420-1B3 - Bureautique

***Block Chain***

Cédric Daigneault (2132903) – Groupe 1020

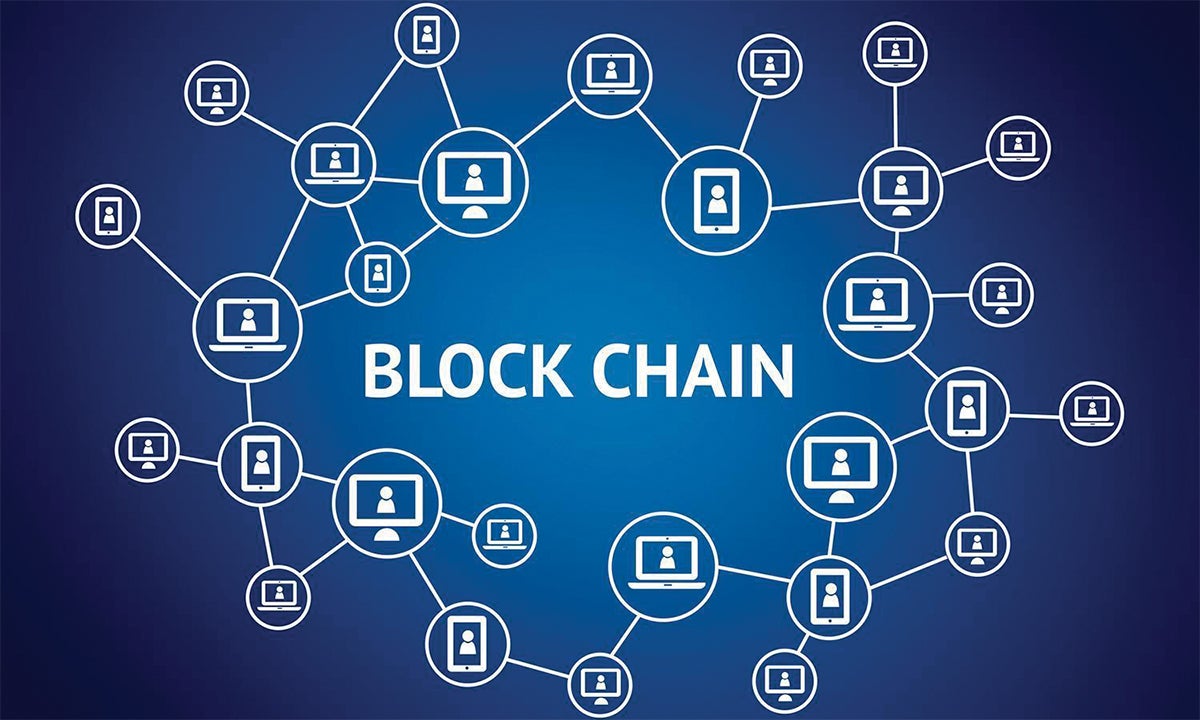
[[1]](#endnote-1)

Table des matières

[Aspects 3](#_Toc114240649)

[Aspects Historique 3](#_Toc114240650)

[Fiabilité 3](#_Toc114240651)

[Fonctionnement 4](#_Toc114240652)

[La preuve de travail, méthode historique de consensus 4](#_Toc114240653)

[Reference 5](#_Toc114240654)

# Aspects

## Aspects Historique

Depuis lors, beaucoup de [monnaies virtuelles](https://fr.wikipedia.org/wiki/Monnaie_virtuelle) et de [cryptomonnaies](https://fr.wikipedia.org/wiki/Cryptomonnaie) utilisent les chaînes de blocs pour leur sécurité. Les transactions sur une chaîne de blocs sont pratiquement impossibles à annuler parce que les chaînes de blocs sont résistantes aux changements[14](https://fr.wikipedia.org/wiki/Blockchain#cite_note-14).

Après 2008, la **b**l**o***c****k****c*h*a*i*n* et les cryptomonnaies qui en dépendent ont souvent été présentées comme une source presque miraculeuse d'enrichissement, suscitant l'intérêt de la bourse alors plongée dans le marasme de la [crise de 2008](https://fr.wikipedia.org/wiki/Crise_bancaire_et_financi%C3%A8re_de_l%27automne_2008). De nombreuses entreprises se sont alors rebaptisées en intégrant le mot « blockchain » ou « bitcoin » dans leur nouveau nom (procédure illégale dans certains pays, dont les États-Unis car pouvant s'apparenter à de la [désinformation](https://fr.wikipedia.org/wiki/D%C3%A9sinformation) et à de la [publicité mensongère](https://fr.wikipedia.org/wiki/Publicit%C3%A9_mensong%C3%A8re)). Une étude, publiée dans *[Economics](https://fr.wikipedia.org/wiki/Economics_Letters" \o "Economics Letters)* [Lettres](https://fr.wikipedia.org/wiki/Economics_Letters" \o "Economics Letters) en août 2019, a montré que ces entreprises y gagnent significativement en notoriété ou valeur durant deux mois, mais que cet effet s'estompe et s'inverse ensuite en effet négatif (dans les cinq mois après le changement)[15](https://fr.wikipedia.org/wiki/Blockchain#cite_note-NomHyst2019-15). Les auteurs invitent les investisseurs à être prudents à l'égard d'entreprises changeant de nom avant d'investir réellement dans la blockchain, ces changements de nom, de façade, étant généralement uniquement destinés à profiter de « l'hystérie entourant la hausse des prix du bitcoin ».

