Cryptos kézako

Bitcoin, Blockchain, Smart Contract et plus encore

Tous ces mots sont très à la mode, pleins d'articles en parlent sur internet et même à la télé.

Tout d'abord un peu de vocabulaire, le Bitcoin est une crypto monnaie, c'est la première a avoir été crée, elle a démarré le 2 Janvier 2009 (en fait c'était le 3). Depuis cette date des milliers d'autres crypto-monnaies ont été crées. Le Bitcoin est la plus importante, la deuxième en terme d'importance est l'Ethereum. Si vous voulez en voir la liste vous pouvez aller sur des sites comme coinmarketcap.com, binance.com ou pleins d'autres. Vous pouvez même créer votre propre crypto-monnaie, c'est un peu technique, mais il y a des tutos sur Youtube.

Les crypto monnaies utilisent la technologie de la blockchain, il ne faut pas confondre les deux, la blockchain peut servir à autre chose qu'à gérer de la crypto-monnaie.

Mais à quel besoin répond cette fameuse blockchain ?

Pour ça il faut bien comprendre comment fonctionnent nos échanges de biens dans notre vie actuelle. Pour illustrer ça je vais prendre un cas concret. Bien entendu en informatique nous avons l'habitude d'anonymiser les informations, toutes ressemblances avec des personnes existantes serait purement fortuite, je vais donc utiliser des codes complètement incompréhensibles pour bien anonymiser les données.

Alors voici l'histoire : D117 (reconnaissez, c'est totalement indécodable) est un grand fan de l'actrice Lola T qui a des talents de « grande importance ». Il faut préciser que Lola est une lointaine descendante de l'inventeur des séries de Taylor, j'ai nommé « Brook Taylor ». Je rappelle que les séries trouvées par ce Monsieur ne passent pas sur Netflix mais sont massivement utilisées dans notre informatique actuelle. D117 possède tous les DVD de cette actrice sus-nommée, mais dans sa frénésie d'achat il se rend compte qu'il a acheté un DVD en double, il s'agit de l'épisode « Lola exp-ix » (seuls les initiés pourront comprendre). Comme c'est pas très utile de le garder en double, il décide de le mettre en vente sur leboncoin.fr.

Je vous laisse googeler Lola machin pour que vous puissiez vous faire une idée des talents de « grande importance ».

T48 (encore un code), toujours à l'affût de documentaires sur la physique quantique et les mathématiques, est persuadé d'avoir trouvé là, la biographie du grand mathématicien Brook Taylor, il décide de l'acheter. Il fait un virement avec son compte paypal. L'argent est bloqué pendant quelques jours par Leboncoin, D117 envoie l'objet, à la réception l'argent est crédité sur le compte de D117.

Dans cette transaction il y a au moins quatre intervenants tiers qui interviennent et qui se sucrent d'une façon ou d'une autre : il y a Paypal qui demande à la banque de T48 si il a les fonds, il y a la banque de T48 qui débloque les fonds, il y a LeBonCoin, il y a la banque de D117. On appelle cela des tiers de « confiance ». L'idée de la Blockchain c'est de pouvoir se passer de ces tiers, donc de pouvoir s'échanger des choses de valeur de D117 à T48 sans passer par tout ces bouffe'ms.

Les anciens gravaient les transactions « dans le marbre », la blockchain reprend un peu cette idée mais en gravant l'information dans du marbre numérique. Mais même le marbre n'est pas complètement sûr, un faussaire pourrait graver une autre plaque. Mais imaginez qu'on grave mille plaques et qu'on les envoi au quatre coins du monde, ce sera déjà plus compliqué pour le faussaire. La blockchain reprend un peu cette idée en dupliquant l'information de nombreuses fois.

Dans la version « traditionnelle » des systèmes d'information, les données sont généralement stockées dans des bases de données centralisées, même si cette information est souvent répliquée pour des raisons de sécurité. Votre compte en banque est stocké dans une base de données centrale, votre dossier médical est dans une base de données (gérée par la caisse des dépôts et consignation), vos données Facebook sont dans une base centrale, même si elles sont dupliquées dans plusieurs datacenter dans le monde, …

Tout ces organismes qui stockent vos données sont des tiers de « confiance ». Il en est de même quand vous achetez un bien immobilier, le notaire enregistre la transaction sur papier et sans doute dans une base centrale (pas sûr). Il en est de même pour un contrat d'assurance. Tout ça ce sont des transactions entre A et B qui sont enregistrées et validées par un organisme intermédiaire.

Des histoires de piratage de bases de données centralisées, il y en a eu dans l'histoire de l'informatique, mais globalement les techniques de sécurité ont quand même sacrément progressé au cours des trente dernières années. Dans les années 90 certains mots de passe circulaient en clair sur le réseau et on se disait que personne ne serait assez dingue pour aller analyser la trame réseau pour retrouver le mot de passe, ben si !!

Si aujourd'hui une base de données centralisée est hackée, c'est principalement à cause d'un facteur humain, c'est que quelqu'un a fait une bourde. Il faudrait trouver une solution pour se protéger contre ça, et la blockchain y répond.

Dès les années 90 des chercheurs ont commencé à réfléchir sur comment stocker de l'information de façon immuable dans le marbre numérique, la réflexion prendra du temps.

