Cadre de référence et méthodologique

Chapitre 1 : Cadre méthodologique

1.1 Présentation des assurances Non-Vie

Le contrat d'assurance est un contrat aléatoire par lequel un organisme dit "l'assureur", qui pour pratiquer l'assurance doit être autorisé par le Ministère des Finances à exercer ce type d'activité, s'engage envers une ou plusieurs personnes déterminées ou un groupe de personnes dites les "assurées", à couvrir, moyennant le paiement d'une somme d'argent dite "prime d'assurance", une catégorie de risques déterminés par le contrat que dans la pratique on appelle "police d'assurance"[2]. Nous avons 2 types de contrat d'assurance qui sont :

- Les assurances vie ;
- Les assurances non-vie ou de dommages ;

Cependant nous allons ici faire la présentation des assurances non-vie qui, regroupent à la fois des assurances de responsabilité (civile familiale, civile du conducteur, etc.) et des assurances de biens (mobilier, dommages causés au véhicule, etc.). Dans le cas d'une souscription à un contrat prévoyant ce type de risques, une indemnisation des dommages est mise en place. L'indemnisation ne peut jamais excéder la valeur des biens endommagés, c'est le principe indemnitaire[3].
En somme nous possédons tous des biens chers à nos yeux : auto, maison, meubles, moto, ordinateur, etc. L'assurance de dommages a un objectif : **les protéger**.
Vol, incendie, accident, dégât d'eau, vol de données, atteinte à la réputation, les sinistres arrivent sans prévenir, bouleversant la vie des gens et des entreprises.
Pour un individu, l'assurance de dommages protège ses biens les plus importants, soit l'habitation et l'automobile.
Pour une entreprise, elle assure la pérennité de ses affaires qui pourraient être affectées de manière catastrophique advenant un sinistre.

[2] *Voir : https://www.dictionnaire-juridique.com/definition/assurance.php*
[3] *Voir : https://www.mapa-assurances.fr/Questions-frequentes/L-assurance/Les-assurances-de-dommages.-qu-est-ce-que-c-est*

1.2 Définition du besoin

En assurance non-vie les professionnels jouent un rôle essentiel en protégeant les biens des assurés et en les aidant à retrouver rapidement une vie normale en cas de sinistre.
De ce fait les contrats d'assurance non-vie aujourd'hui font intervenir plusieurs aspects juridiques, et aussi d'évènements aléatoires qui constituent une réalité, et prennent beaucoup de temps car il faut faire signer les documents et la rédaction du contrat prend énormément de temps. En outre les données des contrats d'assurance sont centralisées, nous avons donc une sécurité aléatoire. Ainsi cette sécurité entraine une perte de confiance des utilisateurs et aussi une perte d'autonomie car nous dépendons des prestataires. La technologie peut apporter la réponse, dans le passé les réseaux étaient centralisés sur une seule source, le réseau que nous avons aujourd'hui est centralisé autour de plusieurs sources mais nous sommes toujours dépendants d'elle, le réseau du futur il s'agit d'une architecture entièrement distribué dans laquelle nous sommes tous acteurs et nœud de ce réseau, cette architecture s'appelle la blockchain.

1.3 Importance de la question

Les données sont centralisées et les processus en matière d'assurance tournent autour du téléphone et des courriers électroniques. De ce fait les données peuvent être exposées à des pertes, ou des fraudes, ou à des attaques qui exploitent les éléments vulnérables du système d'information.

La décentralisation des données en mettant en place une architecture distribuée a pour objectif d'assurer la transparence, la sécurité et ainsi la confiance.

Les attaques, les pertes, et aussi la falsification sont une réalité. Pour en citer quelques-uns nous avons les pertes incendies, catastrophes naturelles, les attaques telles que les virus ou les vers sur le système utilisé par la blockchain.
Les assurances (Absence de classification…), la faiblesse des acteurs humains (naïveté, corruption, inconscience…), sont autant de sources de vulnérabilités.
Il est donc important de se préoccuper de la mise en place d'un processus de stockage et de transmission de données non modifiable c'est-à-dire qui est gravé a vie, et aussi d'un système sans organe de contrôle.

1.4 Formulation des objectifs

Les données sont au centre de l'industrie d'assurance, les administrations des services d'assurance sont confrontées à la croissance exponentielle de la complexité et du volume de données. C'est dans ce cadre qu'on m'a confié comme sujet de mémoire, la conception et réalisation d'un smart contract pour gérer l'assurance non-vie. Il s'agit de mettre en place un système distribué avec la blockchain qui assurera le stockage, la sécurité et de transmission d'informations. L'objectif de notre travail de recherche est de concevoir un smart contract pour gérer les assurances non-vie, avec solidity qui est un langage de programmation orienté objet permettant de décrire les smart contracts, et sont basées sur le principe de la blockchain. A la fin de notre travail, le smart contract réalisé, devrait permettre à chaque personne d'avoir un accès rapide à l'assurance et avec moins de coûts administratifs. Ainsi les services effectués

seront stockés dans la blockchain, ce qui garantira la sécurité, l'autonomie, donc la confiance pourra être obtenu avec garantie.

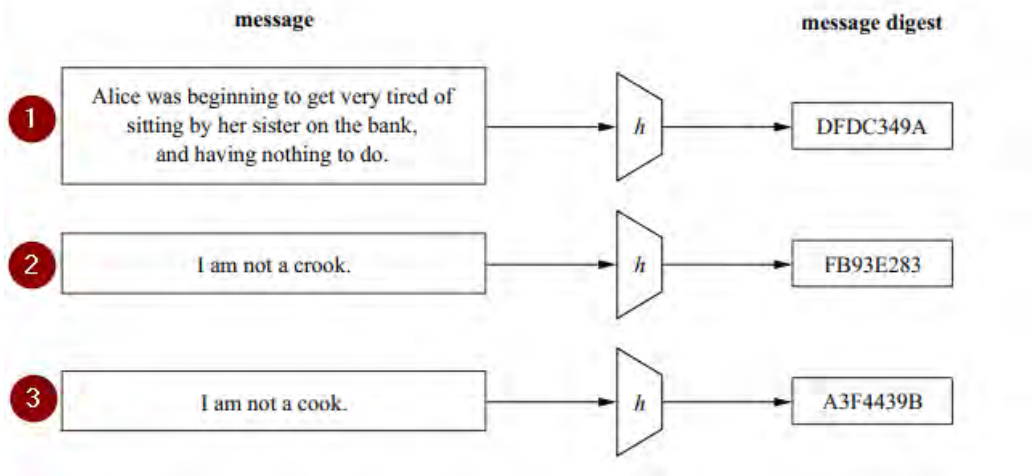
Chapitre 2 : Background

2.1 Architecture de la blockchain

La technologie des blockchain peut sembler complexe, mais elle peut être simplifiée en examinant chaque composant individuellement. À un niveau élevé, la technologie de blockchain fait appel à des mécanismes informatiques bien connus et à des primitives cryptographiques (fonctions de hachage cryptographique, signatures numériques, cryptographie à clé asymétrique) combinées à des concepts de tenue de dossiers (comme les grands livres annexés seulement). Cette section discute de chaque composante principale individuelle: les fonctions de hachage cryptographique, les transactions, la cryptographie à clé asymétrique, les adresses, les grands livres, les blocs, et comment les blocs sont enchaînés ensemble.

2.1.1 Fonctions de Hachage Cryptographique :

Un élément important de la technologie blockchain est l'utilisation de fonctions de hachage cryptographique pour de nombreuses opérations. Le hachage est une méthode d'application d'une fonction de hachage cryptographique aux données, qui calcule une sortie relativement unique (appelé un message digest, ou simplement digest) pour une entrée de presque n'importe quelle taille (par exemple, un dossier, un texte, ou une image). Il permet aux utilisateurs de prendre indépendamment les données d'entrée, de les hacher et d'obtenir le même résultat, ce qui prouve qu'il n'y a pas eu de changement dans les données. Même la plus petite modification apportée à l'entrée (par exemple, la modification d'un seul bit) entraînera un condensé de sortie complètement différent, comme indiqué dans la figure 1.



Comme vous remarquez sur figure ci-dessus, au niveau du 2 et 3 ont le même message d'entrée mais le hachage en sortie est différent, ceci est du car au niveau de la fonction de hachage 3 on a ajouté un nonce (un nombre entier utiliser une et une seule fois) au message.

Figure 1 Comportement principal entrée-sortie des fonctions de hachage [4]

Même si les fonctions de hachage ont de nombreuses applications dans la cryptographie moderne, elles sont peut-être mieux connues pour le rôle important qu'elles jouent dans l'utilisation pratique des signatures numériques.

Les fonctions de hachage cryptographique possèdent ces importantes propriétés de sécurité:

- elles sont résistantes à la pré-image. Cela signifie qu'ils sont à sens unique; il est impossible de calculer la valeur d'entrée correcte compte tenu d'une certaine valeur de sortie (par exemple, étant donné un résumé, trouver x tel que hash (x) = digest) ;

- elles sont résistantes à la deuxième pré-image, ce qui signifie que l'on ne peut pas trouver une entrée hachée sur une sortie spécifique. Plus spécifiquement, les fonctions de hachage cryptographiques sont conçues de sorte que, étant donné une entrée spécifique, il est impossible de trouver une deuxième entrée qui produise la même sortie (par exemple, étant donné x, trouver y tel que hash (x) = hash (y)). La seule approche disponible consiste à rechercher de manière exhaustive l'espace d'entrée, mais cela est impossible à faire sur le plan des calculs avec toute chance de succès ;

- elles sont résistantes aux collisions. Cela signifie que l'on ne peut pas trouver deux entrées hachées vers la même sortie. Plus précisément, il est impossible sur le plan informatique de trouver deux entrées qui produisent le même condensé (par exemple, trouver un x et un y avec hash (x) = hash (y)) ;

La fonction de hachage cryptographique spécifique utilisée dans de nombreuses implémentations de blockchain est L'algorithme de hachage sécurisé (SHA) avec une taille de sortie de 256 bits (SHA-256). De nombreux ordinateurs prennent en charge cet algorithme en matériel, ce qui le rend rapide à calculer. SHA-256 a une sortie de 32 octets (1 octet = 8 bits, 32 octets = 256 bits), généralement affichée comme une chaîne hexadécimale de 64 caractères (Voir tableau 1 ci-dessous))

Input text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World !	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Tableau 1 Exemples de texte d'entrée et de valeurs de synthèse SHA-256 correspondantes

Puisqu'il existe un nombre infini de valeurs d'entrée possibles et un nombre fini de valeurs de résumé de sortie possibles, il est possible, mais très peu probable, d'avoir une collision où hash

[4] *Christof PAAR, Jan PELZL, Understanding cryptography*

(x) = hash (y) (c'est-à-dire que le hachage de deux entrées différentes produit le même condensé). SHA-256 est censé être résistant aux collisions, car pour trouver une collision dans SHA-256, il faudrait exécuter l'algorithme, en moyenne, environ 2^{128} fois (ce qui représente 340 milliards, ou plus précisément 340 282 366 920 938 463 463 374 607 431 738 211 456; environ 3 402 x10^{38}).

Pour mettre cela en perspective, le taux de hachage (hachages par seconde) de l'ensemble du réseau Bitcoin en 2015 était de 300 quadrillions de hachages par seconde (300 000 000 000 000 000 000 / s)[5]. À ce rythme, il faudrait à l'ensemble du réseau Bitcoin environ 35 942 991 748 521 (environ 3,6 x10^{13}) ans[6] pour fabriquer une collision (notez que l'univers est estimé à 1,37 x 10^{10} ans)[7]. Même si une telle entrée x et y produisant le même résumé, il serait également très peu probable que les deux entrées soient valides dans le contexte du réseau de blockchain (c'est-à-dire que x et y sont tous deux des transactions valides).

