Juliette Bois / Bertrand Passieux

La blockchain à travers ses vulnérabilités de sécurité

INFO 002 - Cryptologie

UNIVERSITÉ SAVOIE MONT BLANC

SCIENCES ET MONTAGNE
UNIVERSITÉ SAVOIE MONT BLANC

La blockchain est une technologie qui date des années 1970.
Seule, cette technologie n'a pas beaucoup de valeur.
Mais couplée à la **cryptographie**, un **réseau peer-to-peer** et à un **consensus** (la preuve de travail par exemple) cela donne un assemblage très intéressant pour le partage de données pérennes et infalsifiables.
Cette technologie a été popularisée avec l'arrivée du Bitcoin en 2009, créé par un certain « Satoshi Nakamoto ». Si blockchain et Bitcoin ont été construits ensemble, il existe aujourd'hui de nombreuses blockchains et cryptomonnaies associées.

Sommaire

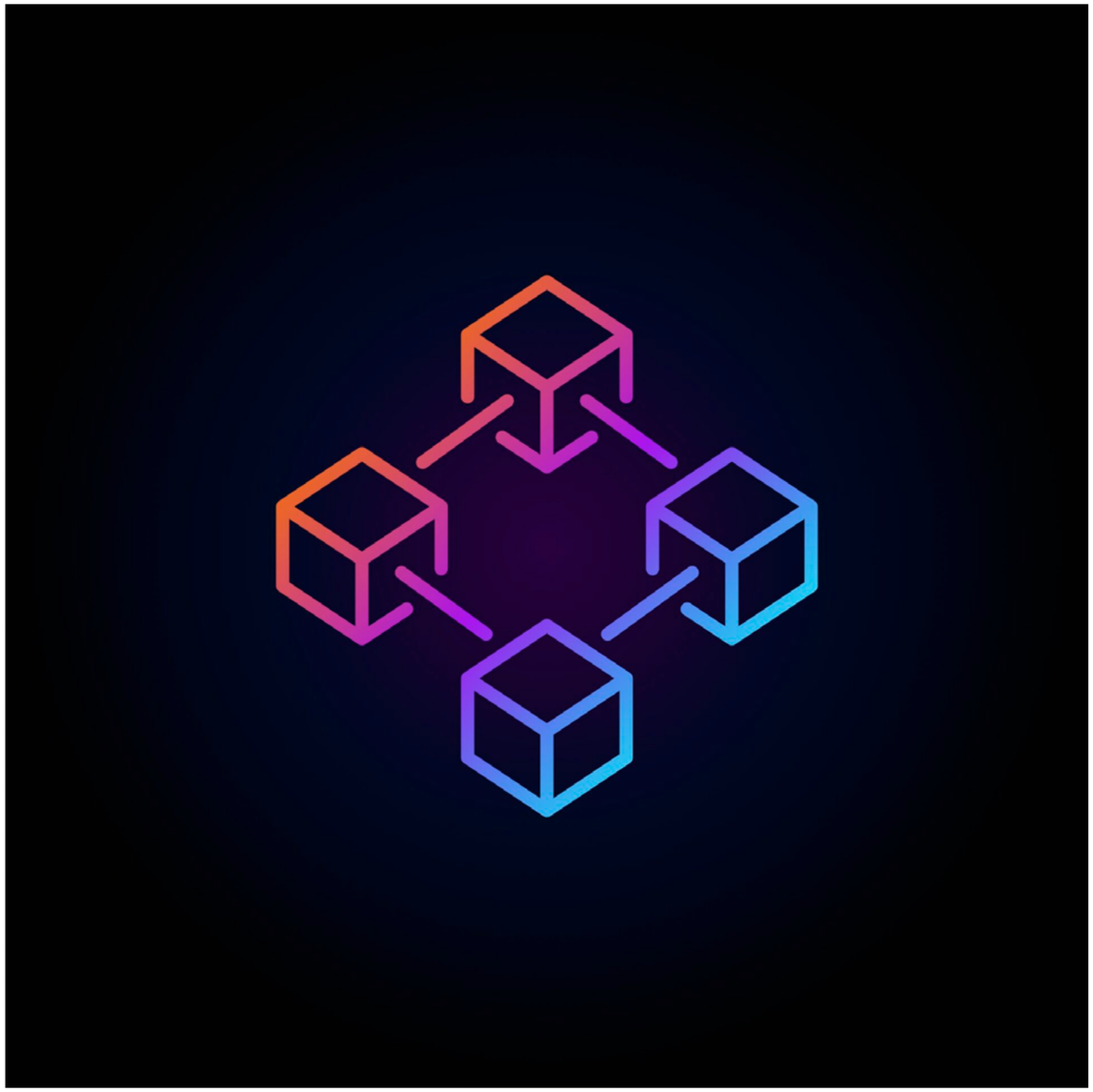
#1 - Introduction P.06
Comprendre le fonctionnement de la blockchain

#2 - Les algorithmes de consensus P.12
La preuve de travail / Proof-Of-Work
La preveu d'enjeu / Proof-Of-Stake
La blockchain permissionée

#3 - Les failles & attaques P.18
Les attaques liées à la blockchain et au minage
Les attaques liées au réseau Peer-to-Peer
Les attaques sur les smart contracts
Les attaques dérivées des blockchains

#4 - Conclusion P.40
Quel est l'avenir de la blockchain ? Ses atouts et ses limites

La blockchain à travers ses failles de sécurité



Comprendre la blockchain

Définir la blockchain simplement n'est pas chose évidente. Si l'on se réfère à l'Ethereum, la blockchain est une sorte de base données qui enregistre toutes les transactions ayant existé avec Ethereum. C'est une base de données décentralisée.

Problème

Avant de définir ce qu'est la blockchain, il faut comprendre ce qu'elle peut résoudre.

Aujourd'hui, si vous voulez transférer 100€ à un membre de votre famille, il vous faudrait contacter votre banque en leur demandant d'effectuer un transfert de votre argent vers le compte d'une autre personne. Votre banquier va donc vérifier que vous possédez la somme requise et fera la demande de transfert si tout est valide.

Ce qu'il vient de se passer, c'est que vous et la personne qui doit recevoir l'argent, avez fait confiance à votre banque pour gérer votre argent. Il n'y a eu aucun transfert physique de billet : tout s'est fait informatiquement dans un registre. Et c'est là où se trouve le « problème » du système actuel : vous devez faire confiance à une tierce personne.