Internet est né dans les années 90, rapidement on a eu droit aux sites de piratage où on pouvait télécharger des musiques, des films, ces sites ont rapidement été fermé. Mais dans la foulée sont apparus les sites peer-to-peer, les films à pirater ne sont plus stockés dans une base de données centrale, ils sont stockés sur le disque dur de particuliers, en gros chacun partage les films qu'il a sur son disque dur à lui. C'est le protocole bit-Torrent, tout le monde connaît j'en suis sûr. Avec l'apparition des plates-formes de streaming type Netflix, Spotify, Salto, … qui proposent un choix quasi illimité de séries et de films, l'intérêt est moindre. Qui télécharge encore avec bit-torrent ? Il faut quand même savoir qu'avec ça, il y a des inconnus qui viennent lire des fichiers sur votre disque dur !! c'est flippant, mais en contre partie vous pouvez aller piquer sur le disque des autres !! que ne ferait-on pas pour avoir un film de Lola T !!

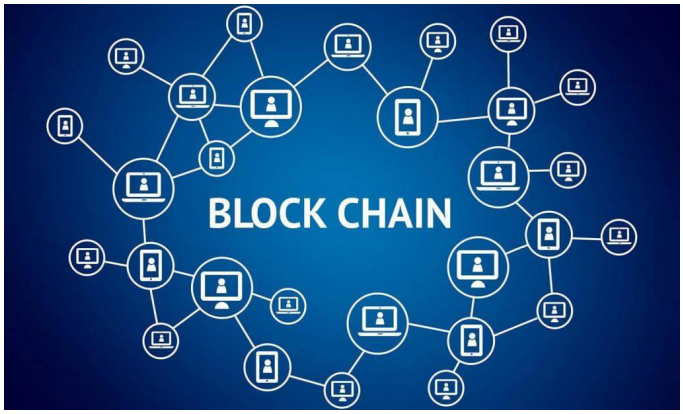
En 1995 (donc on est à l'époque du début du bit-torrent), des chercheurs d'une université Américaine ont sorti un papier de spécification qui donnera naissance à la Blockchain. L'idée c'était d'enregistrer des transactions pendant quelques minutes, de les dupliquer sur de nombreux nœuds du réseau, de les vérifier au niveau de chaque nœud, de les regrouper dans un block, et de les sceller toutes les quelques minutes par une clé infalsifiable. « Infalsifiable » en informatique, ça fait rigoler, combien de fois on a entendu parler de piratage, … il se trouve que celui là va quand même être sacrément complexe à pirater.

Le papier est resté dans un tiroir jusqu'en 2008. Cet année là, surprise, c'est la crise des sub-prime, personne ne comprend d'où ça vient , il s'en suit une crise financière mondiale, quelques tiers de « confiance » ont foutu la merde avec je ne sais quoi.

Un certain Satoshi Nakamoto s'est alors mis en tête de créer une monnaie indépendante de tout organisme central, une monnaie qui ne dépendrait ni d'un pays ni d'une banque centrale, ça a été la naissance du bitcoin. Personne ne sait qui est ce Satoshi Nakamoto, c'est un pseudo utilisé par la ou les personnes ayant développé le Bitcoin.

Pour créer le Bitcoin, il se sont appuyé sur les travaux publiés en 1995, et ont codé pour la première fois un algorithme de type blockchain.

Il faut voir la blockchain comme un livre de compte dupliqué sur de nombreuses machines du réseau mondial. Pour le bitcoin, ce nombre varie entre 5000 et 10000, on parle de nœuds du réseau. Dans le jargon des crypto-monnaies, ces nœuds sont appelés des « mineurs ». Par abus de langage, on appelle aussi « mineurs » les propriétaires de ces machines. Sachez que le propriétaire ne fait rien à part acheter la machine et payer l'électricité pour la faire tourner. Ca coûte cher, mais potentiellement, ça peut rapporter beaucoup.



Chaque nœud reçoit les transactions effectuées sur le réseau. Exemple T48 donne deux bitcoins à D117 pour le DVD de Lola T. Les noms des utilisateurs n'apparaissent pas en clair, chaque utilisateur possède une « adresse bitcoin » représentée par 64 chiffres hexadécimaux. Par contre le montant est en clair. La blockchain est visible de tout le monde, vous pouvez même rapatrier toute la blockchain du bitcoin sur votre PC. Vous pourriez même devenir un nœud du réseau bitcoin et donc devenir un « mineur ». Le code source de l'algorithme du bitcoin est opensource, tout le monde y a accès. Pour info, être mineur de bitcoin en France n'est pas rentable à cause du prix trop élevé de l'électricité, par contre vous pourriez installer votre serveur en Island ou au Kazakstan.

Quand un nœud reçoit une transaction, il fait les vérifications qui vont bien, il vérifie que T48 possède bien deux bitcoins, si c'est bon, il inscrit la transaction dans le livre de compte sur une page « provisoire » à condition que le pourboire proposé par T48 soit suffisant. Et oui, il faut proposer un pourboire pour que ta transaction passe (en se moment, ça peut monter à 10$). Toutes les dix minutes, l'algo ordonne à tous les nœuds de se synchroniser sur un bloc tiré au hasard, il leur donne ensuite l'ordre de « sceller » le bloc et c'est là que les choses se compliquent. Dans les blockchain actuelles, il y a deux façons principales (et il y a des variantes) de sceller un bloc : the proof of work (preuve de travail) et the proof of stake (preuve d'enjeu). Le bitcoin utilise la preuve de travail, mais je vais vous expliquer les deux.

Avant cela je vais expliquer deux notions importantes : le **Hash** d'un fichier informatique et les sécurités de « type » **RSA** (parce que bitcoin utilise une variante). Pop's a déjà fait un article sur le sujet il y a deux ans. Ces deux notions sont fondamentales dans l'informatique d'aujourd'hui, c'est pas des notions complexes, tout ingénieur devrait connaître ça, même s'il ne travaille pas dans le domaine.

C'est quoi le Hash ?