Au sein d'un réseau blockchain, les fonctions de hachage cryptographiques sont utilisées pour de nombreuses tâches, telles que:

- Dérivation d'adresse que nous allons voir dans la section 1.4 ;
- Créer des identifiants uniques ;
- Sécuriser les données de bloc - un nœud de publication hachera les données de bloc, créant un résumé qui seront stockés dans l'en-tête du bloc ;
- Sécuriser l'en-tête de bloc un nœud de publication hachera l'en-tête de bloc. Si le réseau de chaînes de blocs utilise un modèle de consensus de preuve de travail (voir section 2), le nœud de publication devra hacher l'en-tête de bloc avec différentes valeurs de nonce (voir le paragraphe 1.1) jusqu'à ce que les conditions requises soient remplies. Le condensé de hachage de l'en-tête du bloc actuel sera inclus dans l'en-tête du prochain bloc, où il sécurisera les données de l'en-tête du bloc actuel ;

Étant donné que l'en-tête de bloc comprend une représentation hachée des données de bloc, les données de bloc sont également sécurisées lorsque le résumé de l'en-tête de bloc est stocké dans le bloc suivant.

Il existe de nombreuses familles de fonctions de hachage cryptographiques utilisées dans la technologie de blockchain (SHA-256 n'est pas le seul), comme Keccak (sélectionné par le NIST comme le gagnant d'un concours visant à créer le standard de hachage SHA-3[8]).

[5] *https://en.bitcoin.it/wiki/Hash_per_second*
[6] *https://www.wolframalpha.com/input/?i=2%5E128%2F%28300000000000000000+*+60+*+60+*+24+*+365.25%29*
[7] *https://map.gsfc.nasa.gov/universe/uni_age.html*
[8] *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf*

2.1.1.1 Cryptographie Nonce :

Un nonce cryptographique est un nombre arbitraire utilisé une seule fois. Un nonce cryptographique peut être combiné avec des données pour produire différents digests de hachage par nonce:

Hash (data + nonce) = digest

Seule la modification de la valeur nonce fournit un mécanisme permettant d'obtenir différentes valeurs de résumé tout en conservant les mêmes données. Cette technique est utilisée dans le modèle de consensus de preuve de travail (voir section 2.1).

2.1.2 Transaction :

Une transaction représente une interaction entre les parties. Avec les crypto-monnaies, par exemple, une transaction représente un transfert de la crypto-monnaie entre utilisateurs du réseau blockchain. Pour les scénarios d'entreprise à entreprise, une transaction peut être un moyen d'enregistrer des activités se produisant sur des actifs numériques ou physiques. La figure 5 montre un exemple théorique d'une transaction crypto-monnaie. Chaque bloc d'une blockchain peut contenir zéro transaction ou plus. Pour certaines implémentations de blockchain, un approvisionnement constant de nouveaux blocs (même sans transaction) est essentiel pour maintenir la sécurité du réseau de blockchain; en publiant en permanence de nouveaux blocs, cela empêche les utilisateurs malveillants de "rattraper" et de fabriquer une blockchain modifiée plus longue (voir section 2.7).

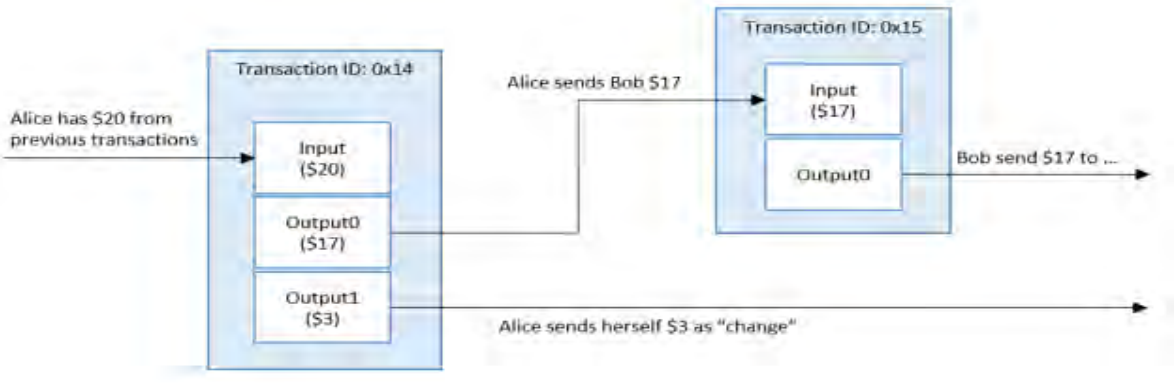


Figure 2 Exemple de transaction crypto-monnaie

Les données qui composent une transaction peuvent être différentes pour chaque implémentation de la blockchain, mais le mécanisme de transaction est en grande partie le même. Un utilisateur du réseau blockchain envoie des informations au réseau blockchain. Les informations envoyées peuvent inclure l'adresse de l'expéditeur (ou un autre identifiant pertinent), la clé publique de l'expéditeur, une signature numérique, des entrées de transaction et des sorties de transaction.

Une transaction de crypto-monnaie unique nécessite généralement au moins les informations suivantes, mais peut en contenir davantage:

- **Inputs** - Les entrées sont généralement une liste des actifs numériques à transférer. Une transaction référencera la source de l'actif numérique (fournissant la provenance), soit la transaction précédente où elle avait été transmise à l'expéditeur, soit, dans le cas de nouveaux actifs numériques, l'événement d'origine. L'entrée dans la transaction étant une référence à des événements passés, les actifs numériques ne changent pas. Dans le cas des crypto-monnaies, cela signifie que la valeur ne peut pas être ajoutée ou retirée des actifs numériques existants ;
  Au lieu de cela, un actif numérique unique peut être divisé en plusieurs nouveaux actifs numériques (chacun ayant une valeur moindre) ou plusieurs actifs numériques peuvent être combinés pour former moins de nouveaux actifs numériques (avec une valeur correspondante supérieure). Le fractionnement ou la jonction d'actifs sera spécifié dans la sortie de la transaction.
  L'expéditeur doit également fournir la preuve qu'il a accès aux entrées référencées, généralement en signant numériquement la transaction - prouvant l'accès à la clé privée ;

- **Outputs** - Les sorties sont généralement les comptes qui seront les destinataires des actifs numériques, ainsi que le montant des actifs numériques qu'ils recevront. Chaque sortie spécifie le nombre d'actifs numériques à transférer au (x) nouveau (s) propriétaire (s), l'identifiant du ou des nouveaux propriétaires et un ensemble de conditions que les nouveaux propriétaires doivent remplir pour dépenser cette valeur. Si les ressources numériques fournies sont supérieures aux besoins, les fonds supplémentaires doivent être explicitement renvoyés à l'expéditeur (il s'agit d'un mécanisme permettant de «rendre la modification») ;

Principalement utilisées pour transférer des actifs numériques, les transactions peuvent plus généralement être utilisées pour transférer des données. Dans un cas simple, une personne peut simplement vouloir publier de manière permanente et publique des données sur la blockchain. Dans le cas de systèmes de smart contract, les transactions peuvent être utilisées pour envoyer des données, les traiter et stocker certains résultats dans la blockchain. Par exemple, une transaction peut être utilisée pour modifier un attribut d'un actif numérisé, tel que l'emplacement d'une expédition dans un système de chaîne logistique basé sur la technologie blockchain.

Quelle que soit la manière dont les données sont formées et traitées, il est important de déterminer la validité et l'authenticité d'une transaction. La validité d'une transaction garantit que celle-ci répond aux exigences du protocole et à tous les formats de données formalisés ou aux exigences du contrat intelligent spécifiques à la mise en œuvre de la blockchain. L'authenticité d'une transaction est également importante, car elle détermine que l'expéditeur d'actifs numériques a accès à ces actifs numériques. Les transactions sont généralement signées numériquement par la clé privée de l'expéditeur (la cryptographie à clé asymétrique est brièvement décrite à la section 1.3) et peuvent être vérifiées à tout moment à l'aide de la clé publique associée.

2.1.3 Cryptographie à clé asymétrique :

La technologie Blockchain utilise la cryptographie à clé asymétrique[9] (également appelée cryptographie à clé publique). La cryptographie à clé asymétrique utilise une paire de clés: une clé publique et une clé privée qui sont liées mathématiquement. La clé publique est rendue publique sans réduire la sécurité du processus, mais la clé privée doit rester secrète pour que les données conservent leur protection cryptographique. Même s'il existe une relation entre les deux clés, la clé privée ne peut pas être déterminée efficacement en fonction de la connaissance de la clé publique. On peut signer avec une clé privée, puis déchiffrer avec la clé publique. Alternativement, on peut chiffrer avec une clé publique, puis déchiffrer avec une clé privée.

La cryptographie à clé asymétrique permet d'établir une relation de confiance entre les utilisateurs qui ne se connaissent pas ou ne se font pas confiance, en fournissant un mécanisme permettant de vérifier l'intégrité et l'authenticité des transactions tout en permettant aux transactions de rester publiques. Pour ce faire, les transactions sont «signées numériquement». Cela signifie qu'une clé privée est utilisée pour chiffrer une transaction de sorte que toute personne possédant la clé publique puisse la déchiffrer. Puisque la clé publique est librement disponible, le cryptage de la transaction avec la clé privée prouve que le signataire de la transaction a accès à la clé privée. Vous pouvez également chiffrer les données avec la clé publique d'un utilisateur, de sorte que seuls les utilisateurs ayant accès à la clé privée puissent la déchiffrer. Un inconvénient est que la cryptographie à clé asymétrique est souvent lente à calculer.

Cela contraste avec la cryptographie à clé symétrique[10] dans laquelle une seule clé secrète est utilisée pour crypter et décrypter. Avec la cryptographie à clé symétrique, les utilisateurs doivent déjà avoir une relation de confiance établie entre eux pour échanger la clé pré-partagée. Dans un système symétrique, toute donnée chiffrée pouvant être déchiffrée avec la clé pré-partagée confirme qu'elle a été envoyée par un autre utilisateur ayant accès à la clé pré-partagée; aucun utilisateur sans accès à la clé pré-partagée ne pourra voir les données déchiffrées. Par rapport à la cryptographie à clé asymétrique, la cryptographie à clé symétrique est très rapide à calculer. Pour cette raison, lorsque l'on prétend chiffrer quelque chose en utilisant la cryptographie à clé asymétrique, les données sont souvent chiffrées avec une cryptographie à clé symétrique, puis la clé symétrique est chiffrée à l'aide de la cryptographie à clé asymétrique. Cette «astuce» peut considérablement accélérer la cryptographie à clé asymétrique.

Voici un résumé de l'utilisation de la cryptographie à clé asymétrique dans de nombreux réseaux blockchain:

---

[9] *FIPS Publication 186-4, Digital Signature Standard specifies a common algorithm for digital signing used in blockchain technologies: Elliptic Curve Digital Signature Algorithm (ECDSA). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf*

[10] *Voir The Advanced Encryption Standard voir: Christof PAAR, Jan PELZL, Understanding cryptography*

• Les clés privées sont utilisées pour signer numériquement les transactions ;

• Les clés publiques sont utilisées pour dériver des adresses ;

• Les clés publiques permettent de vérifier les signatures générées avec des clés privées ;

• La cryptographie à clé asymétrique permet de vérifier que l'utilisateur qui transfère de la valeur à un autre utilisateur est en possession de la clé privée capable de signer la transaction ;

Certains réseaux de blockchain autorisés peuvent exploiter l'infrastructure de clé publique existante d'une entreprise pour la cryptographie à clé asymétrique afin de fournir des informations d'identification d'utilisateur au lieu de laisser chaque utilisateur du réseau de blockchain accéder à ses propres clés asymétriques. Cela se fait en utilisant les services de répertoire existants et en utilisant ces informations dans le réseau blockchain.