Aux [États-Unis](https://fr.wikipedia.org/wiki/%C3%89tats-Unis), de nombreuses sociétés ont été citées à comparaître devant la [Securities and Exchange Commission](https://fr.wikipedia.org/wiki/Securities_and_Exchange_Commission) (SEC) pour avoir inclus le terme « blockchain » dans leur nom en l'absence d'un lien clair avec le domaine. Ainsi de *Riot Blockchain*, qui est passée du domaine vétérinaire au [minage](https://fr.wikipedia.org/wiki/Minage_de_cryptomonnaie) de Bitcoin.[[2]](#endnote-2)

## Fiabilité

Comme les crypto-monnaies dont elle constitue l'armature, la blockchain est presque toujours présentée dans les médias comme immuable, impossible à pirater et anti-fraude.

Alors que dans les années 2020 certains suggèrent de remplacer tout ou partie des [audits financiers](https://fr.wikipedia.org/wiki/Audit_financier) (ou d'autres types d'audits) par des blockchains, une étude (2020) a voulu vérifier si dans les faits, le degré de sécurité des crypto-monnaies et des registres de blockchain est aussi élevé qu'on le dit généralement.

Les auteurs, Castonguay et Stein Smith, ont compilé et étudié la littérature existante sur les offres initiales de cryptomonnaie, les niveaux de sécurité, les vols et piratages de blockchains et de plateformes fondées sur la blockchain ou dans les [portefeuilles de crypto-monnaies](https://fr.wikipedia.org/wiki/Portefeuille_de_crypto-monnaie). Ils en ont conclu : « Contrairement à la presse populaire, nous constatons qu'en pratique, la blockchain et les crypto-monnaies sont plus sujettes aux malversations, à la [fraude](https://fr.wikipedia.org/wiki/Fraude) et à la manipulation qu'on ne le pense généralement. La sécurité et la confiance fournies par la blockchain en tant qu'outil technologique ne sont pas plus sûres que le code sous-jacent qui établit la blockchain et la valeur dérivée des cryptomonnaies n'est pas plus fiable que l'entité développant la crypto-monnaie. Ni l'un ni l'autre ne sont sans vulnérabilités. Le [scepticisme](https://fr.wikipedia.org/wiki/Scepticisme_scientifique) et une [diligence raisonnable](https://fr.wikipedia.org/wiki/Diligence_raisonnable) appropriée doivent être maintenus pour toute entité cherchant à utiliser la technologie blockchain ou à investir dans les crypto-monnaies ».

A picture containing text, several

Description automatically generatedEn d'autres termes la fiabilité de la blockchain dépend largement de la méthode employée pour la sécuriser, elle n'est pas automatiquement immuable.

Selon les professionnels de la finance, la qualité des données vérifiées et stockées « en chaîne » est considérablement inférieure à celle des états financiers résultant d'un véritable audit.

En, juin 2022, un rapport financé par la *[Defense Advanced Research Projects Agency](https://fr.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency" \o "Defense Advanced Research Projects Agency)* (DARPA) américaine indique qu'une blockchain peut être excessivement centralisée en exploitant les faiblesses des propriétés de son implémentation[[3]](#endnote-3)

# Fonctionnement

## La preuve de travail, méthode historique de consensus

* La chaîne de blocs est une forme de mise en œuvre de la solution du « [problème des généraux byzantins](https://fr.wikipedia.org/wiki/Probl%C3%A8me_des_g%C3%A9n%C3%A9raux_byzantins) ».
* Ce problème mathématique consiste à s'assurer qu’un ensemble de composants informatiques fonctionnant de concert sache gérer des défaillances (ou malveillances) et arrive à produire un consensus.
* Le système doit pouvoir maintenir sa fiabilité dans le cas où une part des participants enverrait des informations erronées ou malveillantes, comme dans le cas d'une cryptomonnaie, pour contourner la vérification de la double dépense par les [mineurs](https://fr.wikipedia.org/wiki/Minage_de_cryptomonnaie) du réseau (la double dépense consiste à réaliser deux paiements simultanément : un vers soi-même et un autre vers une victime ; l'objectif est de voir le paiement vers la victime inscrit dans la chaîne de blocs suffisamment longtemps pour tromper la victime mais inscrit de sorte qu'il finisse par être entièrement remplacé par le paiement vers soi-même).

