

LES
**BLOCK
CHAINS**

EN **50** QUESTIONS

**Comprendre le fonctionnement
et les enjeux de cette technologie innovante**

Jean-Guillaume **DUMAS**
Pascal **LAFOURCADE**
Ariane **TICHIT**
Sébastien **VARRETTE**

DUNOD

Couverture : EZ Kommunikation et Pierre-André Gualino
Maquette intérieure : Mélissa Jallier-Lundgren

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements

d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour

les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du

Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, 2018
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-077924-6

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2^o et 3^o a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.



Table des matières

Avant-propos

vii

1 Blockchains et technologies de registres distribués **1**

1	Qu'est-ce qu'un registre distribué ?	3
2	Qu'est-ce qu'une blockchain ?	5
3	Quels sont les principaux types de blockchains et de registres distribués ?	9
4	Qui sont les mineurs et que font-ils ?	11
5	Qu'est-ce qu'un consensus ?	15
6	Qu'est-ce qu'une preuve d'autorité ?	23
7	Qu'est-ce qu'une preuve de travail ?	27
8	Qu'est-ce qu'une preuve de participation ?	37
9	Qu'est-ce qu'une cryptomonnaie ?	45
10	Qu'est-ce qu'un porte-monnaie électronique ?	51
11	Qu'est-ce qu'un contrat intelligent ?	55
12	Pourquoi y-a-t-il des scissions au sein des blockchains ?	61
13	Y-a-t-il un standard pour les technologies blockchains ?	67

2 Un exemple concret : le bitcoin **71**

14	Qu'est-ce que le bitcoin ?	73
15	Quel est le lien entre bitcoins et blockchains ?	77
16	Comment payer en bitcoins et éviter les doubles dépenses ?	81
17	Qu'est-ce qu'une cible de hachage dans bitcoin ?	85
18	Comment miner pour valider des transactions bitcoin ?	87
19	Pourquoi le nombre de bitcoins sera-t-il limité ?	93

20	Pourquoi y-a-t-il division de la récompense de minage ?	95
21	Pourquoi y-a-t-il des frais de transaction ?	97
22	Comment tracer les transactions blockchains des criminels ? . . .	101
23	Quelle est l’empreinte énergétique du bitcoin ?	105

3 **Blockchains et cryptomonnaies** **109**

24	Qu’est-ce qu’une monnaie ?	111
25	Comment la monnaie est-elle créée ?	115
26	Les cryptomonnaies sont-elles des monnaies ?	119
27	Que sont les altcoins ?	121
28	Comment la cryptomonnaie Monero garantit-elle le respect de la vie privée ?	131
29	Qu’est-ce que Lightning Network ?	139
30	Quelle est la part des cryptomonnaies dans l’économie mondiale ?	141
31	Quelle est la rentabilité des cryptomonnaies ?	147
32	Comment déclarer ses cryptomonnaies ?	151
33	Les monnaies locales et les cryptomonnaies vont-elles converger ?	153

4 **Utilisations alternatives des blockchains** **157**

34	Qu’est ce qu’une Organisation Autonome Décentralisée ?	159
35	Qu’est-ce que Ethereum ?	163
36	Qu’est-ce qu’une preuve d’espace (Spacemint) ?	175
37	Qu’est ce que IOTA et la structure de donnée Tangle ?	179
38	Peut-on faire une blockchain sans bloc ?	185
39	Peut-on utiliser les blockchains pour gérer des certificats DNS et SSL ?	199
40	Comment créer un revenu universel avec Dunitier ?	207
41	Comment les blockchains vont changer le monde de demain ? . .	211

5	Concepts et outils techniques	219
42	Quels sont les modèles de déploiement des systèmes distribués ou pair-à-pair ?	221
43	Qu'est ce qui caractérise la sûreté de fonctionnement des block-chains ?	223
44	Qu'est-ce qu'une paire de clefs privée/publique ?	229
45	Qu'est-ce qu'une fonction de hachage cryptographique ?	235
46	Qu'est-ce qu'un arbre de Merkle ?	243
47	Qu'est-ce qu'une signature électronique ?	247
48	Qu'est-ce qu'une preuve à divulgation nulle de connaissance ?	253
49	Qu'est-ce qu'une attaque Sybil ?	257
50	Comment programmer une blockchain ?	261
	Annexes	269
	Liste des figures	269
	Liste des tableaux	270
	Liste des abbréviations	271
	Bibliographie	275
	Bibliographie	275
	Index	279

Avant-propos

Après la révolution de l'écriture aux environs de 3 300 avant notre ère, puis la révolution de l'imprimerie par J. Gutenberg aux XV^{ième} siècle, la révolution numérique est en marche. Le monde du XXI^{ième} siècle est en train de basculer pleinement dans l'ère numérique. La société moderne a vu la naissance de l'ordinateur, conçu par A. Turing dans les années 1930, puis développé par J. Von Neumann quelques années plus tard. Les progrès de la physique ont permis une miniaturisation des composants électroniques et une augmentation significative des performances ce qui a engendré l'avènement de l'ordinateur personnel, des *smart phones* et de l'Internet des objets dans notre quotidien.