Pourrait-il exister un système permettant de transférer de l'argent sans avoir besoin d'une banque ? ***Ou du moins est-il possible de gérer nous même ce registre contenant les transactions ?***
La blockchain est la réponse à cette question.

Explication illustrée

Pour expliquer le fonctionnement, prenons l'exemple d'un groupe de 10 personnes qui ne voudraient plus passer par une banque. Chaque membre connait la somme que chaque personne possède mais sans connaitre leur identité. A la place, un numéro leur est attribué allant de 1 à 10. Chaque personne a accès à une page blanche, prête à noter chaque transaction qui aura lieu.

Imaginons que le numéro 3 souhaite envoyer 5€ au numéro 6 :

1. Le numéro 3 annonce vouloir faire la transaction

2. Le groupe va vérifier qu'il possède bien les 5€

3. Si c'est le cas, ils vont noter sur la page :

- la date et l'heure de la transaction,
- le montant,
- le numéro de la personne qui envoie l'argent
- le numéro de la personne qui reçoit l'argent

4. La transaction est terminée

Avec le temps, d'autres personnes vont effectuer des transactions et elles seront notées sur la page. Cela continue jusqu'à ce que la page soit remplie.

On va dire qu'il est possible d'entrer jusqu'à 15 transactions par page. Pour pouvoir continuer, on va sceller cette page avec une clé sur laquelle tout le monde se sera mis d'accord. Cela servira à s'assurer que personne ne pourra modifier le contenu de ces pages. Une fois cette page placée dans un dossier, elle y restera indéfiniment.

Avant d'utiliser ce système de blockchain, c'était votre banque qui devait s'assurer que le registre des transactions ne soit pas altéré. Désormais, **ce rôle repose sur tous les utilisateurs du sytème**.

Explication technique

Une blockchain est une technologie de **stockage** et de **transmission** de données entre plusieurs utilisateurs.
Cette technologie peut être définie comme un **réseau** contenant un « grand livre partagé » public, **anonyme et infalsifiable**, dont le contenu est validé et sécurisé par un algorithme de calcul dit « minage » ou bien par des clés cryptographiques (voir la partie sur les algorithmes de consensus).

La blockchain s'apparente donc à une grande base de données : on y stocke, transmet et met à jour des informations de toutes sortes. Elle est partagée simultanément entre plusieurs individus.

Chacun des participants a alors accès à une copie de cette base de données mais également à tout l'historique qu'elle renferme. Elle est **partagée** par ses différents utilisateurs, **sans intermédiaire**, ce qui permet à chacun de vérifier la validité de la chaîne. Son architecture est qualifiée de **décentralisée**, puisqu'elle n'est pas hébergée par un serveur unique, mais qu'elle fonctionne en « **peer-to-peer** », c'est-à-dire d'utilisateur en utilisateur.

La blockchain évolue de manière **autonome**, sans organe de contrôle : les utilisateurs sont autorisés à modifier cette base de données à tout moment (ajouter des informations, vérifier une transaction, etc...), seulement après avoir été préalablement identifiés par un système cryptographique.

Un peu de vocabulaire

Cette technologie se compose de 3 concepts importants : les **blocs**, les **nœuds** et les **mineurs**. Lorsqu'une transaction est partagée sur le réseau pair-à-pair, elle est collectée par des mineurs et, pour des raisons d'efficacité, traitées par lots (appelés blocs) afin de les valider.

Les blocs : ce sont des **regroupements de transactions** (la feuille blanche de l'exemple illustré ci-dessus). Ces transactions se distinguent les unes des autres par un **identifiant unique** appelé « hash ». Ces blocs sont chaînés les uns aux autres. Et c'est ce qui rend leurs données immuables.

Les noeuds : ce sont les **machines** connectées à la blockchain. Chacune d'entre elles héberge une **copie de la base de données** qui contient l'intégralité des échanges entre utilisateurs.

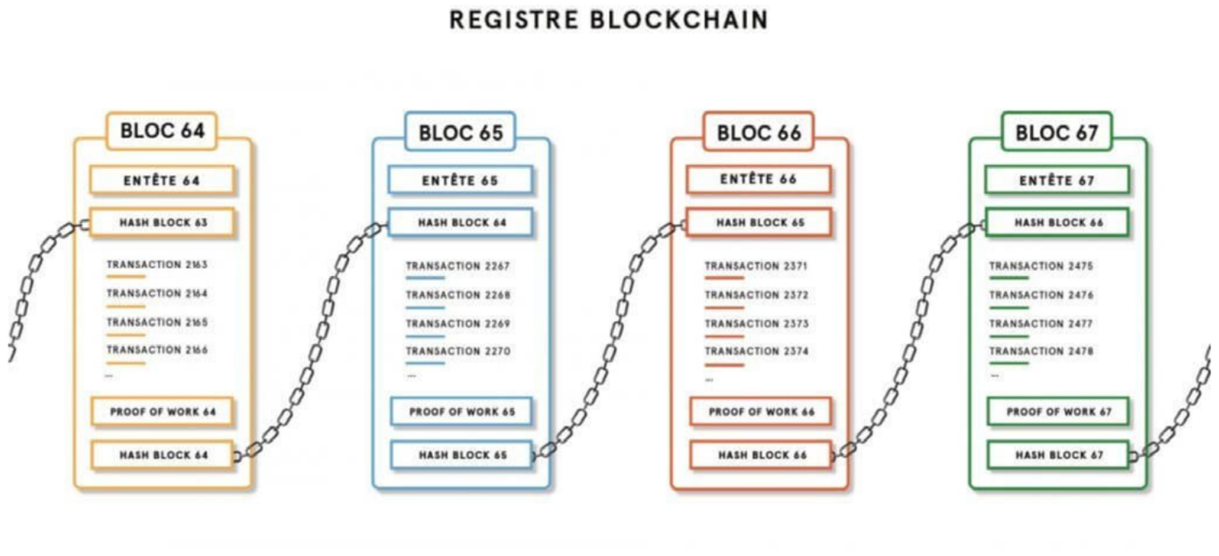
Les mineurs : ils sont chargés de vérifier si les nouveaux blocs créés correspondent aux **standards de sécurité**. Ils possèdent un rôle absolument essentiel au sein de la blockchain, puisqu'ils **garantissent l'authenticité des blocs**, et donc de l'ensemble de la chaîne.