Certains réseaux blockchain autorisés peuvent exploiter l'infrastructure de clé publique existante d'une entreprise pour la cryptographie à clé asymétrique afin de fournir les informations d'identification de l'utilisateur - plutôt que de demander à chaque utilisateur du réseau blockchain de gérer ses propres clés asymétriques. Cela se fait en utilisant les services d'annuaire existants et en utilisant ces informations au sein du réseau blockchain. Les réseaux de chaînes de blocs qui utilisent un service d'annuaire existant peuvent y accéder via des protocoles existants, tels que le protocole LDAP (Lightweight Directory Access Protocol)[11], et utiliser les informations de l'annuaire en mode natif, ou les importer dans une autorité de certification interne au sein du réseau de chaînes de blocs

2.1.4 Adresses et dérivation d'adresses :

Certains réseaux blockchain utilisent une adresse, qui est une courte chaîne alphanumérique de caractères dérivée de la clé publique de l'utilisateur du réseau blockchain à l'aide d'une fonction de hachage cryptographique, ainsi que des données supplémentaires (numéro de version, sommes de contrôle, par exemple). La plupart des implémentations blockchain utilisent des adresses en tant que points d'extrémité "à" et "à partir de" d'une transaction. Les adresses sont plus courtes que les clés publiques et ne sont pas secrètes. Une méthode pour générer une adresse consiste à créer une clé publique en y appliquant une fonction de hachage cryptographique et en convertissant le hachage en texte:

Public key → cryptographic hash function → address

Chaque mise en œuvre de la blockchain peut mettre en œuvre un procédé différent pour dériver une adresse. Pour les réseaux blockchain sans permission, qui permettent la création anonyme de comptes, un utilisateur du réseau blockchain peut générer autant de paires de clés asymétriques, et donc d'adresses, qu'il le souhaite, permettant un degré variable de pseudo-anonymat. Les adresses peuvent servir d'identifiant public dans un réseau de chaînes de blocs pour un utilisateur. Souvent, une adresse est convertie en un QR code (code de réponse rapide,

[11] *https://ldap.com/*

code à barres bidimensionnel pouvant contenir des données arbitraires) pour une utilisation plus facile avec les téléphones mobiles.

Les utilisateurs du réseau blockchain peuvent ne pas être la seule source d'adresses dans les réseaux blockchain. Il est nécessaire de fournir une méthode permettant d'accéder à un contrat intelligent une fois qu'il a été déployé au sein d'un réseau blockchain. Pour Ethereum, les contrats intelligents sont accessibles via une adresse spéciale appelée compte de contrat. Cette adresse de compte est créée lors du déploiement d'un contrat intelligent (l'adresse d'un compte de contrat est calculée de manière déterministe à partir de l'adresse du créateur du contrat intelligent). Ce compte de contrat permet d'exécuter le contrat lorsqu'il reçoit une transaction, ainsi que de créer des contrats intelligents supplémentaires à son tour.

➢ Stockage de clé privée

Avec certains réseaux blockchain (en particulier avec les réseaux blockchain sans autorisation), les utilisateurs doivent gérer et stocker en toute sécurité leurs propres clés privées. Au lieu de les enregistrer manuellement, ils utilisent souvent un logiciel pour les stocker en toute sécurité. Ce logiciel est souvent appelé un portefeuille. Le portefeuille peut stocker des clés privées, des clés publiques et les adresses associées. Il peut également exécuter d'autres fonctions, telles que le calcul du nombre total de ressources numériques qu'un utilisateur peut posséder.

Si un utilisateur perd une clé privée, tous les actifs numériques associés à cette clé sont perdus, car il est impossible en termes de calcul de régénérer la même clé privée. Si une clé privée est volée, l'attaquant aura un accès complet à tous les actifs numériques contrôlés par cette clé privée. La sécurité des clés privées est si importante que de nombreux utilisateurs utilisent un matériel sécurisé spécial pour les stocker ; sinon, les utilisateurs peuvent tirer parti d'une industrie émergente de services de dépôt fiduciaire à clé privée.

Ces services d'en tiercement de clé peuvent également satisfaire aux lois de KYC[12] en plus de stocker des clés privées car les utilisateurs doivent fournir une preuve de leur identité lors de la création d'un compte.

Le stockage de clés privées est un aspect extrêmement important de la technologie blockchain. Quand il est rapporté dans les nouvelles que «la crypto-monnaie XYZ a été volée…», cela signifie certainement que des clés privées ont été trouvées et utilisées pour signer une transaction envoyant de l'argent à un nouveau compte, pas que le réseau de blockchain ait été compromis. Notez que, comme les données de blockchain ne peuvent généralement pas être modifiées, une fois qu'un criminel a volé une clé privée et transféré publiquement les fonds associés à un autre compte, cette transaction ne peut généralement pas être annulée.

Cependant on peut aussi stocker les clés publique avec PKCS#12 (.pfx ou.p12) et.jks* (créés par l'outil Java) sont des fichiers qui contiennent votre paire de clés publiques/privées. Contrairement aux magasins de clés des systèmes d'exploitation et des navigateurs stockés en local, ces fichiers peuvent être stockés pratiquement n'importe où, y compris sur des serveurs distants ; ils sont toujours protégés par un mot de passe (ainsi, chaque fois que vous voulez

[12] *https://www.capfi.fr/blog/it-finance/kyc-know-your-customer*

utiliser votre clé privée, vous devez saisir un mot de passe FORT). Autre avantage : comme il ne s'agit en définitive que de fichiers, vous pouvez facilement en distribuer des copies si plusieurs personnes ont besoin d'utiliser le certificat. Mais justement, comme il ne s'agit que de fichiers, ils risquent d'être distribués de manière non sécurisée. Au vu des rapides progrès des algorithmes utilisés pour craquer les mots de passe, pensez à créer un mot de passe suffisamment long et aléatoire si vous utilisez cette méthode.

2.1.5 Grands livres :

Un grand livre est un ensemble de transactions. Tout au long de l'histoire, les registres à stylos et à papier ont été utilisés pour suivre les échanges de biens et de services. À l'époque moderne, les grands livres ont été stockés sous forme numérique, souvent dans de grandes bases de données appartenant à une tierce partie de confiance centralisée (c'est-à-dire le propriétaire du grand livre) et gérées par elle pour le compte d'une communauté d'utilisateurs. Ces grands livres avec une propriété centralisée peuvent être implémentés de manière centralisée ou distribuée (c'est-à-dire un seul serveur ou un cluster de serveurs de coordination).

Il est de plus en plus intéressant d'explorer la possibilité de répartir la propriété du grand livre. La technologie Blockchain permet une telle approche utilisant à la fois une propriété distribuée et une architecture physique distribuée. L'architecture physique distribuée des réseaux blockchain implique souvent un ensemble d'ordinateurs beaucoup plus grand que celui typique d'une architecture physique distribuée gérée de manière centralisée. L'intérêt croissant pour la propriété distribuée des grands livres est dû aux problèmes de confiance, de sécurité et de fiabilité possibles liés aux grands livres avec propriété centralisée:

- Les grands livres appartenant à l'organisme central peuvent être perdus ou détruits; un utilisateur doit avoir la certitude que le propriétaire sauvegarde correctement le système ;
    - Un réseau de chaînes de blocs est distribué par conception, créant ainsi de nombreuses copies de sauvegarde, mises à jour et synchronisées avec les mêmes données de grand livre entre homologues. Un avantage clé de la technologie blockchain est que chaque utilisateur peut conserver sa propre copie du grand livre. Chaque fois que de nouveaux nœuds complets rejoignent le réseau de chaînes de blocs, ils vont découvrir d'autres nœuds complets et demandent une copie complète du journal du réseau, ce qui rend difficile la perte ou la destruction du registre. Remarque: certaines implémentations de la blockchain permettent de prendre en charge des concepts tels que les transactions privées ou les canaux privés. Les transactions privées facilitent la transmission d'informations uniquement aux nœuds participant à une transaction et non à l'ensemble du réseau ;
- Les grands livres appartenant à un centre peuvent se trouver sur un réseau homogène, où tous les logiciels, le matériel et l'infrastructure réseau peuvent être identiques. En

raison de cette caractéristique, la résilience globale du système peut être réduite car une attaque sur une partie du réseau fonctionnera partout ;

  - Un réseau blockchain est un réseau hétérogène où le logiciel, le matériel et l'infrastructure réseau sont tous différents. En raison des nombreuses différences entre les nœuds du réseau de chaînes de blocs, il n'est pas garanti qu'une attaque sur un nœud fonctionne sur d'autres nœuds ;

- Les grands livres appartenant à des centrales peuvent être situés entièrement dans des zones géographiques spécifiques (par exemple, tous dans un pays). Si des pannes de réseau se produisaient à cet emplacement, le grand livre et les services qui en dépendent pourraient ne pas être disponibles ;

  - Un réseau blockchain peut être composé de nœuds géographiquement divers pouvant être trouvés dans le monde entier. De ce fait, et le réseau de chaînes de blocs fonctionnant entre homologues, il résiste à la perte de tout nœud, voire de toute une région de nœuds ;

- Les transactions sur un grand livre appartenant à l'administration centrale ne sont pas effectuées de manière transparente et peuvent ne pas être valides; un utilisateur doit avoir la certitude que le propriétaire valide chaque transaction reçue ;
  - Un réseau de blockchain doit vérifier que toutes les transactions sont valides; si un nœud malveillant transmettait des transactions non valides, d'autres les détecteraient et les ignoreraient, empêchant ainsi les transactions non valides de se propager à travers le réseau de la blockchain ;
- La liste des transactions sur un grand livre appartenant à l'administration centrale peut ne pas être complète; un utilisateur doit avoir la certitude que le propriétaire inclut toutes les transactions valides reçues ;
  - Un réseau de blockchain contient toutes les transactions acceptées dans son grand livre distribué. Pour construire un nouveau bloc, il est nécessaire de faire référence à un bloc précédent - construisant par conséquent dessus. Si un nœud de publication n'incluait pas de référence au dernier bloc, les autres nœuds le rejetteraient ;
- Les données de transaction sur un grand livre appartenant à la centrale peuvent avoir été modifiées; un utilisateur doit avoir la certitude que le propriétaire ne modifie pas les transactions passées ;
  - Un réseau blockchain utilise des mécanismes cryptographiques tels que des signatures numériques et des fonctions de hachage cryptographique pour fournir des grands livres inviolables et résistants à la fraude ;
- Le système centralisé peut ne pas être sécurisé; un utilisateur doit avoir la certitude que les systèmes informatiques et les réseaux associés reçoivent des correctifs de sécurité critiques et a mis en œuvre les meilleures pratiques en matière de sécurité. Une violation du système et des informations personnelles peuvent avoir été volées en raison d'insécurités ;
  - Un réseau de blockchain, en raison de sa nature distribuée, ne fournit aucun point d'attaque centralisé. En règle générale, les informations sur un réseau de chaînes de blocs sont visibles publiquement et ne proposent rien à voler. Pour attaquer les utilisateurs du réseau blockchain, un

attaquant devrait les cibler individuellement. Le ciblage de la blockchain elle-même rencontrerait la résistance des nœuds honnêtes présents dans le système. Si un nœud individuel n'était pas corrigé, cela n'affecterait que ce nœud, et non le système dans son ensemble ;

2.1.6 Blocs :

Les utilisateurs du réseau de blockchain soumettent des transactions de candidats au réseau de blockchain via un logiciel (applications de bureau, applications pour smartphones, portefeuilles numériques, services Web, etc.). Le logiciel envoie ces transactions à un ou plusieurs nœuds du réseau de chaînes de blocs. Les nœuds choisis peuvent être des nœuds complets non publiés ainsi que des nœuds de publication. Les transactions soumises sont ensuite propagées aux autres nœuds du réseau, mais cela en soi ne place pas la transaction dans la chaîne de blocs. Pour de nombreuses implémentations de la blockchain, une fois qu'une transaction en attente a été distribuée aux nœuds, elle doit attendre dans une file d'attente jusqu'à ce qu'elle soit ajoutée à la blockchain par un nœud de publication.

Les transactions sont ajoutées à la blockchain lorsqu'un nœud de publication publie un bloc. Un bloc contient un en-tête de bloc et des données de bloc. L'en-tête de bloc contient des métadonnées pour ce bloc. Les données de bloc contiennent une liste de transactions validées et authentiques qui ont été soumises au réseau de chaînes de blocs. La validité et l'authenticité sont assurées en vérifiant que la transaction est correctement formatée et que les fournisseurs d'actifs numériques dans chaque transaction (répertoriés dans les valeurs de «saisie» de la transaction) ont chacun signé la transaction de manière cryptographique. Cela permet de vérifier que les fournisseurs d'actifs numériques pour une transaction avaient accès à la clé privée qui pouvait signer les actifs numériques disponibles. Les autres nœuds complets vérifieront la validité et l'authenticité de toutes les transactions d'un bloc publié et n'accepteront pas un bloc s'il contient des transactions non valides.