Non ce n'est pas ce que certains fumaient en cachette au Tabagn's. C'est une cuisine mathématique qui permet de calculer une empreinte d'un fichier informatique, c'est une sorte d'empreinte digitale.

Une des craintes en informatique est qu'un pirate (le méchant) modifie un fichier (ou une donnée) quand elle circule sur le réseau. Avec ce système, on prend l'empreinte avant et après, si elle a changé, on sait que l'information a été modifiée et qu'elle n'est plus valide, on demande donc une retransmission.

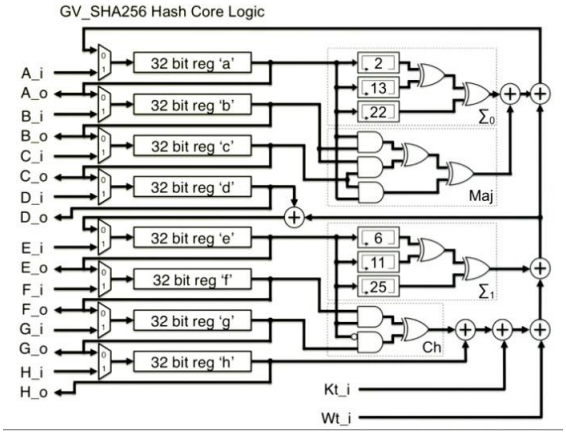
Le bitcoin utilise la fonction SHA256 (pour calculer le hash256 d'un bloc). Cette fonction est une cuisine mathématique, son code est publique, elle a été crée par de vrais mathématiciens comme vous et moi, elle est implémentée dans tous les langages informatiques. Vous mettez n'importe quel texte en entré, elle sort une clé de 64 chiffres hexadécimaux. Pour le même texte, c'est toujours la même clé. Vous changez une virgule dans votre texte d'entrée, la clé change complètement. On ne peut pas retrouver le texte d'origine avec la clé, c'est impossible (pour le moment... mais tous les méchants de la terre y travaillent...).

Il existe plein de fonctions de Hash, la blockchain du Bitcoin utilise le sha256.

Vous pouvez la tester en ligne, tapez 'sha256 online' dans google et prenez la première proposition. Essayez avec votre buque, changez une lettre, vous verrez le résultat.

Au début d'internet, certains sites stockaient les mots de passe en clair, une aubaine pour les pirates. Aujourd'hui plus aucun site ne stocke les mots de passe, il stocke le Hash256 de votre mot de passe. On ne peut rien faire d'un hash à part le comparer au hash du mot de passe que vous êtes entrain de taper quand vous vous connectez à un site. Cette fonction hash256 (ou aussi SHA256, parce que le geek est joueur... il fait du verlant) est utilisée partout.

On peut même réaliser cette fonction SHA256 sous forme électronique. Voici son schéma.



Ca a l'air compliqué comme ça, mais en fait ce ne sont que des portes logiques ET, OU, NON, … on sait faire ça depuis les années 50, on pourrait même la réaliser en pneumatique avec le Grafcet qu'on a appris en Terminale E. Cette implémentation sous forme hardware a un intérêt dans le cas de la blockchain du bitcoin, parce qu'elle est très rapide.

La sécurité RSA c'est quoi ?

RSA c'est les initiales des trois mathématiciens qui ont élaboré le système dans les années 70 (Ronald Rivest, Adi Shamir et Leonard Adleman). Aujourd'hui c'est le système le plus utilisé

pour sécuriser les échanges d'informations sur internet.

Au début d'internet, tout circulait en clair sur le réseau, je me souviens d'une discussion chez Dassault, où quelqu'un a dit à un client « qui serait assez fou pour sniffer les trames réseau pour trouver le mot de passe », les pirates avaient la partie facile à l'époque. Ce quelqu'un c'était moi. A l'époque il fallait des outils spéciaux pour sniffer le réseau, aujourd'hui n'importe quel PC sous Linux peut le faire. Petit à petit la sécurité s'est étoffée et aujourd'hui on en est à RSA et ses variantes.

On dit que RSA est un système de cryptage asymétrique. C'est pas si compliqué que ça, je vais essayer d'expliquer ça comme si je parlais à ma grand-mère (ne m'en voulez pas)

Dans les échanges informatiques, on a deux gros problèmes. Premièrement, il faut que le message échangé soit imbitable par quelqu'un qui écoute la ligne (le méchant,...). Deuxièmement, quand vous recevez un message, vous devez pouvoir faire confiance à celui qui vous l'a envoyé, vous devez être sûr de son identité. Le système RSA permet justement de répondre à ces deux problèmes majeurs. (vous avez remarqué, je n'utilise pas le terme 'algorithme RSA' parce que ce n'est pas un algorithme, c'est une cuisine mathématique basée des nombres premiers et sur le reste de la division entière qu'on appelle le modulo. Ex : 7 modulo 3 = 1, je divise 7 par 3, il reste 1).

Alors comment ça marche ?

Chaque acteur connecté au réseau possède ce qu'on appelle une clé privée et une clé publique, j'explique un peu plus loin ce que c'est. Attention, là ça se complique un tout petit peu, j'ai besoin de votre attention. La clé publique de quelqu'un est publique, vous pouvez la demander à votre interlocuteur (genre « fait péter ta clé publique »), elle peut circuler en clair, un pirate (le méchant) ne peut rien en faire.