Chaque bloc a 5 composants :

- le **hachage** qui permet de faire référence au bloc précédent,
- toutes les **transactions** qui y sont enregistrées,
- un nombre arbitraire donné en cryptographie, appelé **nonce**
- la « **preuve de travail** », une réponse possible au nonce
- le « **hash** » du bloc, qui est l'empreinte numérique unique

Les mineurs créent ainsi de nouveaux blocs faisant suite aux blocs précédents déjà existants, par un processus appelé le **minage**. Grâce à cela, il est quasiment impossible d'extraire un bloc existant pour le modifier, ou de le falsifier.

Une fois vérifié par des milliers d'ordinateurs, le bloc est ajouté à un nœud, appelé **chaîne de blocs**, et le mineur peut être récompensé financièrement. D'où le terme « blockchain ».



Les algorithmes de consensus

Comment les blockchains se sécurisent-elles ?

Lorsqu'une transaction est émise, elle est donc immédiatement mise en commun avec d'autres opérations libérées au même moment : ces dernières sont regroupées en un bloc. Une fois créé, ce bloc doit être contrôlé pour décider par consensus si oui ou non, on peut l'ajouter sur le réseau.

Un algorithme de consensus, ou mécanisme de consensus, est un procédé par lequel les noeuds d'un réseau pair-à-pair **se mettent d'accord** sur un ensemble d'informations. Dans le contexte des cryptomonnaies, un tel algorithme permet aux noeuds d'être en consensus sur le réseau de transactions (la blockchain) afin de **continuer la création de nouveaux blocs**.

Le mécanisme de consensus d'une blockchain permet donc au réseau de se mettre d'accord sur une **version unique de l'histoire**. Mais il existe plusieurs manières de tomber d'accord.

Le Proof-Of-Work : la preuve de travail

Ce procédé cryptographique consiste à créer de nouveaux blocs en résolvant un **calcul mathématique complexe**. Les mineurs assurent cette fonction. Le principe est assez simple : les noeuds du réseau doivent résoudre un problème cryptographique **en dépensant de l'énergie**.
La fonction de hachage utilisé est le **double SHA256**.

Pour résoudre cette énigme et, par conséquent, valider un bloc, il faut ainsi que l'ordinateur soit assez puissant pour effectuer ces calculs. Sur le principe, les utilisateurs d'une blockchain ne sont pas clairement identifiés et peuvent donc créer plusieurs identités afin d'inonder le réseau, dans le but de résoudre une grande quantité de blocs

La preuve de calcul a également pour intérêt de faire en sorte que le registre soit immuable et irréversible, en rendant presque impossible la réécriture des blocs précédents. C'est une manière supplémentaire de freiner les abus.

De plus, si des blocs commencent à être produits trop rapidement, cela signifie que les calculs sont faits (trop) rapidement, un **mécanisme d'auto-ajustement** se met en place en ajustant la difficulté des calculs à la puissance de calcul des ordinateurs, **freinant ainsi la production de blocs**.

Cependant, cette solution amènent une autre problématique : l'importante consommation énergétique que cela entraîne.

Le Proof-Of-Stake : la preuve d'enjeu

Ce procédé est moins gourmand en ressources et se caractérise par une désignation aléatoire d'un mineur pouvant ajouter un bloc à la blockchain, en lui demandant de **mettre en jeu des crypto-monnaies (des tokens)**.

Plus une personne possède de tokens et plus elle aura de chance d'être choisie pour créer un nouveau bloc. En échange, elle touche une partie des **frais de transactions** qui sont inscrites dans ce nouveau bloc. Ainsi, pour avoir une chance de vérifier les transactions d'un bloc - et de percevoir les frais associés - les mineurs doivent bloquer un minimum de fonds virtuels, qu'ils ne peuvent pas dépenser.

Le principal avantage de ce mécanisme de validation est qu'il permet de réduire l'importante dépense d'énergie liée à la preuve de travail. Certains estiment, en revanche, que ce système de validation ne présente pas un aussi bon niveau d'immutabilité.

Résumons, quelles sont les différences entre la preuve d'enjeu et la preuve de travail ?

	Comment miner ?	Que gagnent les mineurs ?	Utilisation de ressources	Degré de décentralisation	Rapidité des transactions	Frais de transactions
Proof-Of-Stake	Grâce à l'achat d'équipement informatique	De nouveaux tokens crées spécialement	Très forte	Faible	Lente	Assez élevées
Proof-Of-Work	Posséder un certain nombre de tokens de la crypto-monnaie	Une partie des frais de transaction	Faible	Elevé	Assez élevée	Faibles

Pour résumer, les deux méthodes permettent la même chose, c'est-à-dire la création et la validation de blocs dans une blockchain. Chaque méthode à des avantages et des inconvénients.

Un des gros avantages de la **preuve d'enjeu (PoS)** est le **gain énergétique**. Inutile de dépenser des quantités astronomiques d'électricité pour pouvoir valider les transactions et les inscrire dans la chaîne de bloc. Un des gros avantage de la **preuve de travail (PoW)** est la **sécurité des transactions** car elles doivent toutes être validées par les mineurs.

La blockchain permissionnée

Dans certains cas, ces deux mécanismes de validation ne sont pas toujours adaptés. La transparence totale et la décentralisation des informations (et donc l'accessibilité par tous), qui apparaissent comme un gros avantage de ces blockchains **publiques**, peuvent en effet poser soucis pour les industriels qui veulent échanger entre eux des informations plus ou moins confidentielles.

La blockchain permissionnée répond à ce problème. Celle-ci voit son réseau accessible seulement à un **nombre limité d'utilisateurs**. Chaque nouveau membre doit ainsi être accepté par les membres déjà existants dans le consensus, et aura des droits d'accès différents à la donnée en question. Les validateurs sont connus, et totalement transparents entre eux.

> Finalement, une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. Ce processus prend un certain temps selon la blockchain considérée (environ une dizaine de minutes pour Bitcoin, 15 secondes pour Ethereum).