Il convient de noter que chaque implémentation blockchain peut définir ses propres champs de données. Cependant, de nombreuses implémentations blockchain utilisent des champs de données tels que:

- En-tête de bloc
    - Le numéro de bloc, également appelé hauteur de bloc dans certains réseaux de chaînes de blocs ;
    - La valeur de hachage de l'en-tête du bloc précédent ;
    - Une représentation en hachage des données de bloc (différentes méthodes peuvent être utilisées pour y parvenir, telles que la génération d'un arbre de Merkle[13] (Figure 10) et le stockage du hachage racine ou en utilisant un hachage de toutes les données de bloc combinées) ;
    - Un horodatage ;

[13] *Une structure de données dans laquelle les données sont hachées et combinées jusqu'à ce qu'il y ait un hachage racine unique qui représente la structure entière.*

- La taille du bloc ;
- La valeur de nonce. Pour les réseaux blockchain utilisant l'extraction, il s'agit d'un numéro manipulé par le nœud de publication pour résoudre le casse-tête (voir la section 2.1 pour plus de détails). D'autres réseaux de chaînes de blocs peuvent ou non l'inclure ou l'utiliser à d'autres fins que la résolution d'un casse-tête ;

- Données de bloc
  - Une liste des transactions et des événements du grand livre inclus dans le bloc ;
  - D'autres données peuvent être présentes ;

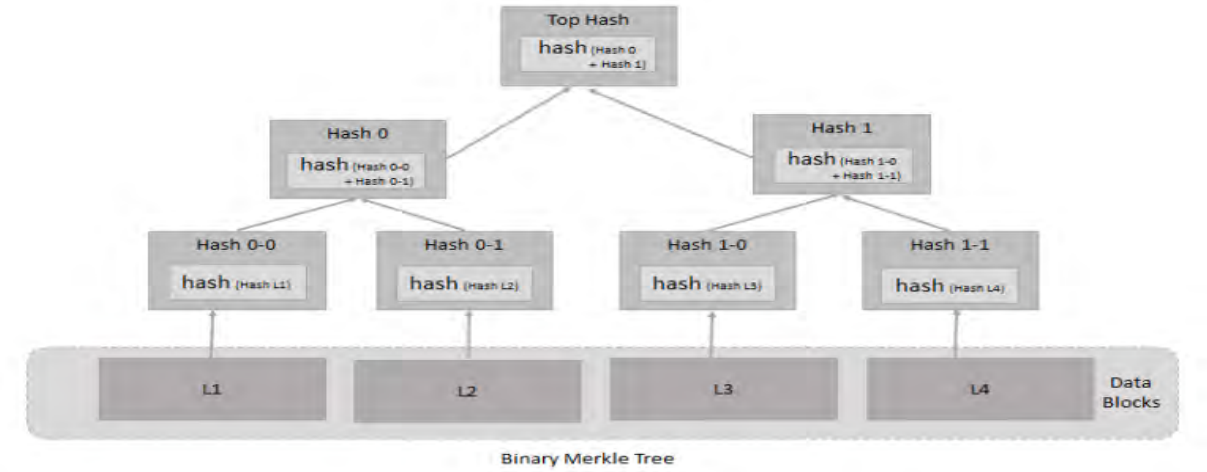


Figure 3 Arbre de Merkle binaire

2.1.7 Chaînage de blocs :

Les blocs sont enchaînés à travers chaque bloc contenant le condensé de hachage de l'en-tête du bloc précédent, formant ainsi la blockchain. Si un bloc précédemment publié était modifié, le hachage serait différent. Cela entraînerait à son tour un hachage différent dans tous les blocs suivants, car il comprend celui du bloc précédent. Cela permet de détecter et de rejeter facilement les blocs altérés. La figure 3 montre une chaîne générique de blocs

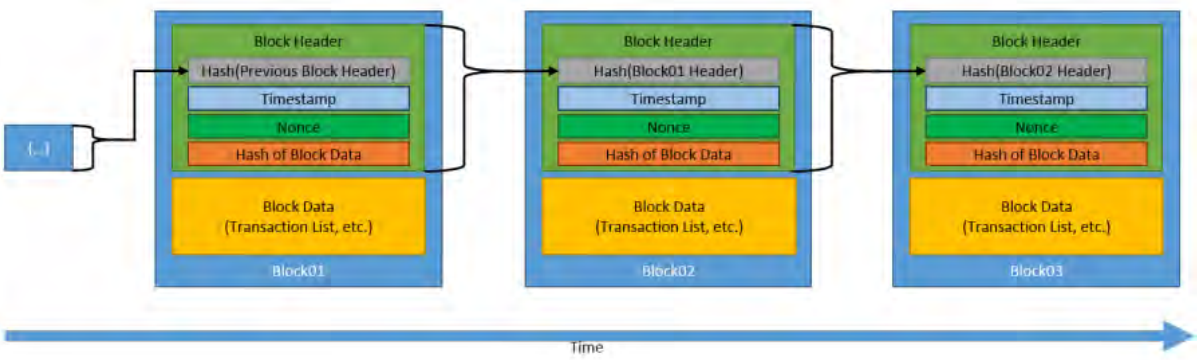


Figure 4 Chaîne générique de blocs

2.2 Consensus

Un aspect clé de la technologie de blockchain consiste à déterminer quel utilisateur publie le prochain bloc. Ce problème est résolu par la mise en œuvre de l'un des nombreux modèles de consensus possibles. Pour les réseaux de blockchain sans permission, il existe généralement de nombreux nœuds de publication en concurrence simultanée pour publier le bloc suivant. Ils le font généralement pour gagner des frais de crypto-monnaie et / ou de transaction. Ce sont généralement des utilisateurs qui se méfient mutuellement et qui ne peuvent se connaître que par leurs adresses publiques. Chaque nœud de publication est probablement motivé par un désir de gain financier et non par le bien-être des autres nœuds de publication ou même du réseau lui-même.
Dans une telle situation, pourquoi un utilisateur propagerait-il un bloc qu'un autre utilisateur tente de publier? En outre, qui résout les conflits lorsque plusieurs nœuds publient un bloc à peu près au même moment? Pour que cela fonctionne, les technologies de blockchain utilisent des modèles consensuels pour permettre à un groupe d'utilisateurs se méfiant mutuellement de travailler ensemble.
Lorsqu'un utilisateur rejoint un réseau de blockchain, il accepte l'état initial du système. Ceci est enregistré dans le seul bloc préconfiguré, le bloc de genèse. Chaque réseau de blockchain à un bloc de genèse publié et chaque bloc doit être ajouté à la blockchain après celui-ci, sur la base du modèle de consensus convenu. Cependant, quel que soit le modèle, chaque bloc doit être valide et peut donc être validé indépendamment par chaque utilisateur du réseau de la blockchain. En combinant l'état initial et la possibilité de vérifier chaque bloc depuis lors, les utilisateurs peuvent s'accorder indépendamment sur l'état actuel de la blockchain. Notez que si deux chaînes valides ont déjà été présentées à un nœud complet, le mécanisme par défaut dans la plupart des réseaux de blockchain est que la chaîne "la plus longue" est considérée comme la chaîne correcte et sera adoptée. C'est parce qu'il a eu le plus de travail mis dedans. Cela se produit fréquemment avec certains modèles consensuels et sera discuté en détail.

Les propriétés suivantes sont alors en place:

- L'état initial du système est convenu (par exemple, le bloc de genèse) ;
- Les utilisateurs acceptent le modèle de consensus selon lequel des blocs sont ajoutés au système ;
- Chaque bloc est lié au bloc précédent en incluant le condensé de hachage de l'en-tête du bloc précédent (à l'exception du premier bloc «genèse», qui n'a pas de bloc précédent et pour lequel le hachage de l'en-tête du bloc précédent est généralement mis à zéro) ;
- Les utilisateurs peuvent vérifier chaque bloc indépendamment ;

En pratique, le logiciel gère tout et les utilisateurs n'ont pas besoin de connaître ces détails.
Une caractéristique clé de la technologie blockchain est qu'il n'est pas nécessaire de faire appel à un tiers de confiance pour fournir l'état du système: chaque utilisateur du système peut vérifier l'intégrité du système. Pour ajouter un nouveau bloc à la blockchain, tous les nœuds doivent parvenir à un accord commun dans le temps. Toutefois, un certain désaccord temporaire est autorisé. Pour les réseaux de blockchain sans permission, le modèle de consensus doit fonctionner même en présence éventuellement d'utilisateurs malveillants, ces derniers pouvant tenter de perturber ou de prendre en charge la chaîne de blocs.

Notez que pour les réseaux de blockchain autorisés, des recours légaux peuvent être utilisés si un utilisateur agit par malveillance.
Dans certains réseaux blockchain, tels que ceux autorisés, il peut exister un certain niveau de confiance entre les nœuds de publication. Dans ce cas, il n'est peut-être pas nécessaire de disposer d'un modèle de consensus utilisant beaucoup de ressources (temps de calcul, investissement, etc.) pour déterminer quel participant ajoute le bloc suivant à la chaîne. En règle générale, à mesure que le niveau de confiance augmente, la nécessité d'utiliser des ressources pour mesurer la confiance créée diminue. Pour certaines implémentations blockchain autorisées, la vision du consensus va au-delà de la garantie de la validité et de l'authenticité des blocs, mais englobe tous les systèmes de contrôles et de validations allant de la proposition d'une transaction à son inclusion finale dans un bloc.

Dans les sections suivantes, plusieurs modèles de consensus ainsi que l'approche de résolution de conflit la plus courante sont abordés.

2.2.1 Modèle de consensus sur la preuve de travail :

Dans le modèle de preuve de travail, un utilisateur publie le bloc suivant en étant le premier à résoudre un puzzle informatique intensif. La solution à ce puzzle est la "preuve" qu'ils ont effectué un travail. Le puzzle est conçu de telle sorte que sa résolution est difficile, mais il est facile de vérifier qu'une solution est valide. Cela permet à tous les autres nœuds complets de valider facilement les blocs suivants proposés, et tout bloc proposé ne satisfaisant pas le casse-tête serait rejeté.

Une méthode de puzzle courante consiste à exiger que le condensé de hachage d'un en-tête de bloc soit inférieur à une valeur cible. Les nœuds de publication apportent de nombreuses modifications mineures à leur en-tête de bloc (modification du nonce, par exemple) en essayant de trouver un condensé de hachage répondant à l'exigence. Pour chaque tentative, le nœud de publication doit calculer le hachage pour l'en-tête de bloc complet. Le hachage de l'en-tête de bloc à plusieurs reprises devient un processus de calcul intensif. La valeur cible peut être modifiée au fil du temps pour ajuster la difficulté (à la hausse ou à la baisse) afin d'influer sur la fréquence de publication des blocs.

Par exemple, Bitcoin, qui utilise le modèle de preuve de travail, ajuste la difficulté du puzzle tous les blocs 2016 pour que le taux de publication des blocs soit d'environ une fois toutes les dix minutes. L'ajustement est effectué en fonction du niveau de difficulté du puzzle et augmente ou diminue le nombre de zéros au début. En augmentant le nombre de zéros non significatifs, la difficulté du puzzle augmente, car toute solution doit être inférieure au niveau de difficulté, ce qui signifie que les solutions possibles sont moins nombreuses. En diminuant le nombre de zéros non significatifs, le niveau de difficulté diminue, car il existe plus de solutions possibles. Cet ajustement a pour but de maintenir la difficulté de calcul du puzzle et, par conséquent, de préserver le mécanisme de sécurité central du réseau Bitcoin. La puissance de calcul disponible augmente avec le temps, tout comme le nombre de nœuds de publication. La difficulté du puzzle augmente donc généralement.

Les ajustements apportés à l'objectif de difficulté visent à garantir qu'aucune entité ne puisse prendre en charge la production de blocs, mais les calculs de résolution de casse-tête nécessitent par conséquent une consommation de ressources importante.

En raison de la consommation importante de ressources de certains réseaux de blockchain de preuve de travail, on souhaite ajouter des nœuds de publication aux régions où il existe un excédent d'approvisionnement en électricité bon marché.

Un aspect important de ce modèle est que le travail inséré dans une énigme n'influence pas les chances de résolution des énigmes actuelles ou futures, car les énigmes sont indépendantes. Cela signifie que lorsqu'un utilisateur reçoit un bloc terminé et valide d'un autre utilisateur, il est incité à abandonner son travail actuel et à commencer à créer le bloc nouvellement reçu, car il sait que les autres nœuds de publication le construiront.