Si Toto veut envoyer un message secret « Sal's Manara » à Manara. Alors voici la séquence :

-Toto envoi à Manara « fait péter ta clé publique », Manara lui envoi

-Toto crypte le message avec la clé publique de Manara, ça donne un texte imbitable

-Toto « signe » le message crypté avec sa clé privée

-Toto envoi à Manara, le message crypté-signé et sa clé publique (celle de Toto)

-Manara vérifie la signature du document avec la clé publique de Toto, et maintenant il est sûr que le message vient de Toto (et pas du méchant)

-Manara décrypte le message avec **sa** clé privée, il peut alors lire le message de Toto, et le méchant s'est fait niquer.

Alors c'est quoi cette histoire de clé ?

On est dans les années 70 ..., Ronald, Shamir et Adleman sont bourrés au pian's, ils tournent au Mazouth et à la Wodka-or's, ils délirent sur la fonction Zeta de Riemann. Je rappelle que cette fonction essaye de trouver le graal des nombres premiers (*), ça fait déjà 60 ans qu'on peut se faire un Million de Dollars avec ça et personne n'a encore trouvé (et aujourd'hui encore, c'est toujours le cas). Et là Shamir, qui était un peu plus bourré que les autres a dit « et si on faisait un système de cryptage avec les nombres premiers », et c'est ça le début de RSA.

(*) je vous rappelle qu'il y a un excellent article sur ce sujet dans le Chibrem's 2021.

Alors voici un extrait approximatif de la recette de cuisine du système RSA :

Vous prenez deux très grands nombres premiers (un ordinateur peut faire ça très facilement pour vous, c'est plus difficile à la main), disons A et B, vous les passez dans une cuisine mathématique composée de multiplications et de modulos, vous obtenez une clé publique et une clé privée.

Je ne vais pas rentrer dans les détails de la recette, mais grosso modo votre clé privée c'est le couple (A et B) et votre clé publique c'est (A multiplié par B), le tout avec un peu d'épice et de wodka-or's.

Vous ne devez jamais donner votre clé privée à qui que ce soit, elle est privée. Par contre votre clé publique, vous pouvez la publier en clair, le méchant ne pourra rien en faire.

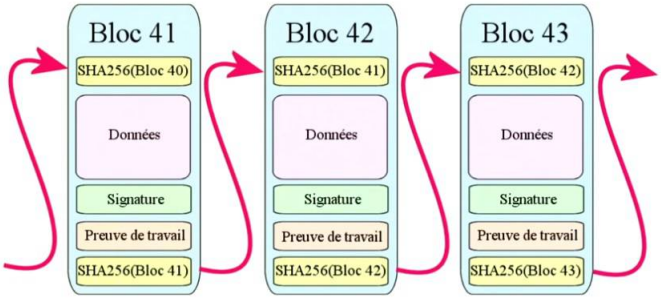
Les blockchain actuelles et celle du bitcoin utilisent massivement ces deux techniques que ce soit le Hash256 ou le système RSA et variantes.

Bon, maintenant revenons à la blockchain du bitcoin

Nous en étions au moment où chaque nœud du réseau doit sceller le block.

Concrètement, il y a quoi comme infos dans un block ?

La première ligne, c'est les SHA256 du block précédent, les block sont donc chaînés, d'où le nom de blockchain.



Vous avez ensuite les transactions enregistrées au cours des 10 dernières minutes (Données sur les schéma), puis ce qu'on appelle le 'Nonce' (preuve de travail sur le schéma) et enfin le SHA256 du block. Pour sceller un block, chaque nœud doit essayer de trouver un Nonce pour que le Sha256 du bloc soit conforme à une certaine condition. Cette condition a été fixée dans l'algorithme en 2008 par Satochi et elle dépend de la puissance de calcul consacrée au réseau bitcoin, donc plus il y a de puissance de calcul connectée, plus la condition est difficile.

La règle fixée par Satochi est assez simple (et absurde), pour valider un block, vous devez trouver un Nonce pour que le Sha256 du bloc commence par un certain nombre de zéros (c'est purement arbitraire, mais c'est lui qui a fixé les règles en 2008 et il faut les accepter). La seule façon de faire est d'essayer des valeurs au hasard, l'ordinateur essaye le plus de Nonce possible pour essayer de trouver une solution commençant avec assez de zéros, c'est du pif !! En fait c'est une espèce du Sudoku géant.

Aujourd'hui en 2022, avec la puissance de calcul mondiale consacrée au bitcoin, pour valider un block, il faut trouver un Sha256 qui commence par 19 zéros (en 2017 c'était 5). Les machines utilisées aujourd'hui sont ultra spécialisées dans le calcul du Sha256, les processeurs utilisés sur les cartes graphiques sont particulièrement performants dans ce domaine, d'où la pénurie actuelle à l'échelle mondiale des composants pour fabriquer des cartes graphiques. Nvidia qui est un de leader des cartes graphiques a essayé d'interdire à ses acheteurs d'utiliser les cartes pour miner du bitcoin, ils se sont fait hacker et ont du renoncer. Cette règle est complètement absurde, mais c'est comme ça que ça marche sous le capot du bitcoin.

Avec la puissance de calcul passée et actuelle, une solution est statistiquement trouvée aux environs de toutes les 10 minutes et c'est ce que voulait Satochi, un bloc est donc validé toutes les dix minutes environ.

Un système de validation comme celui là cause une consommation électrique phénoménale, c'est sans doute la pire invention depuis le moteur à explosion, et là en plus ça ne sert même pas à se déplacer. Certains Youtubers « expert »

pense que c'est la difficulté du problème à résoudre qui donne sa valeur au Bitcoin, il n'y a absolument aucun rapport. La valeur du bitcoin ou de toute autre crypto est juste liée à l'offre et à la demande. Pour justifier la consommation d'énergie, le principal argument utilisé par les Youtubers « expert » est que la blockchain utilise de l'électricité, et que c'est la seule énergie que nous savons produire de façon verte, et que la blockchain utilise l'excédent produit par les barrages et l'éolien, mais bien sûr !!