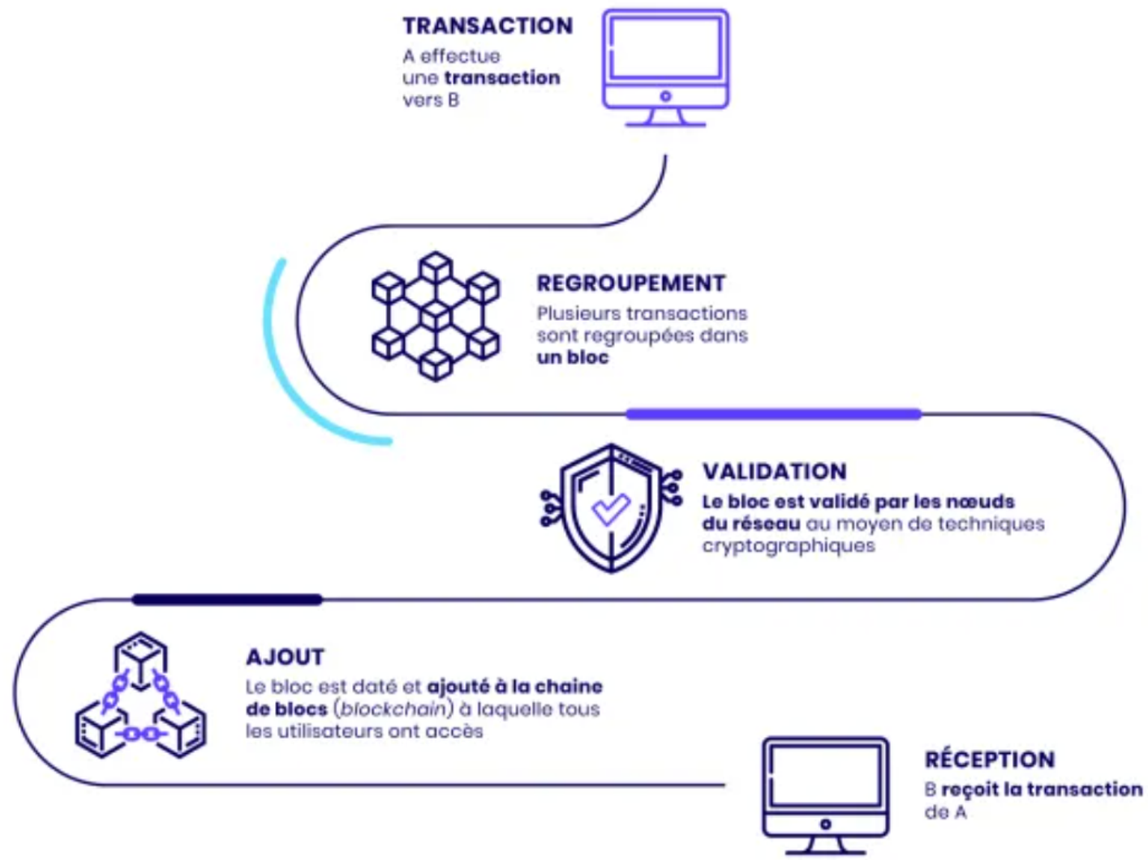


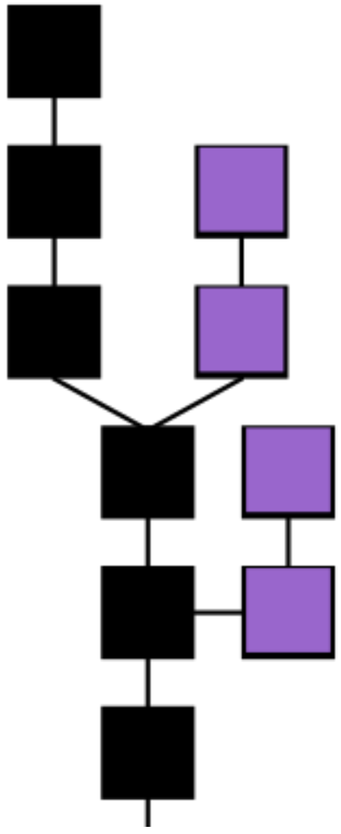
Schéma récapitulatif du fonctionnement d'une blockchain

Les failles et les attaques

Les blockchains ont-elles déjà présentées des failles ? Quelles attaques ont déjà eu lieu ?

Comme tout système, la blockchain n'est pas une solution parfaite : des points de vulnérabilités existent : des risques applicatifs et d'autres liés à l'humain.

1. Les attaques liées à la Blockchain et au minage



Étant donné qu'il est possible d'y avoir deux preuves de travail trouvées en même temps, la plupart des blockchains proposent une solution simple : **la chaîne la plus longue est conservée**.

La plupart du temps, une chaîne devient plus grande que les autres au bout de quelques blocs. Les mineurs se mettent alors à miner sur la « bonne chaine » (la plus longue donc) car rattraper son retard en continuant de miner n'est pas profitable et n'est possible que dans de rares cas.

L’attaque à 51%

Prenons comme exemple l’attaque 51%. Rappelons que l’un des atouts clés de la blockchain est la **nature distribuée** de la création et de la vérification des données. Le travail décentralisé des nœuds garantit que tous les participants du réseau soient d’accord sur l’état actuel de la blockchain.
C’est l’une des principales raisons pour lesquelles les réseaux blockchain ont tendance à être qualifiés de sécurisés.

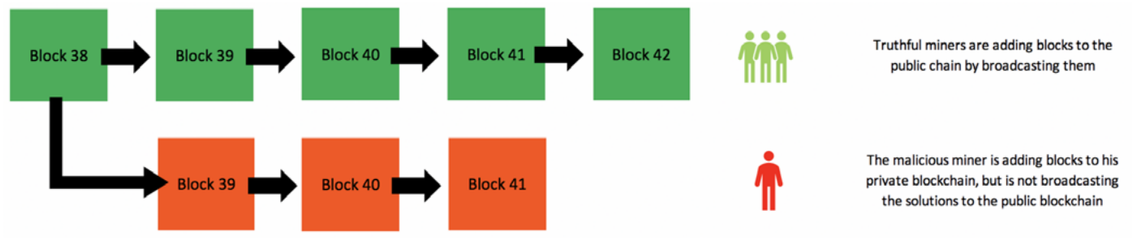
Cela signifie que la majorité des nœuds doivent régulièrement se mettre d’accord sur le processus de minage, la version du logiciel utilisé, la validité des transactions, etc...

Mais alors que se passe-t-il lorsque le taux de hachage n’est plus suffisamment distribué ? Que se passe-t-il si, par exemple, une seule entité est capable d’obtenir plus de 50 % de la puissance de hachage ?

Une des conséquences possibles est ce que l’on appelle une attaque à 51 %, également appelée attaque de majorité.