A titre d'exemple, considérons un puzzle dans lequel, à l'aide de l'algorithme SHA-256, un ordinateur doit trouver une valeur de hachage répondant aux critères cible suivants (appelé niveau de difficulté):

SHA256 ("blockchain" + Nonce) = Hash Digest starting with "000000"

Dans cet exemple, la chaîne de texte «blockchain» est ajoutée à une valeur nonce, puis le résumé de hachage est calculé. Les valeurs nonce utilisées seront uniquement des valeurs numériques. Il s'agit d'un puzzle relativement facile à résoudre. Voici un exemple de résultat:

SHA256 ("blockchain0") =
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 (not solved)

SHA256 ("blockchain1") =
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 (not solved)

...

SHA256 ("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 (solved)

Pour résoudre ce puzzle, il a fallu 10 730 896 hypothèses (achevées en 54 secondes sur du matériel relativement ancien, en commençant à 0 et en testant une valeur à la fois).

Dans cet exemple, chaque valeur supplémentaire du «zéro principal» augmente la difficulté. En augmentant la cible d'un zéro supplémentaire ("0000000"), le même matériel a pris 934 224 175 propositions pour résoudre le puzzle (terminé en 1 heure, 18 minutes, 12 secondes):

SHA256 ("blockchain934224174") =
0x0000000e2ae7e4240df80692b7e586ea7a977eacbd031819d0e603257edb3a81

Il n'existe actuellement aucun raccourci connu vers ce processus. Les nœuds de publication doivent déployer des efforts de calcul, du temps et des ressources pour trouver la valeur de nonce correcte pour la cible. Souvent, les nœuds de publication tentent de résoudre ce puzzle informatique complexe en réclamant une récompense (généralement sous la forme d'une crypto-monnaie offerte par le réseau blockchain). La perspective d'être récompensé pour l'extension et la maintenance de la blockchain est appelée système de récompense ou modèle d'incitation.

2.2.2 Modèle de consensus de preuve de participation :

Le modèle de preuve d'enjeu repose sur l'idée que plus un utilisateur investit dans le système, plus il a de chances de vouloir que le système réussisse et moins il est probable qu'il voudra le renverser. L'enjeu est souvent une quantité de crypto-monnaie que l'utilisateur du réseau blockchain a investi dans le système (par divers moyens, par exemple en le verrouillant via un type de transaction spécial, en l'envoyant à une adresse spécifique ou en le conservant dans un logiciel de portefeuille spécial). Une fois implanté, la crypto-monnaie ne peut généralement plus être dépensée. La preuve d'enjeu des réseaux de blockchain utilise la quantité de participation d'un utilisateur comme facteur déterminant pour la publication de nouveaux blocs. Ainsi, la probabilité qu'un utilisateur du réseau de la blockchain publie un nouveau bloc est liée au rapport de sa mise sur la quantité totale de crypto-monnaie dépendante du réseau de la blockchain.
Avec ce modèle consensuel, il n'est pas nécessaire d'effectuer des calculs nécessitant beaucoup de ressources (temps, électricité et puissance de traitement) comme dans la preuve de travail. Comme ce modèle consensuel utilise moins de ressources, certains réseaux de blockchain ont décidé de renoncer à une récompense pour la création de blocs. Ces systèmes sont conçus de manière à ce que toute la crypto-monnaie soit déjà distribuée parmi les utilisateurs plutôt qu'une nouvelle crypto-monnaie générée à un rythme constant. Dans de tels systèmes, la publication en bloc est généralement récompensée par le gain des frais de transaction supportés par l'utilisateur.

Les méthodes utilisées par le réseau blockchain peuvent varier. Nous abordons ici quatre approches: la sélection aléatoire d'utilisateurs impliqués, le vote à plusieurs tours, les systèmes de vieillissement des pièces et les systèmes de délégation. Quelle que soit l'approche choisie, les utilisateurs ayant plus de participation sont plus susceptibles de publier de nouveaux blocs.

Lorsque le choix de l'éditeur de blocs est un choix aléatoire (parfois appelé preuve de participation basée sur une chaîne), le réseau de chaînes de blocs examine tous les utilisateurs concernés et choisit parmi eux en fonction du rapport entre leur participation et la quantité totale de crypto-monnaie mise. Ainsi, si un utilisateur détient 42% de la totalité de la participation au réseau blockchain, il sera choisi 42% du temps; ceux avec 1% seraient choisis 1% du temps.

Lorsque le choix de l'éditeur de blocs est un système de vote à plusieurs tours (parfois appelé preuve de tolérance de panne byzantine[14]), la complexité est accrue. Le réseau de blockchain sélectionnera plusieurs utilisateurs impliqués pour créer les blocs proposés. Ensuite, tous les utilisateurs mis en jeu voteront pour un bloc proposé. Plusieurs tours de vote peuvent avoir lieu avant qu'un nouveau bloc ne soit décidé. Cette méthode permet à tous les utilisateurs impliqués d'avoir une voix dans le processus de sélection de bloc pour chaque nouveau bloc.
Lorsque le choix de l'éditeur de bloc se fait par l'intermédiaire d'un système de jeu de pièces appelé une preuve de jeu de pièces de monnaie, la crypto-monnaie jouée a une propriété de temps. Au bout d'un certain temps (30 jours, par exemple), la crypto-monnaie impliquée peut être prise en compte dans la sélection de l'utilisateur propriétaire pour la publication du bloc suivant. La crypto-monnaie implicite a alors son âge réinitialisé et elle ne peut plus être utilisée tant que le temps requis n'est pas écoulé.

[14] *https://ieeexplore.ieee.org/document/7161576*

Cette méthode permet aux utilisateurs ayant plus d'enjeu de publier plus de blocs, sans pour autant dominer le système, puisqu'ils ont un temps de recharge attaché à chaque pièce de monnaie crypto-comptée comptabilisée dans la création de blocs. Des pièces plus anciennes et des groupes de pièces plus importants augmenteront la probabilité d'être choisi pour publier le bloc suivant. Pour empêcher les parties prenantes d'accumuler des crypto-monnaies anciennes, il existe généralement un maximum intégré à la probabilité de gagner.

Lorsque le choix de l'éditeur de blocs se fait par l'intermédiaire d'un système délégué, les utilisateurs votent pour que les nœuds deviennent des nœuds de publication, créant ainsi des blocs pour leur compte. Le pouvoir de vote des utilisateurs du réseau Blockchain étant lié à leur enjeu, plus l'enjeu est important, plus le vote a de poids. Les nœuds qui reçoivent le plus de votes deviennent des nœuds de publication et peuvent valider et publier des blocs. Les utilisateurs du réseau Blockchain peuvent également voter contre un nœud de publication établi pour tenter de les supprimer de l'ensemble des nœuds de publication. Le vote pour les nœuds de publication est continu et rester un nœud de publication peut être très compétitif. La menace de perdre le statut du nœud de publication, et par conséquent les récompenses et la réputation étant constantes, incite les nœuds de publication à ne pas agir de manière malveillante. De plus, les utilisateurs du réseau blockchain votent pour les délégués qui participent à la gouvernance de la blockchain. Les délégués proposeront des modifications et des améliorations qui seront mises aux voix par les utilisateurs du réseau blockchain.

Il convient de noter qu'un problème connu sous le nom de «rien en jeu» peut découler de la preuve de certains algorithmes d'enjeu. Si plusieurs chaînes de blocs concurrentes devaient exister à un moment donné (en raison d'un conflit temporaire dans le grand livre, comme indiqué à la section 2.6), un utilisateur mis en jeu pourrait agir sur chacune de ces chaînes en concurrence, car il est essentiellement libre de le faire. L'utilisateur mis en jeu peut le faire pour augmenter ses chances de gagner une récompense. Cela peut faire en sorte que plusieurs branches de la chaîne de blocs continuent de croître sans être réconciliées en une branche unique pendant de longues périodes.

Avec des systèmes de preuve d'enjeu, les «riches» peuvent plus facilement engranger davantage d'actifs numériques, en gagnant plus d'actifs numériques; Cependant, obtenir la majorité des actifs numériques dans un système pour le «contrôler» est généralement d'un coût prohibitif.

2.2.3 Modèle de consensus Round Robin :

Round Robin est un modèle de consensus utilisé par certains réseaux de chaînes de blocs autorisés. Dans ce modèle de consensus, les nœuds créent à tour de rôle des blocs. Round Robin Consensus à une longue histoire fondée sur l'architecture de système distribué. Pour gérer les situations dans lesquelles un nœud de publication n'est pas disponible pour publier un bloc à son tour, ces systèmes peuvent inclure une limite de temps pour permettre aux nœuds disponibles de publier des blocs afin que les nœuds non disponibles ne provoquent pas un arrêt de la publication du bloc. Ce modèle garantit qu'aucun nœud ne crée la majorité des blocs. Il bénéficie d'une approche simple, manque de puzzles cryptographiques et a une faible consommation d'énergie.

Dans la mesure où la confiance entre les nœuds est nécessaire, round robin ne fonctionne pas bien dans les réseaux blockchain sans autorisation utilisés par la plupart des crypto-monnaies. En effet, les nœuds malveillants peuvent ajouter en permanence des nœuds supplémentaires pour augmenter leurs chances de publier de nouveaux blocs. Dans le pire des cas, ils pourraient l'utiliser pour compromettre le bon fonctionnement du réseau de chaînes de blocs.

2.2.4 Modèle consensuel de preuve d'autorité / de preuve d'identité :

Le modèle de consensus preuve d'autorité (également appelé preuve d'identité) repose sur la confiance partielle des nœuds de publication via leur lien connu aux identités du monde réel. Les identités des nœuds de publication doivent avoir une identité prouvée et vérifiable au sein du réseau de chaînes de blocs (par exemple, identifier les documents vérifiés, notariés et inclus dans la chaîne de blocs). L'idée est que le nœud de publication mise sur son identité / réputation pour publier de nouveaux blocs. Les utilisateurs du réseau blockchain affectent directement la réputation du nœud de publication en fonction du comportement du nœud de publication. Les nœuds de publication peuvent perdre leur réputation en agissant de manière à être en désaccord avec les utilisateurs du réseau de chaînes de blocs, tout comme ils peuvent acquérir une réputation en agissant de manière à ce que les utilisateurs du réseau de chaînes de blocs soient d'accord. Plus la réputation est mauvaise, moins il est possible de publier un bloc. Par conséquent, il est dans l'intérêt d'un nœud de publication de conserver une réputation élevée. Cet algorithme ne s'applique qu'aux réseaux blockchain autorisés avec des niveaux de confiance élevés.

2.2.5 Modèle de consensus sur la preuve du temps écoulé :

Dans le modèle de consensus Preuve de temps écoulé, chaque nœud de publication demande un temps d'attente à une source de temps matérielle sécurisée au sein de son système informatique. La source de temps matérielle sécurisée générera un temps d'attente aléatoire et le renverra au logiciel du nœud de publication. Les nœuds de publication prennent le temps aléatoire qui leur est attribué et deviennent inactifs pendant cette durée. Une fois qu'un nœud de publication sort de l'état inactif, il crée et publie un bloc sur le réseau de chaînes de blocs, en alertant les autres nœuds du nouveau bloc. Tout nœud de publication encore inactif cessera d'attendre et le processus entier recommencera.

Ce modèle nécessite de s'assurer qu'un temps aléatoire a été utilisé, car si le temps d'attente n'était pas sélectionné au hasard, un nœud de publication malveillant attendrait simplement la durée minimale par défaut pour dominer le système. Ce modèle nécessite également de s'assurer que le nœud de publication a attendu l'heure actuelle et qu'il n'a pas démarré tôt. Ces exigences sont résolues en exécutant les logiciels dans un environnement d'exécution approuvé, présent sur certains processeurs (tels que Software Guard Extensions d'Intel[15], Processeur de sécurité de plate-forme AMD[16] ou TrustZone d'ARM[17]).

Les logiciels vérifiés et approuvés peuvent fonctionner dans ces environnements d'exécution sécurisés et ne peuvent pas être modifiés par des programmes extérieurs. Un nœud de publication interroge les logiciels s'exécutant dans cet environnement sécurisé pendant une durée aléatoire, puis attend la fin de cette période. Après avoir attendu l'heure attribuée, le nœud de publication peut demander un certificat signé attestant que le nœud de publication a attendu l'heure assignée de manière aléatoire. Le nœud de publication publie ensuite le certificat avec le bloc.