Bien entendu, les nœuds du réseau ne travaillent pas pour des prunes, il y a un récompense aléatoire à la clé. Si vous avez la chance de valider un block (en trouvant le bon Nonce pour qu'il réponde aux critères) vous empochez toutes les commissions du block et 6,25 Bitcoins, ce qui au cours actuel (30000$) est pas mal, mais il ne faut pas oublier l'achat des machines et l'électricité.

Au début du Bitcoin, si vous aviez la chance de valider un bloc (à l'époque vous pouviez le faire avec un simple PC en veille) vous touchiez 50 Bitcoins. Tous les 210000 blocs, cette somme est divisée par 2 (encore une règle arbitraire imposée par Satochi en 2008), donc environ tous les 4 ans, on appelle cela le « halving day » et certains youtubers « expert » pense que ce jour là est « sacré » et provoque l'envolée du Bitcoin, trop drôle, mais le pire c'est que ça marche (parfois).

Sachez que ce système de récompense en bitcoin est le seul mécanisme de création de nouveaux bitcoins, c'est d'ailleurs pour ça que les nœuds du réseau sont appelés des mineurs.

Aujourd'hui, en 2022, le système crée 6,25 bitcoins toutes les dix minutes environ, avec le système du « halving day », tous les bitcoins auront été minés en 2140 environ. A ce moment là il y aura environ 21 millions de bitcoins en circulation (peut être que Loutch ou Geram's se cachent derrière le pseudo Satochi Natamako, allez savoir... je crois me souvenir qu'un changement de bucque, c'est un thermo-couple...)

Pour rester dans le coup, et avoir une chance de remporter la mise, un mineur de bitcoins doit changer son matos tous les deux ou trois ans, cette inflation est absurde.

Si vous voulez voir en concret à quoi ressemble la blockchain du bitcoin, vous pouvez aller sur ce site, vous pourrez consulter les blocs : https://www.blockchain.com/explorer?view=btc

Un système comme celui là est protégé contre toute tentative de piratage, ça ne fait aucun doute pour le moment (*). Si un pirate arrive à modifier les données d'une transaction, ça change le sha256 du bloc, il faut donc qu'il recalcule le 'nonce', mais ça change aussi le sha256 du bloc suivant, donc il faut aussi recalculer le 'nonce', et il faut faire ça simultanément sur au moins la moitié des 5 à 10000 machines du réseau : impossible !! et je rappelle que pour trouver un nonce, les 5 à 10000 machines (sur-vitaminées) mettent en moyenne 10 minutes.

L'information gravée dans la blockchain l'est à jamais.

(*) avec l'arrivée éventuelle d'un ordinateur « quantique » c'est moins sûr, mais rassurez vous, l'ordinateur quantique c'est encore de la science fiction, malgré les annonces de Google et des Chinois.

C'est quoi l'autre protocole de validation des block ? Le Proof of stake (preuve d'enjeu)

Cette énorme consommation électrique du bitcoin a provoqué de nombreux débats. De nouvelles crypto-monnaies ont adopté un système de validation des blocs différent : the proof of stake.

Celui qui veut devenir « mineur » sur une blockchain doit faire un dépôt de garantie important (en crypto-monnaie), ce dépôt est bloqué sur un compte. Le mineur doit disposer d'une infrastructure suffisante (mais un simple PC suffira dans ce cas). Les transactions sont collectées dans un bloc d'attente, à période fixe tous les nœuds se synchronisent sur un bloc, les transactions sont vérifiées par chaque nœud et un niveau de consensus est atteint, le bloc est scellé par son sha256 et on passe au bloc suivant.

A chaque scellement de bloc, l'algorithme tire au hasard quel nœud touche les commissions et la récompense en crypto-monnaie. Plus votre dépôt de garantie est important, plus vous avez de chance d'être tiré au sort par l'algorithme.

C'est un peu logique, plus vous êtes riche en crypto, plus vous avez intérêt à ce que les informations contenues dans la blockchain soient protégées et intègres. Donc dans cette histoire, plus vous êtes riche plus vous avez le droit de contrôler les transactions des pauvres, la morale traditionnelle est sauve...

Par contre si un mineur essaye de tricher et de fausser des informations, ça se verra tout de suite car son bloc ne sera pas en phase avec les autres blocs du réseau, il perdra sa preuve d'engagement (son dépôt de garantie). Aucun des nœuds n'a donc intérêt à tricher.

Le proof of work (avec le calcul du nonce) est une super protection de la blockchain, mais c'est sans doute bien trop fort (et même absurde). Le proof of stake est sans doute moins « protecteur » mais c'est sans doute suffisant. Ce système fonctionne correctement depuis plusieurs années pour de nombreuses cryptos comme le Solana, le Polkadot, … c'est sans doute ça l'avenir de la blockchain.

La suite de l'histoire

Toute idée considérée comme bonne est rapidement copiée. Quelques années après le Bitcoin, de nombreuses autres cryptos se sont crées sur le même schéma avec plus ou moins de succès.

En 2014, Vitalik Buterin et sept de ses potes geek ont crée l'Ethereum qui aujourd'hui est la deuxième crypto en terme d'importance. Ils sont partis de l'idée suivante : la blockchain du bitcoin permet de gérer des échanges de bitcoins mais ne permet pas de remplir le rôle d'une banque ou d'une assurance sans passer par un tiers. En effet si quelqu'un emprunte des bitcoins à une autre personne, l'échéance des remboursements se fait « à la main », le remboursement mensuel n'est pas automatique. Et c'est là qu'ils ont une idée « pas mal ». La blockchain c'est un réseau d'ordinateurs répartis sur toute la planète, et si on utilisait un peu de la puissance de calcul de chaque ordinateur pour constituer une espèce d'ordinateur mondial disponible 24h sur 24 et que personne ne pourrait pirater ni arrêter ?