Les usages changent et profitent de ces progrès technologiques. Il est désormais possible grâce aux avancées en cryptographie moderne de payer sans contact avec une carte bancaire en toute sécurité. Par ailleurs la création de bitcoin en 2009 marque clairement le début d'une nouvelle étape. Cette invention est remarquable et visionnaire à plusieurs titres.

Les chercheurs se sont intéressés à la dématérialisation de la monnaie dès le début des années 80 avec le premier article de D. Chaum¹. Par la suite, celui-ci a créé la société DigiCash pour promouvoir une monnaie dématérialisée qui n'a pas connu le succès escompté et qui a déposé le bilan en 1998. À cette époque notre société n'était peut être pas encore prête pour ce changement. Mais surtout cette monnaie numérique reposait comme toutes les suivantes sur une autorité de confiance qui crée les pièces digitales et assure les échanges entre les utilisateurs. À l'inverse, l'innovation majeure de bitcoin est la possibilité de créer et d'utiliser de manière décentralisée une monnaie sans autorité de confiance. Pour cela chacun peut vérifier le bon déroulement de la création monétaire.

L'autre grande innovation est le mécanisme de la blockchain qui est au cœur de bitcoin. Ce mécanisme permet d'enregistrer de manière distribuée des informations dans un registre irréversible et vérifiable par tout le monde. Ainsi chacun peut, en observant la blockchain, vérifier quel numéro de compte a créé des bitcoins. Ce mécanisme accentue la confiance des utilisateurs dans ce système que personne ne contrôle vraiment totalement.

1. Chaum, David (1983), « Blind signatures for untraceable payments ». *Advances in Cryptology Proceedings*. 82 (3) : 199-203.

Par ailleurs, l'utilisation de la blockchain a permis de faciliter les échanges de bitcoins entre les utilisateurs sans autorité centrale de confiance. Ce changement de paradigme rend le bitcoin utilisable sur smartphone via Internet. De plus, cela le rend aussi inarrêtable, ceci tant que des personnes consacreront de l'énergie pour valider les transactions effectuées avec la blockchain.

Une fois cette innovation découverte, la société et les citoyens du monde moderne ont pris conscience de l'immense potentiel offert par cette nouvelle technologie. Après l'avènement de la cryptomonnaie bitcoin et son essor extraordinaire, de nombreuses autres applications utilisant le principe des blockchains voient le jour et vont révolutionner le monde de demain.

L'objectif de cet ouvrage, construit en 50 questions, est dans un premier temps de faire comprendre comment fonctionnent les technologies de registres distribués et les blockchains. Le second objectif est d'expliquer comment ces innovations peuvent apporter de nouvelles perspectives à ce monde dématérialisé dans lequel la sécurité et la confiance sont des éléments essentiels.

La première partie de cet ouvrage aborde donc les grands principes fondateurs des blockchains. Dans la seconde partie, l'exemple historique et incontournable de bitcoin est présenté de manière pédagogique afin de comprendre les origines des blockchains. Plus généralement, les innovations liées aux différentes cryptomonnaies sont présentées dans la troisième partie, avec leur impact économique. La quatrième partie explore le potentiel novateur des blockchains en tant que technologie de rupture. Enfin la dernière partie revient sur les outils et concepts techniques utiles à la compréhension détaillée des mécanismes sous-jacents aux blockchains.

Les auteurs remercient chaleureusement Benoît Bertholon, Pascal Bouvry, Xavier Bultel, Stenzel Cackowski, Amrit Kumar, Harold Mertzweiller, Jérémy Picot, Paul Pinault, Étienne Roudeix, Pascal Sygnet, Alexis Violland et Vincent Xuereb pour leurs contributions à l'élaboration du contenu de ce livre. Les auteurs expriment également leur gratitude à Jean-Luc Blanc, Matthieu Giraud et Vincent Mazenod et pour leurs commentaires et suggestions de modifications constructifs, suite à leurs relectures assidues.

Grenoble, Clermont-Ferrand, Luxembourg, 24 juillet 2018.

Jean-Guillaume Dumas,

Pascal Lafourcade,

Ariane Tichit,

Sébastien Varrette.