La méthode historique pour aboutir à ce type de consensus est « la [preuve de travail](https://fr.wikipedia.org/wiki/Preuve_de_travail) » (proof of work). Cette méthode utilise un problème mathématique dont la solution permet de vérifier que le « mineur » a bien réalisé un travail. Le protocole utilise un système [cryptographique](https://fr.wikipedia.org/wiki/Cryptographie) fondé sur un système décentralisé de preuves : la résolution de la preuve nécessite une puissance de calcul informatique élevée, fournie par les mineurs. Les mineurs sont des entités dont le rôle est d’alimenter le réseau en [puissance de calcul](https://fr.wikipedia.org/wiki/FLOPS), pour permettre la mise à jour de la base de données décentralisée. Pour cette mise à jour, les mineurs doivent confirmer les nouveaux blocs en validant les données. Dans le cas du [bitcoin](https://fr.wikipedia.org/wiki/Bitcoin) et dans le cas d'ajout de blocs à la chaîne, il faut résoudre un problème de cryptographie par [force brute](https://fr.wikipedia.org/wiki/Recherche_exhaustive) pour pouvoir ajouter un nouveau bloc. Selon la « difficulté » de la chaîne au moment de la résolution, celle-ci peut nécessiter de répéter plusieurs centaines de milliards de fois la même opération. Dans le cas du bitcoin, un mineur est uniquement rémunéré pour son travail fourni s'il a été le premier à résoudre le problème cryptographique.

## Gouvernance[[4]](#endnote-4)

1. Il est important de noter que la notion de Loi dans les blockchains ne doit pas être comprise au sens des [lois](https://fr.wikipedia.org/wiki/Loi) législatives (votées par un parlement d'une nation par exemple), mais d'une loi interne au processus de la blockchain, géré par la gouvernance de cette blockchain.
2. La phrase usuelle Code is law régulièrement utilisée comme règle de gouvernance des blockchains ne se réfère donc pas aux lois nationales ou internationale mais uniquement aux « règles de gouvernance » édictées et applicables à la Blockchain.
3. Dans ce cas, ces lois ne sont souvent que des codes et algorithmes informatiques, afin que les règles édictées puissent être vérifiées par les mineurs lors des sessions de vérification des transactions.
4. Toute transaction qui respecte les codes est acceptée dans la blockchain, sinon, la modification est rejetée, sans intervention humaine de la gouvernance (sauf exception).

Plusieurs modes de gouvernance sont possibles :

Un mode « ouvert » (tout le monde peut lire et écrire les registres de la chaîne). Dans ce cas, en règle générale, la loi applicable à la chaîne est la loi ([code algorithmique](https://fr.wikipedia.org/wiki/Code_source)) désignée par les parties.

Un mode « semi-fermé » (seul un organisme central peut écrire, mais l'accès en lecture est plus libre). Cela peut être utilisé pour les fonctions dévolues aux États ([cadastres](https://fr.wikipedia.org/wiki/Cadastre)…) ou aux institutions gérant une donnée sécurisée (traçabilité alimentaire…). Dans ce cas, les règles sont plus libres, l'organisme central ayant la main sur les aspects techniques de validation de la Blockchain.

Un mode fermé (seul un organisme central peut écrire, personne ne peut lire sauf cet organisme). Dans ce cas, l'intérêt réside dans la robustesse théorique et la traçabilité du processus, qui n'a pas besoin d'être (ou ne doit pas être) public, mais qui a besoin de cette sécurité. À noter que dans ce cas, il reste vulnérable à une [attaque des 51 %](https://fr.wikipedia.org/wiki/Attaque_des_51_%25), du fait de la non-décentralisation, et de la non-publication.

Une gouvernance ouverte ne signifie pas pour autant une absence de gouvernance. Dans le cas du Bitcoin, qui représente 50 % de la totalité de la valeur des cryptomonnaies en circulation au [18](https://fr.wikipedia.org/wiki/18_ao%C3%BBt) [août](https://fr.wikipedia.org/wiki/Ao%C3%BBt_2018) [2018](https://fr.wikipedia.org/wiki/2018), la gouvernance est assurée par la communauté, de manière décentralisée. La décentralisation est un apport majeur de la blockchain et par ricochet, des crypto-monnaies. Il y a un wiki (ouvert en 2010, qui contient plus de 1 500 pages au [18](https://fr.wikipedia.org/wiki/18_ao%C3%BBt) [août](https://fr.wikipedia.org/wiki/Ao%C3%BBt_2018) [2018](https://fr.wikipedia.org/wiki/2018)) des forums de discussion IRC consacrés à la gouvernance, à la technique, etc., et même un protocole d'urgence en cas de piratage ou de bug avéré. Bien sûr, ce qui est disponible pour le Bitcoin n'est pas forcément disponible ou applicable pour les autres cryptomonnaies, en particulier les plus récentes et/ou les plus confidentielles.

### Reference

L’intégralité du contenu de ce document provient des sources suivantes :

1. <https://en.bitcoinwiki.org/wiki/Blockchain#/media/File:Blockchain1.jpg> [↑](#endnote-ref-1)
2. <https://fr.wikipedia.org/wiki/Blockchain#Aspects>

   [↑](#endnote-ref-2)
3. <https://fr.wikipedia.org/wiki/Blockchain#Fiabilité> [↑](#endnote-ref-3)
4. <https://fr.wikipedia.org/wiki/Blockchain#Gouvernance> [↑](#endnote-ref-4)