L'idée était de stocker des « petits » programmes dans la blockchain (ils deviennent donc immuables et infalsifiables) et chaque nœud est chargé de les exécuter. C'est ce qu'ils ont appelé « les Smart Contract ». Comme toujours quand c'est un développeur qui choisi le nom, le résultat est parfois bizarre, et ici ça l'est particulièrement. Smart Contract, on traduit ça par contrat intelligent en français.

Un Smart Contract est un « petit » programme informatique stocké dans la Blockchain de l'Ethereum (il existe maintenant d'autres blockchain supportant les Smart Contract, mais c'est Ethereum qui a été la première).

Ces programmes sont écrits avec le langage Solidity et ça reste une affaire de spécialistes. Ces programmes peuvent encaisser de la crypto (de l'Ether mais aussi d'autres cryptos), ils peuvent gérer des mouvements de fond en crypto d'un compte à un autre, etc... Le maillon faible de ce système, c'est le développeur, il faut faire auditer le code avant une mise en production.

N'empêche que beaucoup d'applications ont été trouvées avec ces Smart Contract. L'idée de stocker des programmes de façon répartie sans qu'un « tiers de confiance » soit responsable de leur exécution est dans la droite ligne de la Blockchain.

Bien entendu, l'entente cordiale entre les huit geeks d'origine a volée en éclat rapidement, seul Vitalin Buterin est resté à la tête d'Ethereum, les autres sont partis et on fondé d'autres blockchain avec d'autres crypto-monnaies, par exemple Polkadot et Solana. Ces deux nouvelles blockchain apportent des améliorations, plus de rapidité, des blocks plus gros... Aujourd'hui, il y a entre 15 et 20000 cryptos différentes et un nombre de blockchain hallucinant, c'est la jungle !!

Pour le vocabulaire, une crypto-monnaie qui a sa propre blockchain (comme le Bitcoin, l'Ether, le Solana, …) s'appelle un « coin ». Une crypto-monnaie hébergée sur une autre blockchain s'appelle un « token ».

Solidity, j'ai testé pour vous !!

Il n'y pas à dire, c'est du costaud !! Plus sérieusement j'ai suivi la formation de « Ben BK », c'est un Foinc's pur jus qui propose quelques vidéos gratos sur Youtube. Pour quelqu'un maîtrisant un langage orienté objet (comme C++, Javascript, …), apprendre Solidity est facile. Il y a quelques particularités liées à la Blockchain. En quelques heures j'ai pu déployer mon premier Smart Contract sur une blockchain de test avec des cryptos fictives. Le développeurs disposent quand même de sacrés possibilités. Comme déjà dit plus haut, il y a intérêt à auditer le code réalisé, d'ailleurs un business s'est crée autour de ça.

Encore deux points importants

La blockchain sert à stocker des informations de « petite » taille comme des transactions, des petits programmes, des hash de titres de propriété. On ne va pas y stoker les films de Lola T par exemple, on ne va pas y stocker de gros documents.

Par contre on pourrait envisager d'y stocker l'empreinte d'un document (donc le hash256). Si une entreprise souhaite inscrire de façon indélébile qu'elle est en possession d'un document au jour d'aujourd'hui, elle numérise le document, elle met le hash256 du document numérisé dans la blockchain et elle conserve le document numérisé en lieu sûr. Dix ans après si elle veut prouver qu'elle était en possession du document (un contrat, un brevet), elle reprend le hash256 du document numérisé et elle démontre qu'il était dans la blockchain dix ans avant. Pour le moment ce n'est pas encore utilisé (à ma connaissance) mais c'est envisageable. L'idée est évoquée dans des vidéos, mais il y a sans doute des obstacles légaux.

La bockchain du bitcoin comme celle de l'Ethereum sont considérées comme étant lentes. Effectivement, valider un bloc toutes les dix minutes, c'est loin d'être du temps réel. La taille des blocs du bitcoin est de 1Mo, c'est très peu, c'était adapté en 2008.

Une anecdote à ce sujet : En 2017, des mineurs mécontents de la taille des blocs ont fait sécession et ont augmenté la taille à 8Mo, il ont crée le bitcoinCash. Le 31 Juillet 2017, si vous possédiez 10 bitcoins, et bien le 1er Août 2017 au matin vous possédiez 10 bitcoins et 10 bitcoinCashs, c'est Magique !! et cette génération spontanée de monnaie n'a pas affectée la valeur du bitcoin, bien au contraire, les gens ont envie de croire aux miracles, c'est ça qui fait la valeur du bitcoin !!

Depuis quelques années de nouvelles blockchain sont apparues (comme Solana, Polkadot, Polygon, Avalanche), certaines proposent de valider jusqu'à 50000 transactions par seconde, c'est prometteur, mais sont-elles aussi sécurisées que celle du bitcoin ?

La blockchain est-elle forcément adossées à une crypto-monnaie ?

A ma connaissance, aujourd'hui c'est le cas, les blockchain gèrent une crypto-monnaie principale pour payer les nœuds du réseau. Il serait tout à fait envisageable de créer une blockchain où les nœuds validateurs (les mineurs) seraient payés en Euros ou en Dollars, on ferait sans doute abstraction de toute cette folie spéculatrice qu'on connaît autour des crypto-monnaies.