1

Blockchains et technologies de registres distribués

The St Lawrence Starch Company Limited				Incorporated by Letters Patent under "The Companies Act"			
Capital Stock				in 500 Shares of \$100 each.			
Subscribed				Liability			
First Issue of 400				Shares \$40,000			
<p>For the purposes of this certificate in the Capital Stock of the St Lawrence Starch and Ice Co. Ltd. the following persons and their shares are listed as to be in - the first issue of 400 shares in such amount and amount as by the is determined.</p>				<p>For the number of shares set opposite the respective names Company (limited) and its do hold for himself and family to pay the full amount of the said shares as shown in this stock book and the balance at such time as the Board of Directors of the said Company may</p>			
Date	Subscribers	Shares	Residence	No. of shares	Balance	Debit	Amount
1889							
Sept	29	Robert Kilgus	Toronto	100	100.00		100.00
Nov	29	Carl Kilgus	Toronto	100	100.00		100.00
Dec	29	Joseph Kilgus	Toronto	100	100.00		100.00
Dec	31	John Paul	Cardinal	100	100.00		100.00
	5	John Paul	Cardinal	100	100.00		100.00

Figure 1.1 – Extrait d'un registre de souscriptions et transactions d'actions, 1889. Documents corporatifs officiels de St. Lawrence Starch Company. Archives publiques de l'Ontario.

1

Qu'est-ce qu'un registre distribué ?

La notion de *registres* (*ledger* en anglais) est au cœur du commerce depuis des temps anciens et l'écriture semble avoir été inventée il y a 5 500 ans par les commerçants sumériens au Proche-Orient pour permettre leur comptabilité. Les registres servent à enregistrer des *transactions* financières ou administratives de façon pérenne. De plus, il est souhaitable qu'il soit impossible de modifier les transactions enregistrées dans le registre, ou du moins que toute modification soit clairement identifiable. Après les tablettes d'argile, le papyrus puis le papier furent utilisés comme support pour l'écriture et l'archivage de ces transactions. La confiance dans un registre s'appuie sur un principe de **garantie** incarné par une institution centralisée (un État ou une banque).

Évidemment, le papier n'est pas le meilleur support pour offrir une fiabilité et une inviolabilité à toute épreuve. L'avènement de la cryptographie moderne a permis l'élaboration et le développement des technologies de registres distribués ou *Distributed Ledger Technology (DLT)*, qui sont une version digitale des registres et qui offrent un certain nombre de garanties qui n'étaient auparavant pas envisageables avec un support papier et une gestion centralisée, fut-ce par une institution étatique.

Une DLT est donc une technologie qui définit une **base de données de transactions, transparente, sécurisée et décentralisée (sans organe de contrôle central), distribuée sur tout ou partie des nœuds d'un réseau, qui enregistre et stocke dans des registres (ou blocs) virtuels et de façon immuable chaque transaction qui se produit dans le réseau.**

Parmi les innovations principales qui caractérisent les DLT, il faut retenir que :

- ▶ chaque enregistrement (transaction) du registre est vérifié et enregistré cryptographiquement à travers l'utilisation de **clefs de chiffrement** et de signatures électroniques (cf. question **47**) et ne peut être inversé, modifié ou répudié, créant ainsi un historique irrévocable et vérifiable des transactions ;
- ▶ la gestion du registre est **décentralisée** et fonctionne sans organe de contrôle ni stockage centralisé ;

- ▶ le registre est **distribué et répliqué** sur plusieurs sites, pays, ou institutions. L'ensemble des participants du réseau peut avoir sa propre copie identique du registre. De même, chaque partenaire impliqué dans l'une des transactions enregistrées dans ce registre dispose d'une copie de ce registre. Enfin, chaque événement répertorié est vérifiable de façon privée ou publique (selon le type de registre considéré) ;
- ▶ la synchronisation des données est **automatisée** : tout changement est répercuté « en temps réel » pour chaque copie du registre et cela sur tous les nœuds où elle est stockée. Cela suppose en général la mise en place d'un algorithme de *consensus* assurant que le contenu de chaque transaction est le même entre les parties.

Ainsi, la caractéristique majeure des DLT est de fournir des transactions en ligne sécurisées, fiables, sans intermédiaire et non répudiables, entre les parties. En particulier, l'ensemble des enregistrements d'une DLT doit être *vérifiable* et *auditable*.

À noter que la distribution des données sur plusieurs nœuds du réseau, inhérente aux concepts des DLT n'implique pas que chacun d'entre eux stocke exactement le même état du registre, bien que cela puisse être le cas (cf. question **5**). Cela n'implique pas non plus que chaque partie qui participe au registre distribué ait accès à toutes les transactions : un contrôle d'accès est tout à fait envisageable.

Dans tous les cas, le concept de DLT a émergé avec l'introduction des **blockchains** en 2008, et le lancement de la cryptomonnaie bitcoin (cf. question **14**). C'est cette structure de données qui est maintenant introduite.

2

Qu'est-ce qu'une blockchain ?

Au plus fort de la crise économique qui toucha le monde en 2008, une nouvelle façon de concevoir la monnaie a été proposée au sein d'un article posté sur internet et intitulé « *Bitcoin : A Peer-to-Peer Electronic Cash System* » [42]. Dans cet article, un certain Satoshi Nakamoto décrivait un nouveau système d'émission et de gestion d'unités monétaires, appelé *bitcoin*, qui reposait sur une structure de données de type DLT et appelée *blockchain*.

