe quand on utilise une carte bancaire, quand on fait un virement par Internet, c'est de l'argent numérique au bout du compte qui circule. Mais il existe depuis 2009, une autre forme d'argent numérique qui est plus intéressante et qui, sur le plan du développement de l'informatique et des idées, va sans doute avoir un grand rôle, c'est ce qu'on appelle les monnaies cryptographiques, dont le bitcoin est le premier exemple.

Le bitcoin, c'est une monnaie qui a été créée à partir de rien, en utilisant ce qu'on appelle un réseau pair-à-pair, donc il a été créé le 3 janvier 2009 pour être précis à partir d'idées d'un certain Satoshi Nakamoto. Il a décrit le protocole et s'est arrangé pour écrire les programmes qui le font fonctionner et le mettre en marche en 2009, et ce protocole aujourd'hui a généré une monnaie qui s'appelle le bitcoin, dont la capitalisation totale aujourd'hui vaut 10 milliards d'euros. Donc le bitcoin est une monnaie réelle, qui n'existe que sous forme numérique, il n'y a pas de billets, il n'y a pas de pièces bitcoin, c'est quelque chose qui circule uniquement sur les réseaux, et dont le fonctionnement est basé sur ce qu'on appelle un fichier partagé (on dit aussi un registre partagé) et qu'on appelle la Blockchain.

3.2. La Blockchain

Alors, comment fonctionne le bitcoin ? Il faut comprendre comment il fonctionne pour comprendre le concept de blockchain. L'idée elle est assez simple : c'est de dire "si tout le monde est d'accord pour savoir qui possède des bitcoins, ces bitcoins n'ont pas besoin d'être réels, ça n'a pas besoin d'être matérialisé par des pièces métalliques ou en or ou je ne sais quoi", si tout le monde est d'accord pour dire "le compte numéro tant détient 10 bitcoins, le compte numéro tant en détient 20, etc.", à ce moment-là, ça peut fonctionner. Cela semble un petit peu bizarre et au début on a du mal à y croire, mais c'est l'idée du bitcoin.

Il y a un fichier qui s'appelle la blockchain, qui indique précisément ce que détient chaque compte, et tout le monde est d'accord parce que ce fichier indique, qui, quel compte détient tant, etc., c'est un fichier qui est reproduit, dans le cas du bitcoin, en 5000 exemplaires à peu près sur 5000 ordinateurs qui gèrent ce fichier. Ils ont tous exactement le même fichier, indiquant quel compte détient combien, et ça crée une sorte de confiance entre les utilisateurs, puisque personne ne peut tricher, personne ne peut dire "moi je modifie ce fichier et puis j'ai le double sur mon compte parce que ça m'arrange d'avoir le double", personne ne peut créer de bitcoins nouveaux sans que ce soit prévu par le fonctionnement général du bitcoin, et cette confiance qui est créée par ce partage de l'information. C'est l'idée de la blockchain, et c'est cette idée-là qui est généralisée et qui peut être utilisée à bien d'autres fonctions.

3.3. La cryptographie

Les blockchains et en particulier celles du bitcoin, se fondent sur les primitives cryptographiques, et des primitives de ce qu'on appelle la cryptographie mathématique, et ce sont elles qui créent la solidité des informations qui sont gérées par la blockchain, et la fiabilité e t l'indestructibilité de ces informations. Le bitcoin, et tout ce qui est blockchain qui a été développé depuis, est basé sur des mathématiques. C'est la maîtrise qu'on a aujourd'hui des protocoles de cryptographie, en particulier des systèmes de signatures numériques, des systèmes de hachage de fichiers, qui permet au

protocole de fonctionner sans que personne ne puisse tricher, parce qu'il ne faut pas que quelqu'un puisse manipuler le protocole pour s'attribuer de l'argent ou autre chose quand il s'agit d'une autre blockchain. Donc les mathématiques, la cryptographie mathématique, grâce à la maturité de cette science informatique, de cette science numérique, c'est la base du bitcoin et de la blockchain.