Les mineurs seraient payés en Euros pour les services qu'ils rendent à la communauté des utilisateurs en vérifiant et en validant les transactions et les titres de propriété et en exécutant les « smart Contract ». On pourrait même envisager une espèce de banque ou d'assurance auto-gérée, avec une équipe de gouvernance décentralisée. Tout ça existe peut être déjà mais je n'ai pas vu.

Il faudrait payer les mineurs au juste prix, au vu du service rendu, ça pourrait être une espèce de Uber de la blockchain (mais sans Uber).

Un mot sur nos Youtubers « expert »

En France on a nos égéries de la blockchain. Historiquement nous avons le Hasheur qui parle du sujet depuis de nombreuses années, il est même consultant BFM, il parle de la blockchain comme de quelque chose de magique, on dirait qu'il a le bar's devant cette beauté ...

Nous avons aussi Claire Balva et Primavera de Filippi qui ont donné de nombreuses conférences USI ou Ted sur le sujet, elles parlent de la blockchain comme d'un truc... j'allais dire un quelque chose, mais non... (#bitcoin, #Rocco, etc...)

Beaucoup de jeunes (même au Tabagn's) ont accumulé des fortunes en crypto-monnaies, certains comme le hasheur sont multimillionnaire sans avoir bossé, tant mieux pour eux. Nombreux sont ceux qui se sont positionnés comme conseil en investissement crypto (token invaders, coin station, crypto farmer, la fricosphère…). En 2021 on a connu une ascension fulgurante (on parle de bull run) des cryptos, depuis quelques mois c'est l'inverse. Le bitcoin a connu un plus haut à 68000$, aujourd'hui il cote aux alentours des 30000$, c'est encore énorme pour quelque chose dont la valeur dépend uniquement de l'offre et de la demande. Tout ça rappelle beaucoup la bulle internet entre 1998 et 2001, mais à l'époque les actions représentaient des entreprises (certes surcotées), mais il y avait quand même l'entreprise en sous-jacent. Avec les cryptos il n'y a pas grand chose derrière, pour ne pas dire « rien » (sauf peut être pour les cryptos liées à des jeux vidéos).

Comment acheter et vendre des cryptos ?

Si vous voulez acheter du Bitcoin ou d'autres crypto-monnaies vous devez créer un compte sur des plates-formes d'exchange comme : binance, coinmarketcap, kucoin, kraken, …

Il y a pléthore de tutos sur internet. D'une certaine façon, ces sites d'Exchange sont une espèce de « tiers de confiance » (finalement on retombe dans le même problème qu'avant, seuls les noms ont changé. Il existe des plate-formes d'échange complètement décentralisée comme Uniswap ou Sushiswap, mais là c'est un sujet très technique que je n'aborderais pas maintenant).

Après inscription et le KYC (comme disent les Youtubers « expert ») vous devez virer des Euros vers votre compte. Ensuite vous pouvez passer des ordres qui vous feront gagner (ou perdre) un tas d'argent fictif.

Il est conseillé de ne pas laisser ses cryptos sur les plate-formes d'exchange (ils y en a qui ont essayés, ils ont eu des problèmes !!).

Il faut à minima se créer un crypto wallet avec des outils comme Metamask ou Phantom, ce sont des plugin pour navigateur. Il est conseillé de les associer à un hardware wallet (Ledger, Treezor, ...). C'est comme une clé USB avec un petit écran, ça vaut dans les 80 Euros. Sachez que si vous avez des Bitcoins ou des Ethers ou d'autres cryptos, vous avez un compte sous la forme d'une adresse sur la blockchain correspondante.

Ces comptes sont protégés par une paire de « clé publique / clé privée » (vous vous rappelez le truc RSA...)

Donc vous aurez autant de paires de clés que de crypto

différentes, vous ne devez jamais perdre vos clés privées ni les donner à qui que ce soit. Le meilleur moyen pour les conserver c'est sans doute le hardware wallet. Si un méchant vous pique votre hardware wallet il ne pourra pas en faire grand chose, car il y a encore un code d'accès.

Si vous cassez votre hardware wallet avec un darak, il reste un ultime système pour le restaurer. Lorsque vous activez votre wallet pour la première fois, vous recevez une liste de 24 mots, vous devez les recopier et les mettre au coffre. Avec ces 24 mots vous pourrez restaurer votre wallet. D'ailleurs une nouvelle technique de fishing a vu le jour, certains sites vous demande vos 24 mots « pour vérification », ne jamais les donner, ébid's.

Aller, un petit dernier pour la route. **C'est quoi un NFT ?**

Encore un mot à la mode, là encore, c'est un développeur geek qui a choisit le nom, donc c'est particulièrement étrange. NFT signifie « Non Fongible Token », il devait avoir des champign's aux arp's ou un truc comme ça ce jour là... Il y a des dizaines de Youtubers « expert » qui essaye de vous expliquer pourquoi ça s'appelle comme ça !! je vais être plus direct

Un NFT est un certificat (numérique) de propriété (c'est une clé de 64 chiffres), associé à une œuvre numérique (dessin, vidéo, musique, son, …) ou à un objet réel. Le principe est que le certificat est stocké dans la blockchain, il est donc immuable et infalsifiable. Comme dans la vie réelle, un certificat de propriété est unique.

Concrètement, au moment où vous achetez un NFT, un programme (smart contract) génère un couple « clé publique/clé privée » (vous vous rappelez le truc RSA). Le SHA256 de la clé publique est stocké dans la blockchain et la clé privée est stockée dans votre portefeuille (votre crypto wallet), c'est ça votre certificat de propriété. Pour votre culture, le moment où on génère les clés est appelé le MINT du NFT (mint = frapper, comme on frappe une pièce je suppose)

Posséder un NFT, ça prouve que vous avez acheté un certain objet et ce de façon immuable et infalsifiable (l'info est dans la blockchain).