Par analogie avec les registres classiques dans lesquels les transactions sont regroupées sur des pages, les transactions sont ici agrégées au sein de *blocs* digitaux chaînés entre eux, d'où le terme de blockchains qui sera utilisé dans la suite de cet ouvrage pour désigner une chaîne de blocs. Dans cette structure de données, les transactions *confirmées* (où validées) sont intégrées dans des blocs bénéficiant d'un identifiant « unique » dépendant de son contenu, une signature (cf. question **47**) qui est obtenue par une empreinte de hachage (cf. question **45**). Chaque bloc contient la signature du bloc précédent de la chaîne, ce qui permet de garantir l'intégrité de l'ensemble des enregistrements et des données de la blockchain depuis le premier bloc (appelé bloc « *Genesis* »).

Les mineurs valident les transactions

Lorsqu'une nouvelle transaction est émise pour être validée, elle est propagée parmi les participants pour entrer dans un ensemble de transactions *non confirmées*. Celles-ci seront choisies pour intégrer un nouveau bloc construit par un *mineur* (cf. question **4**). Les mineurs valideront ces transactions selon des techniques dépendant du type de blockchain¹. Cette orchestration est illustrée dans la figure 2.1. Chaque bloc ne contient pas forcément un nombre fixe de transactions. Une fois validé, un bloc est horodaté et ajouté à la blockchain. Cet horodatage n'est pas forcément nécessaire, car l'ordre des blocs n'est pas nécessairement chronologique (cf. question **5**), mais reste pratique. La valeur

1. Par exemple, dans la blockchain utilisée au sein du bitcoin, cette technique est appelée la preuve de travail ou « *Proof-of-Work (PoW)* » (cf. question **7**), et consiste à résoudre des problèmes algorithmiques qui seront explicités dans la partie 2 de cet ouvrage.

proposée est alors celle de l'horloge locale (*timestamp* Unix typiquement) du mineur. Au moment de la vérification du bloc, il est suffisant de s'assurer que la valeur du timestamp reste cohérent avec les autres temps de la blockchain¹. Il existe plusieurs modèles de déploiement de ce type de structure (cf. question **42**). Mais c'est une implémentation distribuée au-dessus d'un réseau Peer-to-Peer (P2P) comme celle proposée dans l'article fondateur de bitcoin [42] qui permet d'obtenir un DLT tel que défini précédemment. Ainsi, chaque nœud du réseau possède et maintient une copie cohérente et identique de la blockchain. Il convient alors de définir les mécanismes décentralisés permettant de :

1. distribuer de nouveaux blocs à tous les nœuds impliqués ;
2. valider les transactions et plus généralement les blocs ;
3. assurer la cohérence éventuelle de toutes les copies de la blockchain.

Ces mécanismes sont explicités par la suite et dépendent évidemment du système considéré. Mais en les supposant en place, une blockchain constitue alors une **base de données publique, distribuée**, c'est-à-dire partagée par ses différents utilisateurs, **sans autorité centrale, fiable et inviolable**. Ainsi elle peut être assimilée à un grand livre des comptes, *public, infalsifiable* et *vérifiable*.

La blockchain est infalsifiable : toute modification d'un bloc de transactions dans la chaîne rend celle-ci incohérente. En effet, tout bloc est référencé dans le bloc suivant de la chaîne, lui-même référencé dans le bloc suivant, etc. Cette référence est entièrement déterminée par le contenu du bloc et totalement différente pour chaque variation, même infime : ceci est assuré par l'usage d'une empreinte de hachage cryptographique de ce bloc (cf. question **45**). Pour altérer une partie de la chaîne il faudrait donc être capable d'altérer la totalité des blocs à partir de la modification, et cela tellement rapidement que l'ensemble du réseau mondial (qui scrute, vérifie et augmente la chaîne constamment) ne puisse s'en apercevoir.

Les raisons du succès des blockchains

Les technologies de type blockchain sont devenues populaires avec le succès grandissant de bitcoin et le développement d'autres systèmes tels que par exemple Ethereum (cf. question **35**), Ripple, ou Litecoin (cf. question **27**). De par son importance, une partie complète de cet ouvrage est dédiée à bitcoin (cf. partie 2) tandis que les schémas alternatifs sont explicités séparément dans la partie 3. Néanmoins, cette technologie ne se limite pas seulement au domaine économique et monétaire. L'utilisation de la blockchain se répartit en trois cas, détaillés dans la partie 4 :

1. voir par exemple https://en.bitcoin.it/wiki/Block_timestamp.