2.2.6 Conflits et résolutions du grand livre :

Comme indiqué précédemment, pour certains réseaux de blockchain, il est possible que plusieurs blocs soient publiés à peu près au même moment. Cela peut entraîner l'existence de versions différentes d'une blockchain à un moment donné; ceux-ci doivent être résolus rapidement pour avoir une cohérence dans le réseau blockchain. Dans cette section, nous discutons de la façon dont ces situations sont généralement gérées.

Avec n'importe quel réseau distribué, certains systèmes du réseau seront en retard sur les informations ou auront des informations alternatives. Cela dépend de la latence du réseau entre les nœuds et de la proximité des groupes de nœuds. Les réseaux de blockchain sans autorisation sont plus susceptibles d'avoir des conflits en raison de leur ouverture et du nombre de nœuds d'édition concurrents. La résolution des conflits de données est un élément essentiel pour s'accorder sur l'état du réseau de chaînes de blockchain (pour en arriver à un consensus).

---

[15] *Intel SGX - https://software.intel.com/en-us/sgx*
[16] *AMD Secure Technology - https://www.amd.com/en/technologies/security*
[17] *ARM TrustZone - https://www.arm.com/products/silicon-ip-security*

Par exemple :

- Nœud_A crée block_n (A) avec les transactions n ° 1, 2 et 3. Nœud_A le distribue à certains nœuds.
- Nœud_B crée block_n (B) avec les transactions n ° 1, 2 et 4. Nœud_B le distribue à certains nœuds.
- Il y a un conflit.
    - block_n ne sera pas identique sur le réseau.
        - block_n (A) contient la transaction n ° 3, mais pas la transaction n ° 4.
        - block_n (B) contient la transaction n ° 4, mais pas la transaction n ° 3.

Les conflits génèrent temporairement différentes versions de la blockchain, comme illustré à la figure 12. Ces différentes versions ne sont pas «fausses»; ils ont plutôt été créés avec les informations disponibles par chaque nœud. Les blocs en concurrence contiendront probablement différentes transactions. Par conséquent, ceux qui ont block_n (A) peuvent voir des transferts d'actifs numériques qui ne sont pas présents dans block_n (B). Si le réseau de blockchain traite de la crypto-monnaie, il peut arriver qu'une partie de la crypto-monnaie soit dépensée ou non, en fonction de la version de la chaîne de blocs visualisée.

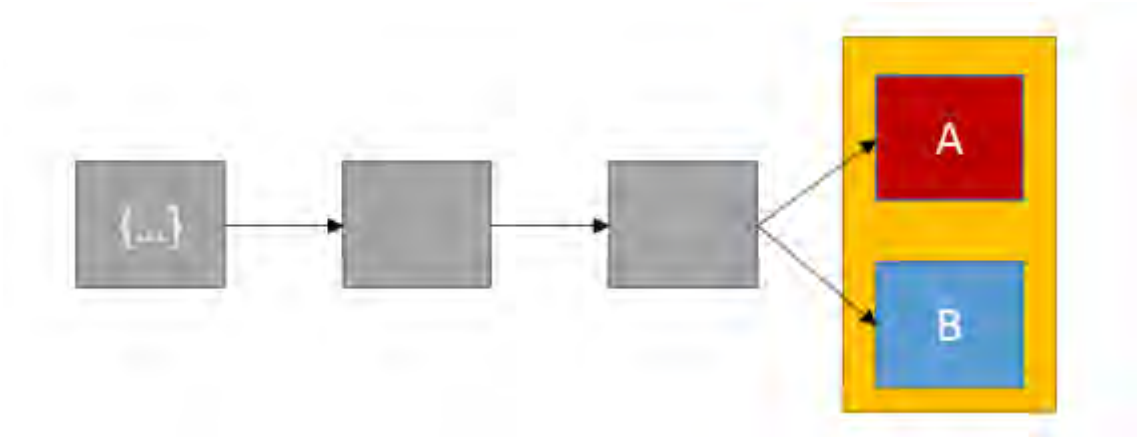


Figure 5 Grands livres en conflit

Les conflits sont généralement résolus rapidement. La plupart des réseaux de chaînes de blocs attendent la publication du bloc suivant et utilisent cette chaîne comme «chaîne de blocs officielle», adoptant ainsi la «chaîne de blocs plus longue». Comme dans la figure 13, la chaîne de blocs contenant block_n (B) devient la chaîne «officielle», car elle a obtenu le prochain bloc valide. Toute transaction présente dans block_n (A), le bloc orphelin, mais non présent dans la chaîne block_n (B), est renvoyée au pool de transactions en attente (c'est-à-dire où résident toutes les transactions non incluses dans un bloc). Notez que cet ensemble de transactions en attente est géré localement sur chaque nœud, car il n'existe aucun serveur central dans l'architecture.

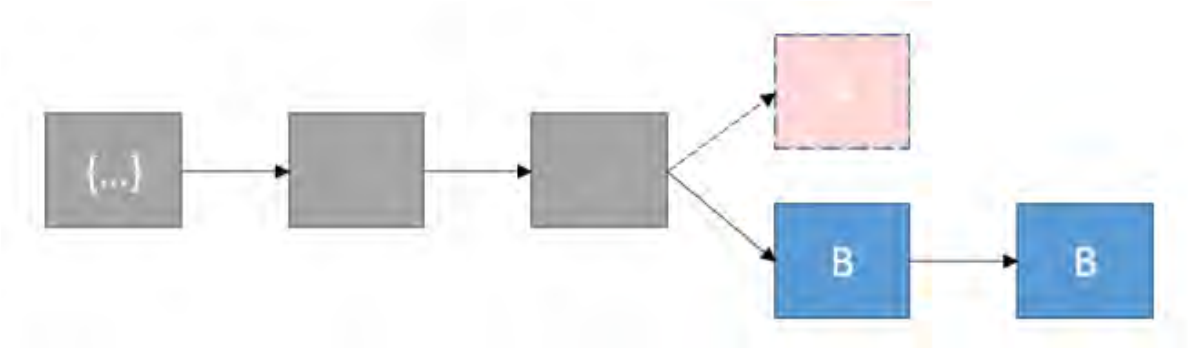


Figure 6 La chaîne avec block_n (B) ajoute le bloc suivant, la chaîne avec block_n (A) est maintenant orpheline.

En raison de la possibilité que des blocs soient écrasés, une transaction n'est généralement pas acceptée comme confirmée tant que plusieurs blocs supplémentaires n'ont pas été créés par-dessus le bloc contenant la transaction correspondante. L'acceptation d'un bloc est souvent plus probabiliste que déterministe, car les blocs peuvent être remplacés. Plus le nombre de blocs créés sur un bloc publié est élevé, plus il est probable que le bloc initial ne sera pas écrasé.

Hypothétiquement, un nœud dans un réseau de blockchain de preuve travail avec des quantités énormes de puissance de calcul pourrait commencer au bloc de genèse et créer une chaîne plus longue que la chaîne existante, effaçant ainsi toute l'histoire du blockchain. Cela ne se produit pas dans la pratique en raison de la quantité prohibitive de ressources que cela exigerait. De plus, certaines implémentations de blockchain bloquent des blocs plus anciens spécifiques dans le logiciel blockchain en créant des points de contrôle pour s'assurer que cela ne puisse jamais se produire.

2.3 Forking

Effectuer des changements et mettre à jour la technologie peut être difficile dans le meilleur des cas. Cela devient extrêmement difficile pour les réseaux de blockchain sans permission, composés de nombreux utilisateurs, répartis dans le monde entier et régis par le consensus des utilisateurs. Les modifications apportées au protocole et aux structures de données d'un réseau de blockchain sont appelées forks. Ils peuvent être divisés en deux catégories: soft forks et hard forks. Pour un soft forks, ces modifications sont rétro compatibles avec les nœuds qui n'ont pas été mis à jour. Pour un hard forks, ces modifications ne sont pas compatibles avec les versions antérieures, car les nœuds qui n'ont pas été mis à jour rejetteront les blocs après les modifications. Cela peut conduire à une scission du réseau de chaînes de blocs créant plusieurs versions de la même chaîne de blocs. Les réseaux de blockchain autorisés, en raison de la connaissance des nœuds de publication et des utilisateurs, peuvent atténuer les problèmes de forking en exigeant des mises à jour logicielles.

Notez que le terme fork est également utilisé par certains réseaux de chaînes de blocs pour décrire les conflits temporaires dans le grand livre (par exemple, deux blocs ou plus dans le réseau de chaînes de blocs avec le même numéro de bloc), comme décrit dans la section 2.7. Bien que ce soit un fork dans le grand livre, il est temporaire et ne découle pas d'un changement de logiciel.

2.3.1 Soft Forks :

Un soft fork est une modification apportée à une implémentation blockchain compatible avec les versions antérieures. Les nœuds non mis à jour peuvent continuer à effectuer des transactions avec des nœuds mis à jour. Si aucun (ou très peu) nœud n'est mis à niveau, les règles mises à jour ne seront pas suivies.

Un exemple fictif de "soft fork" serait si une blockchain décidait de réduire la taille des blocs (par exemple de 1,0 Mo à 0,5 Mo). Les nœuds mis à jour ajusteraient la taille du bloc et continueraient à effectuer leurs transactions normalement; Les nœuds non mis à jour verront ces blocs comme valides, car la modification apportée n'enfreint pas leurs règles (c'est-à-dire que la taille du bloc est inférieure à leur maximum autorisé). Toutefois, si un nœud non mis à jour créait un bloc d'une taille supérieure à 0,5 Mo, les nœuds mis à jour les rejetteraient comme non valides.

2.3.2 Hard Forks :

Un hard fork est une modification d'une implémentation blockchain qui n'est pas compatible avec les versions antérieures. À un moment donné (généralement à un numéro de bloc spécifique), tous les nœuds de publication devront passer au protocole mis à jour. De plus, tous les nœuds devront passer au nouveau protocole afin de ne pas rejeter les blocs récemment formatés. Les nœuds non mis à jour ne peuvent pas continuer à effectuer des transactions sur la blockchain mise à jour car ils sont programmés pour rejeter tout bloc qui ne suit pas leur version de la spécification de bloc.

Les nœuds de publication qui ne se mettent pas à jour continueront à publier des blocs en utilisant l'ancien format. Les nœuds utilisateur qui ne se sont pas mis à jour rejetteront les blocs nouvellement formatés et n'accepteront que les blocs avec l'ancien format. Cela se traduit par deux versions de la blockchain existantes simultanément. Notez que les utilisateurs de différentes versions de hard fork ne peuvent pas interagir les uns avec les autres. Il est important de noter que bien que la plupart des hard forks soient intentionnelles, les erreurs de logiciel peuvent produire des hard forks non intentionnelles.

Ethereum est un exemple bien connu du hard fork. En 2016, un contrat intelligent a été construit sur Ethereum, appelé Decentralized Autonomous Organization (DAO). En raison de failles dans la manière dont le contrat intelligent a été construit, un attaquant a extrait Ether, la crypto-monnaie utilisée par Ethereum, entraînant un vol de 50 millions de dollars. Les détenteurs d'Ether ont voté pour une proposition d'un hard fork, et la grande majorité des utilisateurs a accepté de créer une nouvelle version de la blockchain, sans la faille, et qui a également restitué les fonds volés.

Avec les crypto-monnaies, s'il existe un hard fork et que la blockchain se divise, les utilisateurs disposeront d'une monnaie indépendante sur les deux fourchettes (le double du nombre de pièces au total). Si toute l'activité passe à la nouvelle chaîne, l'ancienne peut ne plus être utilisée car les deux chaînes ne sont pas compatibles (il s'agira de systèmes monétaires indépendants). Dans le cas du hard fork Ethereum, la grande majorité du support est passée à la nouvelle fourche. L'ancienne fourche a été renommée Ethereum Classic et a continué à fonctionner.

2.3.3 Changements cryptographiques et forks :

Si des failles sont trouvées dans les technologies de cryptographie à l'intérieur d'un réseau à blockchain, la seule solution peut être de créer un hard fork, en fonction de l'importance de la faille. Par exemple, si un défaut était trouvé dans les algorithmes sous-jacents, il pourrait y avoir un fork exigeant que tous les futurs clients utilisent un algorithme plus fort. Le passage à un nouvel algorithme de hachage pourrait poser un problème pratique important, car il pourrait invalider tout le matériel minier spécialisé existant.