Le principe est simple : l’attaquant (ou le groupe d’attaquants) dispose de **51% ou plus du hashrate** du réseau de la blockchain, entraînant potentiellement une perturbation du réseau. Le hashrate, ou taux de hachage, est la vitesse/puissance de minage. Il est calculé en unité d’hash/seconde. Avec une telle puissance, il aura beaucoup plus de chance de découvrir une preuve de travail qui satisfera le nonce.

Ainsi, lorsque les attaquants disposent d’une majorité de la puissance de calcul du réseau, ils peuvent volontairement **exclure ou modifier l’ordre des transactions**. L’attaquant pourrait également **inverser les transactions** qu’il a effectué tout en possédant le contrôle, ce qui entraînerait un problème de double dépense.



L’attaquant mine plus vite sans publier ses blocks pour faire de la double dépense

Une attaque à 51% permettrait aussi à l'attaquant d'empêcher la confirmation de certaines ou de toutes les transactions (déni de service de transaction) ou d'empêcher certains autres mineurs de miner, ce qui conduirait au **monopole de minage**. En d'autres termes, l'attaquant peut décider des transactions qui seront validées et de celles qui ne le seront pas.

D'un autre coté, une attaque à 51% ne permettrait pas à l'attaquant de renverser les transactions des autres, ni d'empêcher la diffusion des transactions sur le réseau. Changer les récompenses du bloc, créer des tokens à partir de rien ou voler les tokens qui n'ont jamais appartenu à l'attaquant sont également des scénarios très improbables.

Cependant, l'attaquant peut aussi décider de ne pas partager les blocs qu'il trouve. Auquel cas, il va dépenser la monnaie sur la chaîne public actuelle et falsifier son bloc en cours, où il ne dépensera pas d'argent.

Généralement, l'attaque des 51 % est dirigée contre les blockchains de type Proof-of-Work (PoW), tout simplement parce que dans ce type d'architecture décentralisée, ce sont les transactions approuvées par la majorité qui sont enregistrées dans le registre de transactions.

Quelle est la probabilité d'une attaque à 51 % ?

De manière générale, plus le réseau est grand, plus il bénéficie d'une protection renforcée contre les attaques et la corruption de données car la possibilité qu'une seule personne obtienne une puissance de calcul suffisante pour submerger tous les autres participants atteint rapidement des niveaux invraisemblables.

Dans le cas du Bitcoin ou de l'Ethereum, les mineurs rejoingnent le réseau afin de **contribuer à la croissance et à la sécurité** du réseau.

Ils n'ont donc aucune raison d'investir de grandes quantités de ressources si ce n'est pour agir honnêtement et **s'efforcer de recevoir la récompense du bloc**. Par conséquent, une attaque des 51 % sur la blockchain du Bitcoin est plutôt improbable.

De plus, le changement des blocs précédemment confirmés devient de plus en plus **difficile** au fur et à mesure que la chaîne se développe, car **les blocs sont tous liés** par des preuves cryptographiques. Pour la même raison, plus un bloc a de confirmations, plus les **coûts** de modification ou d'annulation des transactions de ce bloc sont élevés. Par conséquent, **une attaque réussie ne pourrait probablement modifier que les transactions de quelques blocs récents, pendant une courte période.**

Ethereum Classic (ETC) a été la cible de deux attaques des 51 %. Une première tentative a eu lieu entre le 31 juillet et le 1er août 2018. Le responsable de cette attaque avait pu s'en tirer avec plus de 807 000 ETC, soit 5,68 millions $ à l'époque. Pour la réussite de ce projet, il avait déboursé 192 000 $ en Bitcoin (BTC). Quelques jours plus tard, le 6 août, une nouvelle attaque avait eu lieu et avait entraîné la réorganisation de 4 000 blocs de la blockchain.

Il existe cependant d'autres crypto-monnaies dont leurs blockchains ont un pouvoir de hachage trop faible pour se sécuriser suffisamment, ce qui permet à des attaques à 51 % de se produire. Monacoin, Bitcoin Gold et ZenCash sont quelques exemples notables de crypto-monnaies victimes d'attaques à 51%.

Pour aller plus loin, imaginons un scénario dans lequel une entité malveillante n'est pas motivée par le profit et décide d'attaquer le réseau Bitcoin uniquement pour le détruire, quel qu'en soit le coût. Même si l'attaquant parvient à perturber le réseau, le logiciel et le protocole Bitcoin seraient rapidement modifiés et adaptés en réponse à cette attaque.

Cela nécessiterait que les autres nœuds du réseau parviennent à un consensus et à un accord sur ces changements, mais cela se produirait probablement très rapidement lors d'une situation d'urgence. Bitcoin est très résistant aux attaques et est considéré comme la crypto-monnaie la plus sécurisée et la plus fiable qui soit.

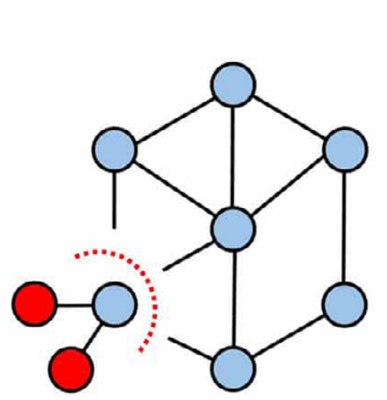
Selfish mining attack

Il s'agit d'un dérivé de l'attaque 51%. Si on a la chance d'avoir une preuve de travail en premier, on peut choisir de risquer sa récompense de minage pour une double dépense. En revanche, cette méthode est moins rentable que l'attaque 51%.

2. Les attaques liées au réseau peer-to-peer

L'attaque Eclipse

L'attaque Eclipse est une attaque malicieuse qui consiste à **isoler un nœud** d'un réseau Peer-to-Peer afin de **rediriger les connexions** entrantes et sortantes de la victime vers des nœuds contrôlés par l'attaquant.



La victime se retrouve alors dans un réseau séparé de celui dont elle pense faire partie : elle répond alors des nœuds de l'attaquant.

Cette attaque est rendue possible car il est impossible pour un nœud dans un réseau décentralisé d'être en relation avec tous les nœuds du réseau. Contrairement à l'attaque Sybil, l'attaquant n'a donc pas besoin de cibler l'entièreté du réseau.

Pour ce faire, l'attaquant peut utiliser des botnet pour **créer un « barrage d'adresses IP » afin d'en inonder la cible**. Avec suffisamment d'adresses IP, un attaquant peut éclipser n'importe quel nœud. Ainsi, lors de la reconnexion de la victime sur le réseau de la blockchain, elle se synchronisera peut-être sur une de ces adresses.