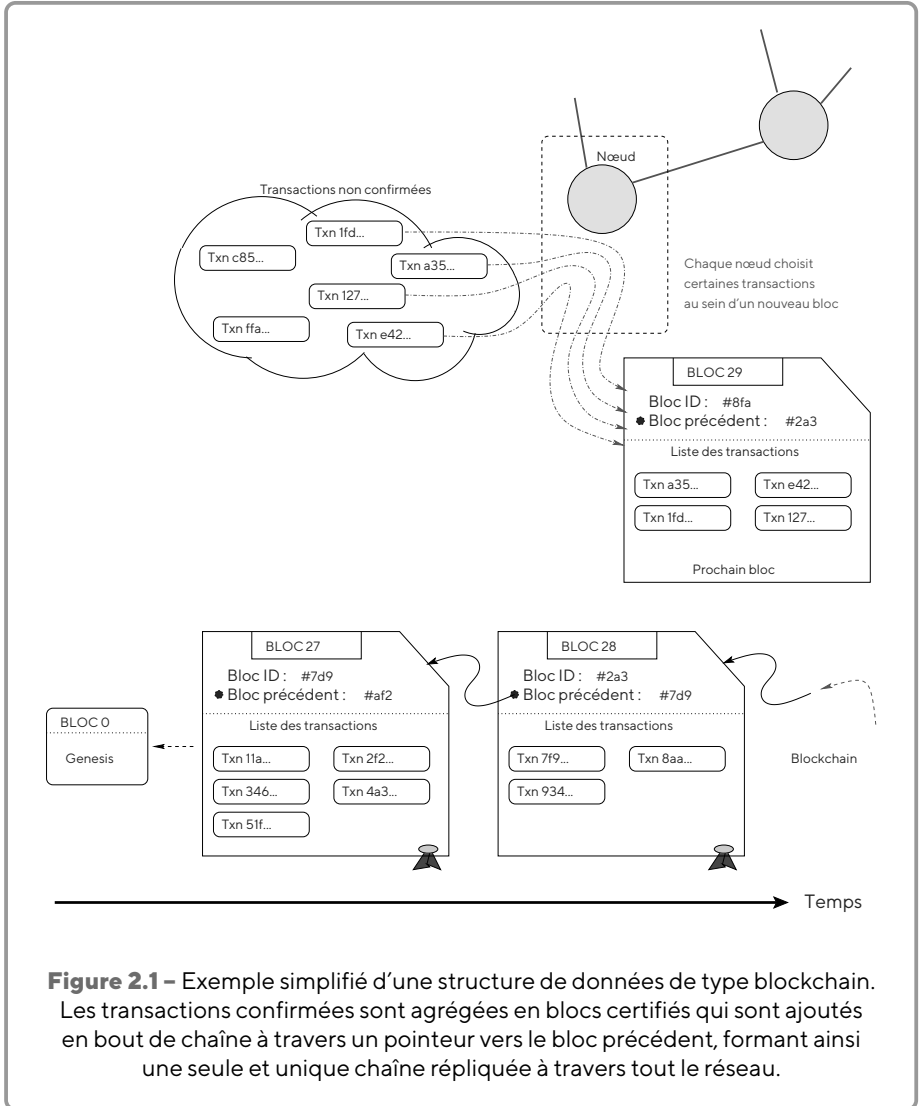


Figure 2.1 – Exemple simplifié d’une structure de données de type blockchain. Les transactions confirmées sont agrégées en blocs certifiés qui sont ajoutés en bout de chaîne à travers un pointeur vers le bloc précédent, formant ainsi une seule et unique chaîne répliquée à travers tout le réseau.

1. les applications pour le transfert d'actifs, dans le cadre d'une utilisation monétaire via les cryptomonnaies (cf. question **9**), des titres, des actions ou des obligations ;
2. les applications de la blockchain en tant que DLT, assurant ainsi une meilleure traçabilité des produits et des actifs ;
3. les *smart contracts* (cf. question **11**) *i.e.*, des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

Principaux DLT qui ne sont pas des blockchains

Il existe des systèmes DLT qui ne reposent pas à proprement parler sur des *blockchains*. À titre d'exemple :

- ▶ *Corda*¹ émane d'un consortium d'instituts financiers de régulation comprenant plus de 70 des principales banques et assureurs de par le monde. Ce DLT est conçu pour enregistrer, gérer, et synchroniser les agréments légaux du secteur financier et améliorer l'interopérabilité des firmes associées. *Corda* partage de nombreux attributs des blockchains pour des consortium d'entreprises mais repose sur un concept de changements d'état et de transactions au lieu de blocs chaînés. En outre, des notaires sont introduits et remplissent essentiellement la fonction de mineurs qui valident les transactions, mais sans la surcharge d'exécution des algorithmes coûteux de preuve de travail (PoW).
- ▶ *IOTA*² est un DLT proposant une cryptomonnaie (cf. question **9**) appelée *MIOTA*. Cette cryptomonnaie est dédiée à une utilisation dans l'Internet des objets (Internet of Things (IoT)). À la place d'une simple chaîne, *IOTA* utilise comme structure de données décentralisée une chaîne avec des ramifications, c'est-à-dire un graphe orienté sans cycle, ou *Direct Acyclic Graph (DAG)*, appelé *Tangle* (cf. question **37**). Pour pouvoir supporter des micro-transactions, chaque nœud du graphe est une transaction (et non un bloc).