Hypothétiquement, si SHA-256 étaient découverts pour avoir un défaut, les réseaux de blockchain qui utilisent SHA256 auraient besoin d'un hard fork pour migrer à un nouvel algorithme de hachage. Le bloc qui est passé au nouvel algorithme de hachage "verrouillerait" tous les blocs précédents dans SHA-256 (pour vérification), et tous les nouveaux blocs devraient utiliser le nouvel algorithme de hachage.

Il existe de nombreux algorithmes de hachage cryptographique, et les réseaux de blockchain peuvent utiliser celui qui convient à leurs besoins. Par exemple, alors que Bitcoin utilise SHA-256, Ethereum utilise Keccak-256[18].
Une possibilité de modifier les caractéristiques cryptographiques présentes dans un réseau blockchain serait la mise au point d'un système informatique quantique pratique, capable d'affaiblir considérablement (et, dans certains cas, de rendre inutile) les algorithmes cryptographiques existants. Le rapport interne NIST (NISTIR) 8105, Rapport sur la cryptographie post-quantique[19], fournit un tableau décrivant l'impact de l'informatique quantique sur des algorithmes de chiffrement courants. Le tableau 2 reproduit ce tableau.

Algorithme cryptographique	**Type**	**Objectif**	**Impact de l'ordinateur quantique à grande échelle**
AES	Symetric Key	Encryption	Grandeurs de clé nécessaires
SHA-2, SHA3	N/A	Hash Functions	Plus grande sortie nécessaire
RSA	Public Key	Signatures, Key establishment	N'est plus sécurisé
ECDSA, ECDH (Elliptic Curve Cryptography)	Public Key	Signatures, Key Exchange	N'est plus sécurisé
DSA (Finite Field Cryptography)	Public Key	Signatures, Key Exchange	N'est plus sécurisé

Tableau 2 Impact de l'informatique quantique sur les algorithmes cryptographiques courants

Les algorithmes cryptographiques utilisés dans la plupart des technologies blockchain pour les paires de clés asymétriques devront être remplacés si un ordinateur quantique puissant devient une réalité. En effet, les algorithmes reposant sur la complexité de calcul de la factorisation de nombres entiers (telle que RSA) ou travaillant à la résolution de logarithmes discrets (tels que DSA et Diffie-Hellman) sont très susceptibles d'être détruits par l'informatique quantique. Les algorithmes de hachage utilisés par les réseaux de chaînes de blocs sont beaucoup moins sensibles aux attaques informatiques quantiques mais sont encore affaiblis.

[18] *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf*
[19] *https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf*

2.4 Catégorisation de la Blockchain

Les réseaux de blockchain peuvent être classés en fonction de leur modèle d'autorisation, qui détermine qui peut les gérer (par exemple, des blocs de publication). Si quelqu'un peut publier un nouveau bloc, il est sans permission. Si seuls des utilisateurs particuliers peuvent publier des blocs, l'autorisation est accordée. En termes simples, un réseau blockchain autorisé est comme un intranet d'entreprise contrôlé, alors qu'un réseau blockchain sans autorisation s'apparente à l'internet public, où tout le monde peut participer. Les réseaux de chaînes de blocs autorisés sont souvent déployés pour un groupe d'organisations et d'individus, généralement appelé consortium. Cette distinction est nécessaire pour comprendre car elle affecte certains des composants de la chaîne de blocs décrits plus loin dans ce document.

2.4.1 Permission :

Les réseaux de blockchain autorisés sont ceux où les utilisateurs qui publient des blocs doivent être autorisés par une autorité (centralisée ou décentralisée). Etant donné que seuls les utilisateurs autorisés gèrent la blockchain, il est possible de restreindre l'accès en lecture et de restreindre l'accès aux transactions. Les réseaux de blockchain autorisés peuvent ainsi permettre à quiconque de lire ces chaînes ou restreindre l'accès en lecture à des personnes autorisées. Ils peuvent également permettre à quiconque de soumettre des transactions à inclure dans la blockchain ou, encore une fois, restreindre cet accès uniquement aux personnes autorisées. Les réseaux de blockchain autorisés peuvent être instanciés et maintenus à l'aide de logiciels open source ou fermés.

Les réseaux de blockchain autorisés peuvent avoir la même traçabilité des actifs numériques lorsqu'ils passent dans la blockchain, ainsi que le même système de stockage de données distribué, résilient et redondant en tant que réseaux de blockchain sans autorisation. Ils utilisent également des modèles consensuels pour la publication de blocs, mais ces méthodes ne nécessitent souvent pas de dépense en ressources ni en maintenance (comme c'est le cas avec les réseaux de blockchain sans autorisation actuels). C'est parce que l'établissement de l'identité est nécessaire pour participer en tant que membre du réseau de chaînes de blocs autorisé; ceux qui gèrent la blockchain ont un niveau de confiance réciproque, puisqu'ils étaient tous autorisés à publier des blocs et que leur autorisation peut être révoquée s'ils se conduisent mal. Les modèles de consensus dans les réseaux de blockchain autorisés sont généralement plus rapides et moins onéreux en termes de calcul.

Les réseaux autorisés à utiliser une blockchain peuvent également être utilisés par les organisations qui ont besoin de contrôler et de protéger plus étroitement leur blockchain. Cependant, si une seule entité contrôle qui peut publier des blocs, les utilisateurs de la blockchain devront avoir confiance dans cette entité. Les réseaux de blockchain autorisés peuvent également être utilisés par les organisations qui souhaitent travailler ensemble mais ne se font pas entièrement confiance. Ils peuvent établir un réseau de blockchain autorisé et inviter les partenaires commerciaux à enregistrer leurs transactions sur un grand livre distribué. Ces organisations peuvent déterminer le modèle de consensus à utiliser, en fonction de leur degré de confiance mutuel. Au-delà de la confiance, les réseaux de blockchain autorisés offrent une transparence et des informations qui peuvent aider à mieux éclairer les décisions commerciales et responsabiliser les parties qui se conduisent mal.

Cela peut inclure explicitement des entités d'audit et de supervision, faisant des audits une occurrence constante par rapport à un événement périodique.

Certains réseaux de blockchain autorisés prennent en charge la possibilité de révéler de manière sélective des informations sur les transactions en fonction de l'identité ou des informations d'identification des utilisateurs du réseau de chaînes. Avec cette fonctionnalité, un certain degré de confidentialité dans les transactions peut être obtenu. Par exemple, il se peut que la blockchain enregistre qu'une transaction a eu lieu entre deux utilisateurs du réseau de blockchain, mais que le contenu réel des transactions n'est accessible qu'aux parties impliquées.

Certains réseaux blockchain autorisés exigent que tous les utilisateurs soient autorisés à envoyer et recevoir des transactions (ils ne sont ni anonymes ni même pseudo-anonymes). Dans de tels systèmes, les parties travaillent ensemble pour mettre en place un processus commercial commun avec des éléments dissuasifs naturels de commettre une fraude ou de se comporter autrement comme un mauvais acteur (car ils peuvent être identifiés). Si un mauvais comportement devait se produire, il est bien connu où les organisations sont incorporées, quels recours juridiques sont disponibles et comment exercer ces recours dans le système judiciaire compétent.

2.4.2 Sans permission :

Les réseaux de blockchain sans autorisation sont des plates-formes de grand livre décentralisées ouvertes à tous ceux qui publient des blocs, sans avoir besoin de l'autorisation d'une autorité. Les plates-formes blockchain sans autorisation sont souvent des logiciels open source, disponibles gratuitement pour tous ceux qui souhaitent les télécharger. Etant donné que tout le monde a le droit de publier des blocs, il en résulte que tout le monde peut lire la blockchain et émettre des transactions sur la blockchain (en incluant ces transactions dans des blocs publiés). Tout utilisateur du réseau blockchain au sein d'un réseau blockchain sans autorisation peut lire et écrire dans le grand livre. Étant donné que les réseaux de chaînes de blocs sans autorisation sont ouverts à la participation de tous, des utilisateurs malveillants peuvent tenter de publier des blocs de manière à sous-inverser le système (exposé en détail plus loin). Pour éviter cela, les réseaux de blockchain sans permission utilisent souvent un accord multipartite ou un système de «consensus» (voir la section 2) qui oblige les utilisateurs à dépenser ou à maintenir des ressources lorsqu'ils tentent de publier des blocs. Cela empêche les utilisateurs malveillants de renverser facilement le système. Des exemples de tels modèles consensuels incluent les méthodes de preuve de travail (voir section 2.1) et de preuve d'enjeu (voir section 2.2). Les systèmes de consensus dans les réseaux de blockchain sans permission encouragent généralement les comportements non malveillants en récompensant les éditeurs de blocs conformes au protocole avec une crypto-monnaie native.

2.5 Cryptocurrencies

De nombreuses applications des technologies blockchain sont principalement axées sur le transfert de devises d'un compte à un autre. Cette section présente plusieurs exemples d'applications de blockchain

2.5.1 Bitcoin (BTC) :

Le Bitcoin est un système de paiement numérique qui a déjà été présenté comme le pionnier de l'utilisation d'une blockchain. De nouveaux blocs sont créés environ une fois toutes les 10 minutes à l'aide du hachage SHA-256 (voir section 1.4) pour les lier ensemble. C'est un système de preuve de travail où les nœuds d'exploration de données doivent trouver un nonce à inclure dans leur bloc de telle sorte que le hachage du bloc soit inférieur à une valeur de difficulté prédéterminée. La difficulté est ajustée vers le haut ou vers le bas pour tenter d'atteindre l'objectif de 10 minutes pour la création de blocs. Au début de l'histoire de Bitcoin, des ordinateurs individuels pouvaient extraire et publier des blocs; Actuellement, Bitcoin nécessite du matériel spécialisé, de grands centres de données ou de nombreuses personnes travaillant ensemble dans un pool de minage pour gagner la compétition pour publier un bloc.

Avec Bitcoin, le paiement des frais de transaction est techniquement facultatif car les nœuds miniers obtiennent la plupart de leurs fonds via la publication de blocs. Ces frais sont conçus pour être peu élevés pour chaque transaction, mais ils peuvent et sont devenus importants en raison d'un important arriéré de transactions en attente. Payer des frais de transaction plus élevés peut donner à une transaction une plus grande priorité pour être ajouté à la blockchain. Initialement, les nœuds d'exploration de données ont obtenu 50 Bitcoin pour chaque bloc, et seulement la moitié après un certain nombre de blocs. Par exemple, la récompense pour l'extraction d'un bloc était de 12,5 Bitcoins en juillet 2016. Selon le protocole Bitcoin, cette récompense diminuera de moitié tous les 210 000 blocs (environ quatre ans) et passera à zéro une fois que 21 millions de Bitcoins auront été produits. L'extraction de Bitcoin continuera à ce stade, mais la récompense sera entièrement dérivée des frais de transaction.

2.5.2 Ethereum (ETH) :

Ethereum est une plate-forme de blockchain axée sur la fourniture de smart contracts. Les smart contracts sont des programmes qui existent sur le blockchain et auxquels les utilisateurs d'Ethereum peuvent accéder. Ils peuvent à la fois recevoir et envoyer des fonds tout en effectuant des calculs arbitraires. Un contrat correctement conçu peut agir comme un tiers de confiance dans les transactions financières puisque son code est à la fois public et immuable. Le langage de programmation des transactions Ethereum est complet. Les nœuds miniers reçoivent des fonds par le biais de droits miniers et de frais de transaction.

Ethereum a également un concept appelé " gas " utilisé pour alimenter les calculs transactionnels (et est généralement autour de 1/100 000 d'un Ether). Chaque transaction consomme du gas comme il s'exécute, et à l'origine d'une transaction particulière doit payer suffisamment de gas, ou de l'exécution de la transaction échoue.

Il y a une limite maximale de gaz par contrat smart (actuellement trois millions de gas) pour empêcher les programmes coûteux en calcul d'être soumis aux nœuds miniers Ethereum. Cela est dû au fait que tous les nœuds miniers doivent exécuter les transactions en parallèle.