Les premiers essais sur les NFT ont été fait en 2017 et c'était juste pour du test. Une série de 10000 dessins ont été mis en vente pour zéro Ether, donc gratuit. C'était la série des cryptopunk

Celui-ci, c'est le punk.5822, il s'est échangé en février dernier à 23 Millions de Dollar. Vous allez me dire que ce n'est qu'un dessin moche, peut être, mais c'est de l'art. Quelqu'un est propriétaire de cette œuvre, comme d'autres possèdent un Rembrand. Je peux reproduire le Rembrand dans le Chibrem's, mais je n'en suis pas le propriétaire. Un dessin fait sur une matrice de pixels peut avoir autant de valeur qu'un dessin fait sur une toile tissée avec des fils de coton.

Pour l'anecdote, les dessins cryptopunk ont été générés par assemblage de calques Photoshop, donc tous les dessins se ressemblent plus ou moins. L'un des calques utilisé pour le cryptopunk 5822 n'a été utilisé que 10 fois pour l'ensemble de la collection, c'est la rareté qui en fait le prix.

Il y a quelques années, le New-York Yacht Club a lancé une collection de 10000 NFT représentant des singes moches (tout est relatif) : les Bored Ape Yacht Club. Ils se sont associés à quelques célébrités comme Neymar, Beyoncé, … qui se sont chargés de faire le buzz sur les réseaux sociaux, la collection s'est écoulées à prix d'or (plusieurs centaines de milliers de Dollars chaque)

Posséder un « Bored Ape », c'est plus que posséder un simple dessin, le fait d'en posséder un vous donne accès à des soirées VIP et à des événements privatifs. C'est une appartenance à un club fermé, tout ça est une affaire marketing bien huilée, mais aussi un outil de spéculation. Pour l'anecdote, là encore c'est un assemblage de calques Photoshop.

Vous pouvez lancer votre propre collection de NFT avec Photoshop, il y a des tutos sur Youtube qui vous expliquent comment faire, mais à moins d'être fort en marketing ce serait étonnant que ça se vende. Attention quand vous « mintez » un NFT, vous écrivez une information dans la blockchain, et là il y a des frais non négligeables (on appelle cela le « gas »).

Tous les NFT ne sont pas des assemblages de calques Photoshop, de véritables artistes ont lancé la vente d'œuvres numériques sous forme de NFT, on trouve des dessins, des sculptures numériques, des animations, etc...

La place de marché la plus importante pour les échanges de NFT est https://opensea.io

Vous pouvez y jeter un œil pour vous faire une idée. Attention, si vous décidez de vendre une de vos œuvres par cette plate-forme, elle prend des frais qui sont loin d'être négligeable, et ils peuvent varier du simple au double d'une seconde à l'autre, c'est assez drôle, c'est une espèce d'enchère inversée qu'il faut saisir au bon moment.

Un NFT n'est pas forcément lié à une œuvre numérique, il peut aussi être associé à un objet physique, il y a une marque de chaussure de luxe qui fait déjà ça. A chaque achat, vous recevez votre titre de propriété sous la forme de NFT inscrit dans la blockchain et dans votre crypto-wallet. C'est peut-être du marketing, mais c'est sans doute l'avenir, les NFT constitueront peut-être un outil pour se protéger de la contre façon.

Les NFT pourraient aussi compléter ou remplacer les titres de propriété actuels et peut être permettre de se passer à terme de la fonction de Notaire.

Les jeux « play to earn »

Les crypto-monnaies et les NFT ont trouvé un positionnement très intéressant dans le monde du jeu vidéo et notamment dans les jeux liés aux premiers métaverses.

Par exemple dans le jeu « Axie Infinity », vous avez une crypto-monnaie (le AXS) qui vous permet d'acheter des personnages (qui sont en fait des NFT stockés dans la blockchain), des armes, des accessoires...

Cette crypto est cotée sur les sites d'Exchange comme Binance.com, d'ailleurs voici sont évolution sur un an (je reconnais que c'est pas très encourageant en ce moment, la valeur a été divisé par six en quelques mois mais elle a aussi été multiplié par six en quelques mois auparavant). C'est peut être le bon moment pour investir... ou pas !!

Pour commencer à jouer, vous devez acheter au minimum trois personnages, il peut y en avoir pour quelques centaines d'Euros si vous prenez des personnages un peu costaud. Vous partez ensuite au combat dans le métaverse, et si vous gagnez vous remportez de nouveaux personnages que vous pouvez revendre. Si vous perdez, binnnn, vous perdez !!

La bonne nouvelle, si vous achetez pour quelques crypto AXS une « Smooth Love Potion » vous pouvez tenter de multiplier vos personnages en les faisant se reproduire entre eux (c'est pas une blague). Il paraît que ce jeu fait fureur en Corée du sud, il y aurait même des personnes qui vivent des gains réalisés avec ce jeu.

Des jeux « play to earn » comme celui-ci, il y en a beaucoup d'autres comme Illuvium, Decentraland, … d'ailleurs Facebook cherche à se positionner sur ce marché.

Si vous avez eu l'énergie de me lire jusque là, vous êtes maintenant largement au même niveau que certains Youtubers « expert », bravo !!

Bon après ce « rapide » tour d'horizon du monde merveilleux des cryptos, de la blockchain … il reste quand même une question importante en suspend : « **et Lola, elle en pense quoi de tout ça ? »**

Merci de m'avoir lu et surtout que Gorgu vous l'agrandisse !! (la cotation du Bitcoin, ébid's)

Steeve