Le délai de confirmation des transactions est rapide mais ne suppose pas forcément un parcours complet du graphe, et le nombre de transactions simultanées pouvant être gérées par le système est illimité.

- ▶ Dans la même veine, *Hashgraph* et *Nano* sont deux autres exemples de DLT reposant sur un DAG et non pas sur des blocs chaînés ; ils sont étudiés dans la question **38**.

1. <https://www.corda.net/>

2. <https://iota.org/>

3

Quels sont les principaux types de blockchains et de registres distribués ?

Le tableau 3.1 montre les différents types de blockchains.

	Type de blockchain		
	Publique	Consortium	Privée
Accès (en général)	<i>Permissionless</i> Anonyme & Publique	<i>Permissioned</i> Identifié & Autorisé	<i>Permissioned</i> Identifié & Autorisé
Gestion	Décentralisée	Partagée au sein de plusieurs organisations	Centralisée
Exemple	Bitcoin, Ethereum, Dashcoin, Monero, Litecoin, Dogecoin ...	R3 (Banques), EWF (Energie), B3i (Assurance) ...	MONAX, Multichain ...
Sécurité, Consensus	Preuve de travail (PoW) Preuve de participation (PoS) Preuve de récupérabilité (PoR) Accord byzantin (BA) ...	Preuve d'autorité (PoA) Preuve de participation déléguée (DPoS) Tolérance aux fautes (<i>Practical BFT</i>) ...	

Tableau 3.1 – Les principaux types de blockchains.

Les blockchains publiques

Les *blockchains publiques* sont par définition ouvertes et accessibles à tous. En particulier, tout le monde peut participer aux transactions (et ainsi espérer les voir incluses dans la blockchain sous réserve de validité), mais aussi collaborer aux opérations de *consensus* de la blockchain permettant de déterminer quel bloc peut être ajouté à la chaîne et à l'état courant (cf. question 5), et cela sans besoin d'une autorisation particulière de la part d'une autorité de contrôle (éventuellement distribuée). En particulier, une blockchain publique peut être assimilée à un grand livre comptable public et infalsifiable.

Enfin, de telles blockchains sont souvent *permissionless* : les nœuds comme les utilisateurs n'ont pas besoin d'autorisation ni d'être authentifiés.

Les blockchains privées et de consortium

L'autre grand type de blockchains est celui des *blockchains privées* dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs qui, par ailleurs, ne se font pas nécessairement entièrement confiance. Ici, il convient de dissocier les blockchains **complètement privées**, dans lesquelles les droits d'écriture sont restreints et centralisés au sein d'une seule institution, des **blockchains de consortium** où le processus de consensus est contrôlé par un sous-ensemble de nœuds et de participants pré-sélectionnés (selon une approche centralisée ou non) et disposant ainsi d'un rôle privilégié pour la gestion de la blockchain.

Dans les deux cas, l'accès en lecture de la blockchain peut être entièrement public ou restreint, que ce soit au niveau des participants ayant été autorisés ou du nombre de requêtes effectué. Éventuellement, certains systèmes permettent de limiter l'accès aux preuves cryptographiques à seulement une partie de la blockchain. Enfin et de façon générale, une blockchain privée est dite **permissioned**, si les nœuds du réseaux, tout comme les utilisateurs, sont authentifiés et autorisés selon des critères prédéfinis, comme sur la figure 3.1.

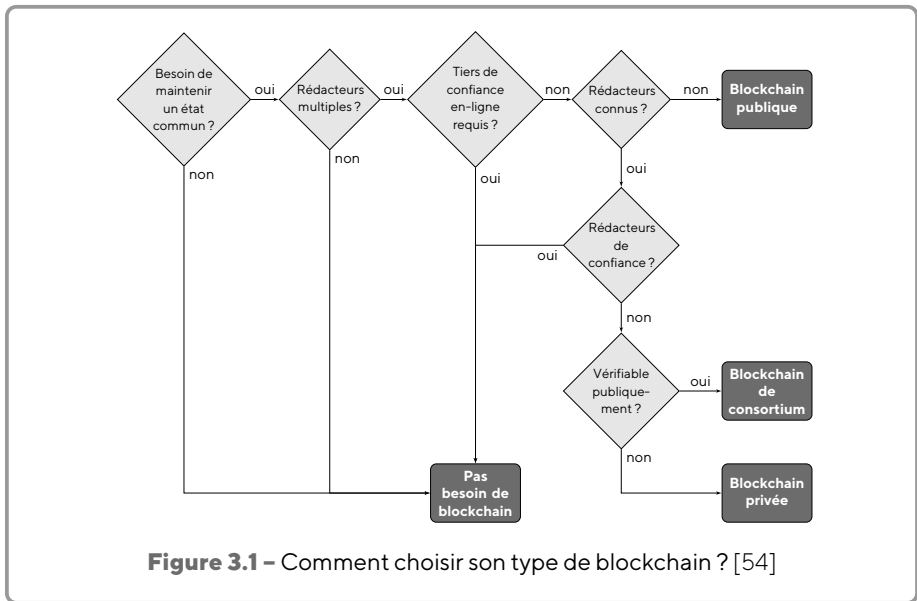


Figure 3.1 – Comment choisir son type de blockchain ? [54]

4

Qui sont les mineurs et que font-ils ?