Dans le protocole, il y a des signatures numériques, des signatures cryptographiques, et c'est absolument essentiel. L'idée est la suivante : quand quelqu'un détient des bitcoins, il va détenir deux informations concernant le compte sur lequel ces bitcoins sont déposés :

- une information qui est le numéro de son compte, comme un numéro de compte bancaire, on va appeler ça la clé publique.
- une information qui est la clé secrète qui permet de signer sa transaction de façon unique, car elle seule dispose de cette clé privée.

Mais tous ceux qui connaissent son numéro de compte vont pouvoir vérifier que c'est bien lui qui a signé, donc ces systèmes à double clé permettent cette chose où tout le monde peut vérifier qu'une signature est bonne, et c'est évidemment essentiel dans le protocole bitcoin, puisqu'il faut bien que l'argent puisse circuler. Il ne s'agit pas simplement que certains comptes détiennent de l'argent, il faut aussi qu'on puisse les faire passer d'un compte à l'autre, et donc il faut qu'il y ait une sorte d'action, donc ce qu'on appelle les transactions, et ces transactions vont être signées à chaque fois par les détenteurs du compte, et personne ne pourra tricher, personne ne pourra signer une transaction qui dit "du compte A qui est le mien, je vais verser l'argent vers le compte B", il n'y a que, moi détenteur du compte A, qui pourrait signer les transactions du compte A vers un autre compte.

3.4. Les applications de la blockchain

La blockchain sert à bien d'autres applications, et c'est ça qui est très étonnant dans l'histoire du bitcoin, c'est que dans un premier temps, on a pensé que ça ne pouvait servir qu'à créer des monnaies cryptographiques tellement l'idée a semblé intéressante, voire géniale. Mais on s'est aperçu depuis 3, 4 ans, qu'on pouvait faire bien d'autres choses.

L'idée est très simple : ce qui sert à stocker les transactions du bitcoin, c'est un fichier qui est impossible de truquer, on ne peut pas le modifier, il est répliqué 5000 fois, ce qui fait qu'il est in destructible, totalement indestructible. Si on fait sauter la moitié de la terre, il restera encore des copies de la blockchain du bitcoin. Cette notion de fichier qui soit partagé, indestructible et sur lequel personne ne puisse écrire sans qu'un certain contrôle ne soit effectué par un ensemble d'autres acteurs, qui sont les autres détenteurs de la blockchain, ça permet de faire beaucoup de choses...

On a envisagé de faire un cadastre à base de blockchains, c'est-à-dire que les informations de propriété pour des terrains découpés, etc., seraient inscrites sur une blockchain. Seules évidemment certaines autorités auraient le droit d'aller inscrire des informations sur cette blockchain, quand il y aurait une vente, on écrirait une information, non pas en effaçant la précédente, mais en venant compléter l'information précédente, que tel terrain a été vendu, et le propriétaire a changé, et cette information donc, à partir du moment où elle serait multipliée, et rendue indestructible par l'utilisation de primitives cryptographiques. On pourrait savoir uniquement en se branchant sur Internet, qui possède quoi et d'une manière beaucoup plus fiable que si c'était géré par un fichier centralisé. Cela permet d'établir une sorte de confiance, y compris dans les pays où justement, à cause de la corruption et toutes sortes de choses, le cadastre n'existe pas ou existe d'une manière très peu fiable.

Tous les jours il y a des gens qui proposent de nouvelles applications des blockchains, donc de cette information partagée et garantie. Et on s'aperçoit qu'on peut faire des tas de choses et une sorte de véritable révolution numérique est en train de se produire. C'est pour ça que les banques, les organismes gouvernementaux, tout le monde s'intéresse à la blockchain et essaye de comprendre comment elle marche et quelle blockchain nouvelle on pourrait imaginer pour faire telle chose, aujourd'hui considérée comme impossible à faire.