Plusieurs itérations peuvent être nécessaires. Néanmoins, un redémarrage peut être forcé (avec une attaque DDoS sur la cible) pour **forcer la victime à se reconnecter au réseau**, ou alors l'attaquant peut simplement attendre que cela se produise.

Une fois l'attaque lancée, la victime sans méfiance est à la merci des nœuds malveillants. La victime est isolée et l'attaquant va lui **envoyer de fausses données**, sans que la victime puisse s'en rendre compte.

Quelles sont les conséquences d'une attaque Eclipse ?

1. Une double dépense sur des transactions 0-confirmations :

Une transaction peut avoir été diffusée. Mais tant qu'elle n'a pas été incluse dans un bloc (et donc engagée dans la blockchain), l'expéditeur peut facilement créer une nouvelle transaction qui dépense les mêmes fonds ailleurs. Si la nouvelle transaction a des frais plus élevés, un mineur l'inclura probablement avant l'original, invalidant la précédente.

Certaines entreprises et certaines personnes acceptent ces transactions 0-confirmations. *Prenons par exemple un marchand, Bob, qui vend des véhicules. Il ignore qu'Alice a éclipsé son nœud et il ne soupçonne rien alors qu'elle commande sa voiture de luxe.*

Elle crée une transaction, que Bob diffuse ensuite sur le réseau. Satisfait que le paiement soit en cours, il remet les clés de la voiture et Alice s'échappe. Bien sûr, la transaction n'a pas été diffusée sur le réseau : Bob n'a fait que la relayer aux nœuds malveillants d'Alice, qui ne la transmettront donc pas à des noeuds honnêtes.

Alors que cette transaction est bloquée, Alice dépense ces mêmes fonds sur le réseau (réel), que ce soit en direction d'une autre partie ou à une adresse qu'elle possède elle-même. Même si la transaction initiale vers Bob est finalement ouverte, elle sera rejetée car les coins ont déjà été dépensés.

2. Une double dépense sur des transactions N-confirmations :

Cela nécessite plus de préparation. Beaucoup d'entreprises préfèrent **attendre un certain nombre de confirmations avant de marquer un paiement comme valide**, pour plus de sécurité. Pour contourner cette situation, l'attaquant doit éclipser en même temps les mineurs et le marchand.

Une fois que l'attaquant a établi l'ordre auprès du marchand, il transmet une transaction aux mineurs (éclipsés). La transaction est confirmée et incluse dans la blockchain – mais cette blockchain n'est pas la chaîne que la majorité du réseau partage, puisque le mineur est momentanément coupé du réseau.

À partir de là, l'attaquant relaie cette version de la blockchain au marchand, qui libère les marchandises selon la croyance que la transaction a été confirmée. Une fois que les nœuds éclipsés rejoignent le réseau actuel, la blockchain sur laquelle ils croient par erreur être valides se trouve en réalité devenue orpheline de celle sur laquelle le reste du réseau a travaillé.

3. Perturbation de la puissance de minage et affaiblissement des mineurs concurrents

Un nœud éclipsé continuera à fonctionner, aveugle quant au fait d'avoir été séparé du réseau. Les mineurs continueront à miner des blocs dans le cadre des règles établies par le protocole, mais les **blocs ajoutés seront supprimés** lorsque les noeuds se synchroniseront de nouveau avec des pairs honnêtes.

Ainsi, en ne communiquant pas ou à posteriori le fait qu'un bloc ait été miné, la victime gâchera son hashrate en minant « pour rien ». De ce fait, la part de l'hashrate sur le réseau augmente.

Théoriquement, en multipliant le nombre d'attaques sur une blockchain de faible/moyenne valeur, il est possible d'augmenter ses revenus de cryptomonnaie voire même de pouvoir essayer une attaque à 51%.

En réalité, le coût pour prendre en charge la majorité de la puissance de hachage de certaines blockchains (Bitcoin par exemple) est tout simplement bien trop élevé même pour le plus riche des attaquants possible – à ~80TH/s, l'entité aurait besoin de plus de 40TH/s pour tenter une telle manœuvre.

Comment éviter une attaque Eclipse ?

La meilleure manière d'empêcher un attaque Eclipse est d'anticiper. Étant donné qu'il s'agit d'une attaque dépendant du réseau, il est bon de **faire le nécessaire lors de la conception** et non de alors que le réseau est déjà déployé.

Le mieux étant de :

- Mettre en place une sélection de nœuds aléatoire. Si le réseau se base sur moins de critère, alors les manipulations de l'attaquant ne seront pas aussi simples.
- OU Faire une sélection de nœuds déterminée, se faisant, quasi-impossible à attaquer avec cette méthode. En précisant que ce genre de sélection inclut souvent des restrictions sur les nouveaux nœuds (1 seul nœud par @IP/machine,…).
- Augmentation du nombre de connexions entre les nœuds. Donc plus difficile d'isoler la cible.
- Bloquer les connexions entrantes, et de ne faire que des connexions sortantes vers des noeuds spécifiques (comme ceux qui ont été mis en liste blanche par d'autres pairs).

Au final, il ne s'est encore jamais produit d'attaque Eclipse ayant eu des conséquences sérieuses, mais la menace existe toujours malgré les contre-mesures intégrées dans le réseau. Comme pour la plupart des vecteurs d'attaque qui existent, **la défense la plus forte sera celle qui rend financièrement irréalisable** les tentatives d'attaque de la part de parties malveillantes.

L'attaque Sybil

L'attaque Sybil se rapproche de l'attaque Eclipse, sauf que ce n'est pas un ou quelques nœuds qui sont pris pour cible, mais le **réseau entier**.

Les fins de l'attaquant restent les mêmes, mais la faille principale est le fait de pouvoir multiplier au plus ses identités sur le réseau (c'est-à-dire créer énormément de nœuds à partir d'une seule machine).

3. Les attaques sur les smart contracts

L'augmentation de la visibilité des blockchains a amené de nouveaux types d'organisations : les Organisations Autonomes Décentralisées (DAO : Decentralized Autonomous Organisation).

Ces Organisations sont dites **autonomes** car elles sont **publiques**, car publiées sur une blockchain, et leurs « comportements » sont régis par des « smart contracts ». Les smart contracts se présentent sous la forme de code qui permet **automatiquement** la **vérification**, l'**exécution** ou la **réfutation** des clauses d'un contrat.