La question **2** a permis de présenter de façon générale les différents composants d'une blockchain. Pour les blockchains dites *permissionless* (cf. question **3**), toute ressource de calcul (ordinateur, smartphone, dispositif IoT etc.) qui exécute le logiciel de la blockchain est considéré comme un nœud participant à la blockchain. Organisé au sein d'un réseau P2P (cf. question **42**), ce logiciel définit les protocoles permettant de communiquer et de diffuser les informations (notamment les blocs et les transactions à confirmer) et s'accompagne d'un rôle que chaque nœud peut choisir d'endosser ou non :

- ▶ **observateur** : accès aux transactions, mais sans pouvoir les modifier ;
- ▶ **wallet** : création de nouvelles transactions au moyen d'un porte monnaie électronique – *wallet* en anglais (cf. question **10**) ;
- ▶ **nœud simple (lightweight node)** : vérification et diffusion des transactions à travers le réseau, mais sans maintenir une copie locale de la blockchain. Ce type de nœud est particulièrement adapté aux ressources disposant de capacités de calcul et/ou de stockage limitées ;
- ▶ **nœud complet (full node)** : vérification et diffusion des transactions via le réseau, tout en maintenant une copie locale cohérente de la blockchain ;
- ▶ **mineur** : nœud complet qui participe à la construction et donc à la publication de nouveaux blocs.

Comme précisé dans la figure 2.1 page 7, toute nouvelle transaction est diffusée sur le réseau pour entrer dans un ensemble de transactions *non confirmées*. Ces transactions non confirmées sont stockées par les mineurs en attendant leur vérification et leur intégration éventuelle au sein d'un nouveau bloc. Ainsi le rôle du mineur est d'utiliser sa capacité de calcul informatique pour :

1. *vérifier les transactions* en attente au sein de l'ensemble des transactions non confirmées et intégrer celles qui sont valides au sein de nouveaux blocs soumis aux autres nœuds du réseau. Un mineur a tout intérêt à effectuer ces opérations de vérifications car aucun autre nœud du réseau n'acceptera un bloc comportant des transactions invalides ;

- participer à la gestion et à la surveillance de la cohérence de la blockchain en *vérifiant les blocs* reçus comme nouveau maillon de la chaîne et en rejetant les blocs invalides.

La confirmation d'une transaction consiste à s'assurer que l'opération est correctement signée cryptographiquement par chaque partie (cf. question **47**). En outre, dans le cadre d'une cryptomonnaie, il s'agit de vérifier que l'émetteur de la transaction dispose bien des fonds nécessaires pour satisfaire la dépense mentionnée. Pour cela, il « suffit » de remonter l'intégralité de la blockchain jusqu'au premier bloc *genesis* et retracer l'historique des transactions antérieures qui affectent le compte de l'émetteur pour laisser un solde d'un montant au moins égal à la somme à régler.

Méthodes de consensus

Certaines blockchains nécessitent une forme de sacrifice pour ajouter le bloc suivant et ainsi limiter des attaques par déni de service ou autres abus consistant à *spammer* le réseau avec de nouveaux blocs. L'idée est de faire en sorte que la création de blocs valides soit difficile, par exemple en rendant cette opération très gourmande en ressources de calcul, il s'agit alors d'une preuve de travail ou *Proof-of-Work (PoW)* (cf. question **7**), ou en nécessitant d'apporter la preuve de la possession d'une certaine quantité de cryptomonnaie, par preuve de participation ou *Proof-of-Stake (PoS)* (cf. question **8**). De plus, il existe de nombreuses autres stratégies de consensus. Elles sont décrites dans la question **5**.

Minage et preuve de travail (PoW)

L'approche par preuve de travail est la méthode historique utilisée pour la monnaie bitcoin pour aboutir à un consensus dans la blockchain quant à l'ajout d'un bloc. Le terme « mineur » vient d'ailleurs de l'analogie avec les chercheurs d'or qui creusaient les mines au prix d'efforts intensifs pour espérer trouver une pépite. En effet, pour pouvoir créer un bloc valide dans une blockchain de type bitcoin, il faut résoudre un problème mathématique très complexe, dont la solution ne peut être trouvée que par force brute, c'est-à-dire en testant au hasard des solutions jusqu'à en trouver une ayant la propriété voulue.