3.5. L'impact écologique

Le Bitcoin entraîne une dépense colossale d'énergie d'électricité. La quantité d'électricité qui est dépensée pour faire fonctionner le protocole du Bitcoin est absolument énorme. Mais il faut bien comprendre, c'est absolument essentiel pour l'avenir du développement des blockchains, que cette particularité du Bitcoin n'est absolument pas générale. Les blockchains n'ont absolument pas, d'une manière générale, cette obligation d'avoir un système, ce qu'on appelle le système de minage du Bitcoin, qui entraîne une dépense importante d'électricité. Mais c'est une erreur de croire que le développement des blockchains va être freiné par ça.

Glossaire

- Internet : un ensemble de standards et de technologies qui permettent de relier les ordinateurs et les réseaux entre eux.
- Web : (World Wide Web, parfois aussi appelé la Toile) une des applications d'Internet qui permet de lier et consulter à distance des documents (ex. un journal), des interfaces d'applications (ex. un service de réservation), des données (ex. les températures d'une ville), etc.
- Lien : élément qui établit des liaisons. Lorsqu'on parle de graphes, les liens sont ce qui relie les différents sommets.
- Graphe (nœuds, arcs) : un type de structure de données composé de sommets (aussi appelés points, nœuds) reliés par des liens (aussi appelés arrêtes ou arcs).
- Graphe orienté : si les liens d'un graphe sont orientés (l'orientation est matérialisée par des flèches), cela signifie que la relation va dans un seul sens, est asymétrique. Le graphe est donc orienté.
- Graphe étiqueté : il s'agit d'un graphe dont les liens sont étiquetés par un chiffre, un symbole, une lettre, etc.
- Matrice d'adjacence : outil mathématique qui permet de modéliser sous forme d'un tableau (ou matrice) les liens d'un graphe et donc, dans notre cas, les relations d'un réseau.
- Centralité d'intermédiarité : une mesure, parmi d'autres, de la centralité d'un sommet d'un graphe. Elle capture le nombre de fois où un nœud agit, dans un graphe, comme un point de passage le long du plus court chemin entre deux autres nœuds.
- Web social : évolution du Web caractérisée par l'interaction entre les utilisateurs et la production de contenus par ces derniers.
- Réseau social : côté Web, il s'agit d'une application qui utilise les sciences et technologies de l'information et de la communication pour mettre en relation des personnes. Hors monde numérique, un réseau social est un groupement de personnes qui a un sens.

- Data center ou centre de données est un site physique sur lequel se trouvent regroupés des équipements constituants de systèmes d'information : ordinateurs, baies de stockage, équipements réseaux et de télécommunications, etc.
- Cloud : désigne le fait, au lieu de stocker ses données et d'effectuer ses calculs sur son propre ordinateur, de confier les deux à un centre de données se trouvant sur Internet.
- Sûreté : la sûreté de fonctionnement d'un système informatique est son aptitude à remplir à remplir ses fonctions en dépit de pannes matérielles ou logicielles.
- Externaliser : désigne le fait qu'une entreprise fasse appel à un service extérieur pour certains pans de son fonctionnement plutôt que d'embaucher en interne un employé ayant la compétence requise (par exemple pour le ménage, la comptabilité ou l'accueil téléphonique). Avec le numérique, il devient plus facile et plus rentable d'externaliser beaucoup de services.
- Ingénieur système : désigne un métier de l'informatique qui prend en charge tout ce qui est l'exploitation des infrastructures informatiques matérielles et logicielles.
- Bitcoin : une monnaie planétaire, cryptographique, basée sur un système transaction et de contrôle, la block-chain.
- Cryptographie (monnaie) : une monnaie électronique basée sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même.
- Blockchain : c'est une technologie de stockage et de transmission d'informations avec un protocole de gestion de données numériques, qui est :
  - Transparente : chacun peut consulter l'ensemble des échanges, présents et passés.
  - Sans organe de contrôle : elle est fondée sur des échanges de pair-à-pair -> c'est ce qui créé une rupture par rapport aux autres technologies.
  - Infalsifiable et sécurisée : car différents exemplaires existent simultanément à de nombreux endroits ce qui empêche d'en falsifier un ou quelques-uns.