Pour résumer, une DAO se forme à partir d'une campagne de financement ; tous les acteurs font à la fin partie de l'organisation. L'organisation fonctionne autour des smart contracts qui ont été définis et rendus publiques durant la campagne de financement.

Une fois la DAO et les smarts contrats dans la blockchain, impossible de les modifier (sauf s'il s'agit d'une modification prévue dès la conception).

La blockchain semble parfaitement adaptée à l'application des DAO et des smart contracts. Cependant, si la DAO est exposée à des vulnérabilités, il est bien plus difficile voire impossible de faire des modifications. Les effets de bords peuvent alors être immenses

L'exemple le plus célèbre : The DAO, une des premières DAO

The DAO a émergé au sein de la société Slock-it, profitant de la blockchain Ethereum. Ses participants pouvaient voter pour des projets et les financer. Avec plus de 4000 membres sur le Github du code de The DAO, la campagne de financement fut un succès.

Il s'agit d'ailleurs de la campagne de crowdfunding la plus fructueuse de tous les temps, avec plus de 150 Millions de dollars engagés par plus de 11 000 personnes à la fin de la campagne en Mai 2016.

Cependant, une faille dans un smart contract a été rapidement aperçue par plusieurs utilisateurs. L'un d'entre eux procèdera à une attaque le 17 Juin 2016. Le bilan : l'attaquant réussit à récupérer près de 3 millions d'Ether soit environ 50 millions de dollars à ce moment-là. 35 jours plus tard, il prend le contrôle total d'un autre smart contract dans lequel il injecte ces fonds.

35 jours, c'est le délai qu'il faut à l'attaquant pour récupérer sa crypto-monnaie. Pendant ce temps, l'organisation et la communauté Ethereum prennent conscience de ce qu'il vient de se passer. **La confiance sur la blockchain baisse**.

La communauté vote à la grande majorité pour fork la chaîne, afin de « préserver » l'argent que l'attaquant a récupéré. Cela reste cependant contre le principe de la blockchain.

Le fork se fait le 20 Juillet et divise la communauté Ethereum, la majorité se concentrant sur la « nouvelle » blockchain, l'autre sur l'ancienne désormais appelée Ethereum Classic.

Cette attaque a soulevé plusieurs points critiques sur la blockchain. Elle nous montre l'engagement et la confiance que beaucoup ont en cette technologie, mais, nous fait surtout relativiser sur le principe même de la blockchain : elle n'est pas purement et simplement immuable.

La politique et les décisions sont toujours appliquées par des **humains qui peuvent choisir d'intervenir** quand cela leur semble nécessaire. La sécurité, la conception des organisations sur les blockchains ainsi que les modèles de gouvernance des blockchains plus globalement.

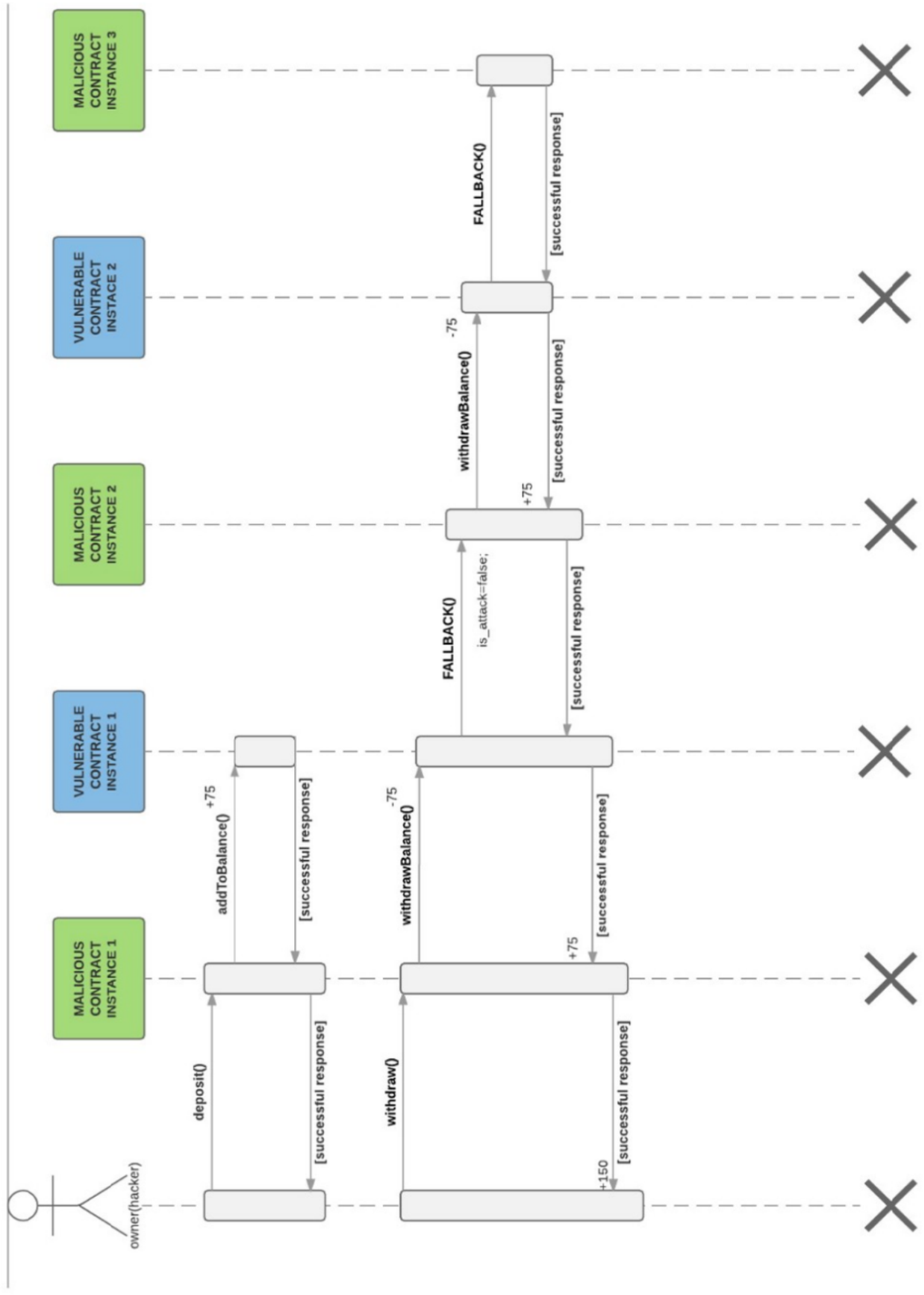
Comment un smart contract peut-il être vulnérable ?