Il est inutile de pousser plus loin la description des preuves de travail qui couvrent un spectre extrêmement large d'activités – ce modèle de consensus est en effet détaillé dans la question **7**. Dans tous les cas, le minage d'un nouveau bloc relève donc de deux facteurs :

- ▶ La puissance de calcul du mineur.
- ▶ La chance, puisqu'il est possible de trouver une solution en quelques secondes ou en plusieurs dizaines de minute. C'est cela que le temps moyen de création d'un bloc est en pratique variable.

Pour s'adapter à l'augmentation de la puissance de calcul des mineurs, il est prévu que la difficulté des problèmes mathématiques à résoudre augmente ou diminue en fonction des besoins pour maintenir un temps moyen entre chaque nouveau bloc miné statistiquement constant, 10 minutes pour bitcoin (cf. question **18**), 12 secondes pour Ethereum (cf. question **35**).

Rémunération des mineurs

Pour son travail, le mineur d'une blockchain à vocation monétaire telle que bitcoin est rémunéré de deux façons :

1. Toute monnaie prévoit un processus de création monétaire. Dans le cas des cryptomonnaies (cf. question **9**), c'est généralement au minage que la masse monétaire est augmentée. Ainsi, le mineur va créer de la monnaie à chaque nouveau bloc, dont il sera le premier propriétaire. Et il sera d'autant plus « indemnisé » que son bloc sera choisi par consensus (cf. question **5**) comme nouveau bloc de tête de la chaîne. Cette récompense de création évolue au cours du temps et définit une succession d'*ères de récompenses* (cf. question **19**).
2. Les utilisateurs du système monétaire ont la possibilité d'associer à leurs transactions des frais de commission (cf. question **21**). Si ces rémunérations complémentaires sont facultatives et peuvent être fixées librement par l'émetteur d'une transaction, elles permettent d'inciter un mineur à traiter en priorité une transaction intégrant des frais de commission élevés (parmi toutes celles restant à confirmer) dans la mesure où elle sera plus lucrative pour lui si le bloc qu'il proposera pour compléter la blockchain est choisi. Au niveau de bitcoin, et bien que ces frais de transaction étaient envisagés dès le début dans l'article original de Satoshi Nakamoto (voir [42] §.6), ces commissions n'ont joué pratiquement aucun rôle jusqu'en 2016 et l'avènement d'une nouvelle ère de récompense dans bitcoin (voir le tableau 19.1 page 94). Puis progressivement, elles ont acquis de l'importance et sont appelées à devenir incontournables dès lors qu'il n'y aura plus de nouveaux bitcoins à créer (cf. question **19**) – ces commissions seront la seule façon de garantir une rémunération aux mineurs.

Ce double système assure qu'il existe et existera toujours des volontaires, les mineurs, pour continuer de participer à la gestion de la blockchain ainsi qu'à la surveillance des autres mineurs.

5

Qu'est-ce qu'un consensus ?

Se faire confiance sans confiance

L'une des caractéristiques essentielles des blockchains est d'assurer la cohérence des copies du registre distribué construites indépendamment par un grand nombre d'acteurs (les nœuds du réseau) n'ayant a priori aucune raison de se faire confiance, ni même de collaborer. Dans un tel contexte, les blockchains reposent sur un algorithme de *consensus* permettant de s'accorder sur l'état et donc l'ordre des blocs de la chaîne, une propriété primordiale pour assurer la cohérence des transactions et éviter les doubles dépenses dans le cadre des cryptomonnaies (cf. question **16**).

La problème vient du fait que les communications dans un réseau P2P (cf. question **42**) ne sont pas instantanées. Ainsi certains nœuds du réseau peuvent être temporairement isolés, ce qui peut conduire à l'apparition de blockchains concurrentes émanant de l'ajout de blocs différents, par des nœuds n'ayant pas conscience l'un de l'autre. De telles duplications sont rares, mais se produisent parfois. En outre, rien n'exclut qu'une part des utilisateurs ne cherche à corrompre la blockchain en envoyant des informations erronées ou malveillantes, par exemple pour tenter d'enregistrer des transactions illégales.

En pratique, ce problème est connu depuis longtemps [37] sous le nom de « problème des généraux byzantins » (*Byzantine Generals' Problem (BGP)*). Il s'agit d'une métaphore historique qui traite de la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs dans un réseau distribué (voir encadré ci-après). L'analyse de ce problème est fondamentale pour l'étude de la sûreté et de la tolérance aux pannes des systèmes distribués (cf. question **43**). Les fautes dites *byzantines* voient d'ailleurs leur nom tiré de cette analyse et caractérisent un comportement arbitraire erroné, éventuellement malveillant, qui peut s'avérer transitoire ou définitif. C'est précisément de cette façon qu'il convient de modéliser les nœuds du réseau et les utilisateurs de la blockchain dont le comportement dévie du protocole attendu. Ainsi, toute approche tolérante aux fautes byzantines (*Byzantine Fault Tolerance (BFT)*) en