La soumission d'une transaction à un contrat Ethereum fait qu'un programme est exécutée en parallèle sur les ordinateurs des nœuds miniers. L'état résultant du contrat est stocké sur le blockchain par l'utilisateur qui publie le bloc suivant.

2.5.3 Ripple (XRP) :

Ripple est le nom à la fois d'une crypto-monnaie et du réseau de paiement sur lequel elle est transférée. L'objectif de Ripple est de s'appuyer sur l'approche du Bitcoin et de connecter différents systèmes de paiement ensemble. Il dispose d'une offre fixe de 100 milliards de XRP, dont la moitié est destinée à la circulation. Les clients Ripple n'ont pas besoin de télécharger l'intégralité de la blockchain, ce qui facilite la connexion des clients en quelques secondes. De plus, il n'y a aucune récompense minière pour l'exécution d'un serveur car chaque transaction coûte une petite quantité d'ondulation, similaire au gas Ethereum. Par conséquent, il n'y a pas de nœuds d'exploration ou de pools d'exploration de données; au lieu de cela, environ un millième de cent de chaque transaction est détruit. Ripple n'est pas conçu avec des objectifs explicites d'anonymat, mais il dispose de fonctionnalités assurant la confidentialité, telles que l'utilisation de paiements par passerelle mandatés.

2.6 Limitations de Blockchain et idées fausses

Il y a une tendance à sur-typer et à abuser de la technologie naissante. De nombreux projets tenteront d'intégrer la technologie, même si elle est inutile. Cela tient au fait que la technologie est relativement nouvelle et mal comprise, entourée d'idées fausses et de la peur de passer à côté. La technologie Blockchain n'a pas été épargnée. Cette section met en évidence certaines des limitations et idées fausses de la technologie blockchain.

2.6.1 Immutabilité :

La plupart des publications sur la technologie blockchain décrivent les registres comme étant immuables. Cependant, ce n'est pas strictement vrai. Ils sont inviolables et c'est une raison de leur confiance pour les transactions financières. Ils ne peuvent pas être considérés comme totalement immuables, car il existe des situations dans lesquelles la blockchain peut être modifiée. Dans cette section, nous examinerons différentes manières de violer le concept d'immuabilité pour les registres à blocs.

La blockchain elle-même ne peut être considérée comme totalement immuable. Pour certaines implémentations de la blockchain, les blocs les plus récemment publiés, peuvent être remplacés (par une chaîne alternative plus longue, avec des blocs "taille" différents). Comme indiqué précédemment, la plupart des réseaux de blockchain utilisent la stratégie consistant à adopter la chaîne la plus longue (celle avec le plus de travail fourni) comme une vérité lorsqu'il existe plusieurs chaînes en concurrence. Si deux chaînes sont en compétition mais que chacune d'elles comprend sa propre séquence de blocs de queue, la plus longue des deux sera adoptée. Toutefois, cela ne signifie pas que les transactions au sein des blocs remplacés sont perdues elles peuvent plutôt avoir été incluses dans un bloc différent ou renvoyées au pool de transactions en attente. C'est ce degré de faible immuabilité des blocs d'extrémité qui explique pourquoi la plupart des utilisateurs du réseau blockchain attendent plusieurs créations de bloc avant de considérer qu'une transaction est valide.

2.6.2 Utilisateurs impliqués dans la gouvernance de Blockchain :

La gouvernance des réseaux de blockchain traite des règles, pratiques et processus par lesquels le réseau de blockchain est dirigé et contrôlé. Une idée fausse commune est que les réseaux blockchain sont des systèmes sans contrôle ni propriété. La phrase «personne ne contrôle une blockchain!» s'exclame souvent. Ce n'est pas strictement vrai. Les réseaux de blockchain autorisés sont généralement configurés et gérés par un propriétaire ou un consortium, qui régit le réseau de blockchain. Les réseaux blockchain sans autorisation sont souvent régis par les utilisateurs du réseau blockchain, les nœuds de publication et les développeurs de logiciels. Chaque groupe a un niveau de contrôle qui influe sur la direction de l'avancement du réseau de blockchain.

Les développeurs de logiciels créent le logiciel blockchain utilisé par un réseau blockchain. Étant donné que la plupart des technologies blockchain sont open source, il est possible d'inspecter le code source et de le compiler indépendamment. Il est même possible de créer un logiciel séparé mais compatible pour contourner les logiciels précompilés publiés par les développeurs.

Cependant, tous les utilisateurs ne seront pas en mesure de le faire, ce qui signifie que le développeur du logiciel Blockchain jouera un rôle important dans la gouvernance du réseau Blockchain. Ces développeurs peuvent agir dans l'intérêt de la communauté en général et sont tenus pour responsables. Par exemple, en 2013, les développeurs de Bitcoins ont publié une nouvelle version du client Bitcoin le plus répandu, introduisant une faille et démarrant deux blockchain en concurrence. Les développeurs devaient décider de conserver la nouvelle version (qui n'avait pas encore été adoptée par tous) ou de revenir à l'ancienne version. Dans les deux cas, une chaîne sera rejetée et certaines transactions de l'utilisateur du réseau blockchain deviendront invalides. Les développeurs ont fait leur choix, sont revenus à l'ancienne version et ont contrôlé avec succès la progression de la blockchain Bitcoin.

En résumé, les développeurs de logiciels, les nœuds de publication et les utilisateurs du réseau blockchain jouent tous un rôle dans la gouvernance du réseau blockchain.

2.6.3 Blockchain Death :

Les systèmes centralisés traditionnels sont constamment créés et démantelés, et les réseaux à chaînes multiples ne seront probablement pas différents. Cependant, parce qu'ils sont décentralisés, il y a une chance que lorsqu'un réseau de blockchain "s'arrête" il ne sera jamais complètement arrêté, et qu'il peut toujours y avoir des nœuds de blockchain en cours d'exécution.

Un blockchain obsolète ne serait pas adapté à un enregistrement historique, car sans beaucoup de nœuds d'édition, un utilisateur malveillant pourrait facilement dominer les quelques nœuds d'édition restants et refaire et remplacer n'importe quel nombre de blocs.

2.6.4 Au-delà du Digital :

Les réseaux de blockchain fonctionnent extrêmement bien avec les données au sein de leurs propres systèmes numériques. Cependant, lorsqu'ils ont besoin d'interagir avec le monde réel, certains problèmes se posent (souvent appelé le problème Oracle[20]). Un réseau blockchain peut être un endroit pour enregistrer à la fois les données d'entrée humaines et les données d'entrée de capteurs du monde réel, mais il peut ne pas y avoir de méthode pour déterminer si les données d'entrée reflètent des événements du monde réel. Un capteur peut ne pas fonctionner correctement et enregistrer des données inexactes. Les humains pourraient enregistrer de fausses informations (intentionnellement ou non). Ces problèmes ne concernent pas uniquement les réseaux blockchain, mais l'ensemble des systèmes numériques. Cependant, pour les réseaux de blockchain qui sont pseudonymes, le traitement de fausses déclarations de données en dehors du réseau numérique peut être particulièrement problématique.

Par exemple, si une transaction de crypto-monnaie a eu lieu pour acheter un article du monde réel, il est impossible de déterminer dans le réseau de blockchain si l'envoi a eu lieu, sans faire appel à un capteur extérieur ou à une intervention humaine.

[20] *https://cointelegraph.com/explained/blockchain-oracles-explained*

2.6.5 Cybersecurité :

L'utilisation de la technologie blockchain ne supprime pas les risques inhérents à la cybersécurité qui nécessitent une gestion des risques réfléchie et proactive. Bon nombre de ces risques inhérents comportent un élément humain. Par conséquent, un solide programme de cybersécurité reste essentiel pour protéger le réseau et les organisations participantes des cyber-menaces, en particulier à mesure que les pirates informatiques développent davantage de connaissances sur les réseaux blockchain et leurs vulnérabilités.

Les normes et directives existantes en matière de cybersécurité restent extrêmement pertinentes pour garantir la sécurité des systèmes qui interfacent et / ou reposent sur des réseaux blockchain. Sous réserve de certains ajustements pour tenir compte d'attributs spécifiques de la technologie de la blockchain, les normes et directives existantes constituent une base solide pour la protection des réseaux de la blockchain contre les cyberattaques.

En plus des principes généraux et des contrôles, il existe des normes spécifiques de cybersécurité qui s'appliquent à la technologie blockchain et qui existent déjà et sont largement utilisées par de nombreuses industries. Par exemple, le cadre de cybersécurité du NIST stipule expressément qu'il ne s'agit pas d'une approche universelle de gestion du risque de cybersécurité, car « les organisations continueront d'avoir des risques uniques, différentes menaces, différentes vulnérabilités, différentes tolérances au risque et la façon dont elles mettent en œuvre les pratiques du [Framework] variera. » Cela dit, même si le Framework n'a pas été conçu spécifiquement pour la technologie blockchain, ses normes sont suffisamment générales pour couvrir la technologie blockchain et pour aider les institutions à élaborer des politiques et des processus qui permettent de cerner et de contrôler les risques qui touchent la technologie des blockchain.

2.6.6 Cyberattaques et attaques réseau :

Les technologies de blockchain sont considérées comme extrêmement sécurisées en raison de leur conception inviolable et résistante à la falsification une fois qu'une transaction est validée dans la chaîne de blocs, elle ne peut généralement pas être modifiée. Toutefois, cela n'est vrai que pour les transactions qui ont été incluses dans un bloc publié. Les transactions qui n'ont pas encore été incluses dans un bloc publié dans la blockchain sont vulnérables à plusieurs types d'attaques. Pour les réseaux blockchain qui ont des horodatages transactionnels, le temps d'usurpation d'identité ou le réglage de l'horloge d'un membre d'un service de commande peut avoir des effets positifs ou négatifs sur une transaction, faisant du temps et de la communication du temps un vecteur d'attaque. Les attaques par déni de service peuvent être menées sur la plate-forme blockchain ou sur le contrat intelligent implémenté sur la plate-forme.

Les réseaux de blockchain et leurs applications ne sont pas à l'abri des acteurs malveillants qui peuvent effectuer une analyse et une reconnaissance de réseau afin de découvrir et d'exploiter des vulnérabilités et de lancer des attaques «zero day». Dans la hâte de déployer des services basés sur des blockchain, les applications nouvellement codées (telles que les contrats intelligents) peuvent contenir des vulnérabilités nouvelles et connues ainsi que des faiblesses de déploiement qui seront découvertes puis attaquées via le réseau, tout comme les sites Web ou les applications sont attaqués aujourd'hui.

2.6.7 Infrastructure à clé publique et identité :

En entendant que la technologie blockchain intègre une infrastructure à clé publique, certaines personnes pensent immédiatement qu'elle supporte intrinsèquement l'identité. Ce n'est pas le cas, car il peut ne pas y avoir de relation un à un de paires de clés privées avec les utilisateurs (un utilisateur peut avoir plusieurs clés privées), et il n'existe pas non plus de relation un à un entre les adresses en chaîne et les clés publiques (plusieurs adresses peuvent être dérivées d'une seule clé publique).

Les signatures numériques sont souvent utilisées pour prouver l'identité dans le monde de la cybersécurité, ce qui peut entraîner une confusion quant à l'application potentielle d'une blockchain à la gestion des identités. Le processus de vérification de la signature d'une transaction de la blockchain relie les transactions aux propriétaires de clés privées, mais ne permet pas d'associer des identités réelles à ces propriétaires. Dans certains cas, il est possible de connecter des identités du monde réel à des clés privées, mais ces connexions sont établies via des processus extérieurs et non explicitement pris en charge par la blockchain. Par exemple, un organisme chargé de l'application de la loi pourrait demander des enregistrements à un échange qui relierait des transactions à des individus spécifiques. Un autre exemple est une personne qui affiche une adresse de crypto-monnaie sur son site Web personnel ou sa page de média social pour les dons, ce qui fournirait un lien d'adresse à l'identité du monde réel.

Bien qu'il soit possible d'utiliser la technologie blockchain dans les cadres de gestion des identités nécessitant un composant de grand livre distribué, il est important de comprendre que les implémentations classiques de blockchain ne sont pas conçues pour servir de systèmes de gestion d'identités autonomes. La sécurité des identités numériques ne se limite pas à la simple mise en place d'une blockchain.