En reprenant la vulnérabilité du contrat de The DAO, il s'agit simplement d'une erreur de conception dans le code de retrait de fonds.

La procédure de retrait du smart contrat se fait de telle manière :
- l'appel à la fonction de retrait
- le retrait
- la mise à jour des fonds

Le problème se trouve au niveau de l'ordre d'exécution. Effectuer le retrait avant la mise à jour des fonds est une faille que l'attaquant a su exploiter.

En effet grâce à du code malveillant (ici un autre contrat), il est possible de faire un appel récursif au smart contrat vulnérable, cela va exécuter une nouvelle fois le retrait des fonds AVANT la mise à jour de ces derniers. C'est ainsi, grossièrement, que l'attaquant a pu s'en prendre à The DAO.



4. Les attaques dérivées des blockchains

Le cryptojacking

Le cryptojacking n'est pas vraiment une faille des blockchains. Mais depuis leurs apparitions et surtout celles des cryptomonnaies, une nouvelle arnaque est apparue : le cryptojacking.

Le but du cryptojacking est d'utiliser les appareils des victimes (ordinateurs, smartphones, tablettes, serveurs) et **s'en servir pour miner en secret de la cryptomonnaie**. Le hacker peut alors augmenter son hashrate sans avoir à acheter d'équipement dédié, et donc, augmenter ses revenus en cryptomonnaie.

Le cryptojacking peut être **difficile à percevoir** pour la victime, selon la subtilité du hack. Il y a une possibilité de le détecter avec le ralentissement des autres processus, l'augmentation des factures d'électricité, et le raccourcissement de la durée de vie des appareils.

L'attaque se fait à travers des pièces jointes malicieuses ou via le navigateur de la victime (JavaScript).

Difficile de se défendre contre ce hack, le plus efficace reste les antivirus, les programme de cybersécurité et des add-ons anti-minage pour les navigateurs (par exemple « No Coin » ou « minerBlock ».

Conclusion

Quel est l'avenir de la blockchain ? Quels sont ses atouts ? Et quelles sont ses limites ?

Au final, la blockchain est une technologie jeune mais dont **l'avenir est prometteur**. Le chemin vers une adoption grand public est encore long, mais de nombreux secteurs commencent à prendre conscience des atouts d'un tel système.

En effet, en promettant **transparence et sécurité des données**, cette technologie trouve progressivement sa place dans plusieurs secteurs, créant une multitude de nouveaux cas d'utilisation en dehors de du domaine **monétaire** (**médical**, **agroalimentaire**, **énergie**, **immobilier**, **assurance**, **banque** ...).

Les blockchains pourraient enregistrer en toute sécurité des données sous forme de dossiers médicaux, d'identités, de récits historiques, d'enregistrements fiscaux, de votes, de certificats d'authenticité et bien d'autres choses encore !

La blockchain à travers ses failles de sécurité

Les prochaines années verront probablement les entreprises et les gouvernements expérimenter de nouvelles applications, afin de déterminer dans quels domaines la blockchain apporterait le plus de valeur.

La blockchain, c'est

Traçabilité + Sécurité + Efficacité

Ainsi, les données de la blockchain demeurent :

- **chronologiques** : les transactions sont intégrées les unes à la suite des autres au fil du temps
- **immuables** : les informations ne peuvent être supprimées. Une fois la transaction certifiée, elle est inscrite dans l'historique de façon indélébile
- **infalsifiables** : il est impossible de modifier une transaction après son intégration à la blockchain. En cas d'erreur, une deuxième transaction annulant la première doit apparaître. Les deux seront alors visibles

Bien qu'elle soit extrêmement prometteuse, la technologie blockchain semble encore immature sur certains points. Elle comporte des zones d'ombre qu'il est essentiel de connaître :

- Les différentes **attaques** présentées dans ce document et bien d'autres !

- La **modification des données** très difficile. Cette stabilité est un point positif certes, mais si vraiment nous avons besoin de faire une modification pour une raison exceptionnelle, modifier les données ou le code d'une chaîne de blocs est généralement très exigeant et nécessite souvent une bifurcation dure (ou hard fork en anglais). Une chaîne est abandonnée alors qu'une nouvelle est formée.

- La **clé privée** : si l'utilisateur final perd sa clé privée et que des transactions sont effectuées sans son accord, les données seront inaltérables compte tenu des principes vus précédemment et il pourra perdre tous ses tokens car il ne pourra plus accéder à ses fonds.

- L'**inefficacité des Proof-Of-Work** : le minage est très compétitif et comme il n'y a qu'un seul gagnant toutes les dix minutes, le travail de tous les autres mineurs est gaspillé. Dans cet esprit compétitif, les mineurs cherchent continuellement à augmenter leur puissance et consomment de plus en plus d'énergie. Pour le Bitcoin, cela représentent une consommation plus grande que celle de nombreux pays, comme le Danemark, l'Irlande ou le Nigéria.

- **Espace de stockage** : les registres sur la Blockchain peuvent devenir très volumineux avec le temps. La blockchain Bitcoin nécessite actuellement environ 200 Go de stockage. La croissance actuelle de la taille de la blockchain semble dépasser celle des disques durs. Le réseau risque de perdre des nœuds si le registre devient trop volumineux pour être téléchargé et stocké par les utilisateurs.

Finalement, la blockchain est une technologie sécurisée dont l'avenir est très prometteur. Il ne faut cependant jamais oublier le principal facteur de risques : le facteur humain.

Tout ce qui est créé hors de la blockchain se doit d'être également sécurisé ! C'est le cas des portefeuilles (support où l'on stocke les clés publiques/privées afin de recevoir ou dépenser des cryptomonnaies). C'est aussi le cas pour les nouveautés (smarts contracts) qui souffrent d'une grande popularité / réussite, sans toujours **réfléchir suffisamment longtemps sur la conception**.

Juliette Bois / Bertrand Passieux

La blockchain à travers ses vulnérabilités de sécurité

UNIVERSITÉ SAVOIE MONT BLANC
SCIENCES ET MONTAGNE
UNIVERSITÉ SAVOIE MONT BLANC