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

LES BLOCK CHAINS

EN 50 QUESTIONS

–

Comprendre le fonctionnement et les enjeux de cette technologie

2e édition

DUNOD

Couverture : Studio Dunod

© Dunod, 2022
11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-083450-1

Table des matières

Avant-propos

Après la révolution de l'écriture aux environs de 3 400 avant notre ère, puis la révolution de l'imprimerie par J. Gutenberg au XV^{e} siècle, la révolution numérique est en marche. Le monde du XXI^{e} 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 1980 avec le premier article de D. Chaum *. 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

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

des bitcoins. Ce mécanisme accentue la confiance des utilisateurs dans ce système que personne ne contrôle vraiment totalement.

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 deuxième 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, 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, Olivier Blazy, Matthieu Giraud, Frédéric Hayek et Vincent Mazenod pour leurs commentaires et suggestions de modifications constructifs, à la suite de leurs relectures assidues.

Grenoble, Clermont-Ferrand, Luxembourg, 6 mai 2022.
Jean-Guillaume Dumas, Pascal Lafourcade,
Ariane Tichit, Sébastien Varrette.

1

Blockchains et technologies de registres distribués

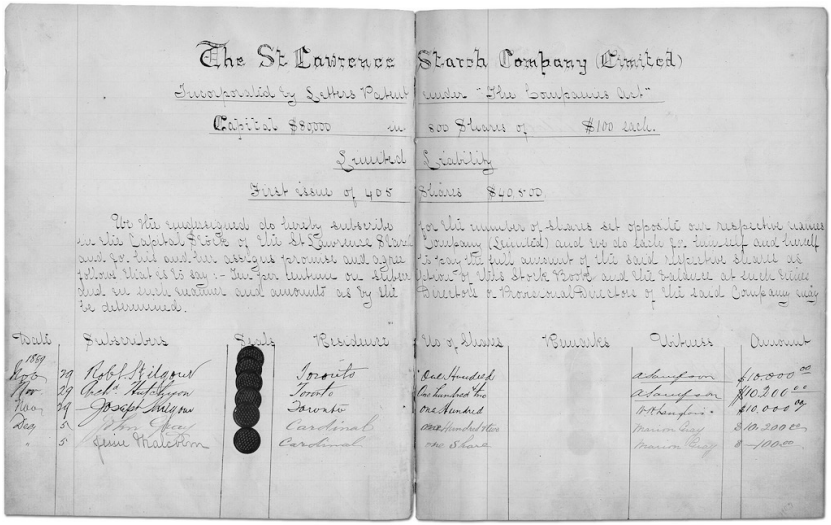

Figure 1.1 – Extrait d'un registre de souscriptions et transactions d'actions, 1889. Documents corporatifs officiels de St. Lawrence Starch Company. Archives publiques de l'Ontario.

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 environ 5 400 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**). En particulier, toute inscription sur le registre 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*. C'est ce qui fait la force de ce paradigme.

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 (*cf.* question **3**). 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* » [43]. 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* (ou 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 **46**). 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 blockchain ◇. 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 block-

* Une empreinte de hachage permet d'obtenir à partir de n'importe quelle entrée une sortie de taille fixe (*cf.* question **46**). Une telle empreinte seule ne permet pas de revenir au message initial.

◇ 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.

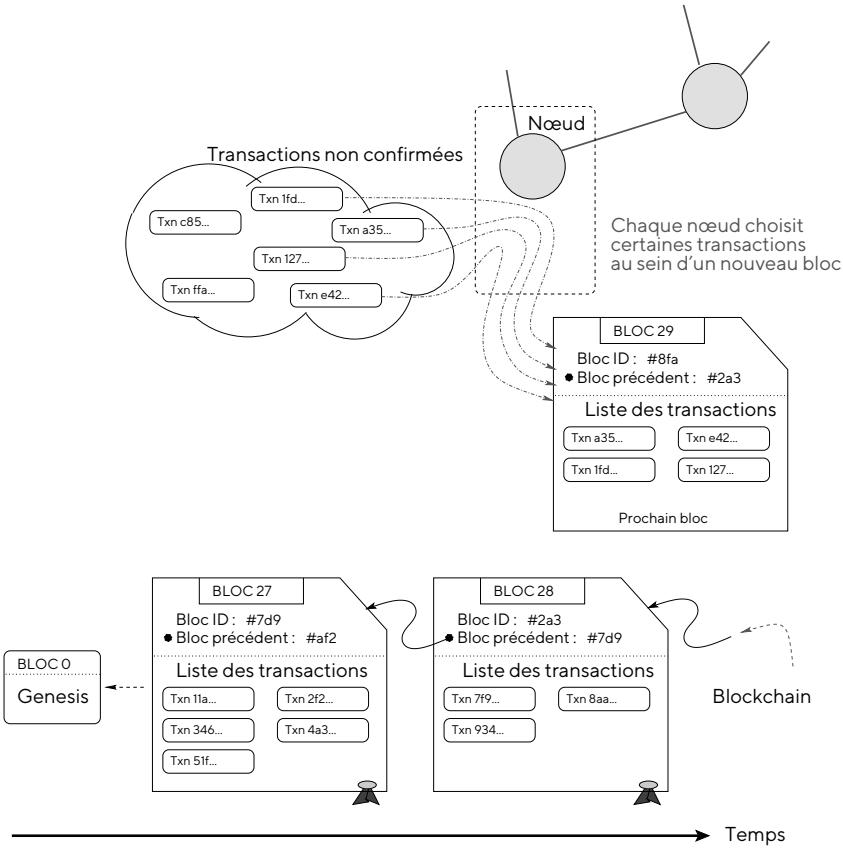

Figure 2.1 – Exemple simplifié d'une structure de données de type blockchain. Les transactions confirmées sont agrégées en blocs certifiés qui sont ajoutés en bout de chaîne à travers un pointeur vers le bloc précédent, formant ainsi une seule et unique chaîne répliquée à travers tout le réseau.

chain. Cet horodatage n'est pas forcément nécessaire puisque l'ordre des blocs n'est pas nécessairement chronologique (*cf.* question **5**), mais cela reste pratique. La valeur 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 cohérente avec les autres temps de

la blockchain * Il existe plusieurs modèles de déploiement de ce type de structure (*cf.* question **44**). Mais c'est une implémentation distribuée avec un réseau Peer-to-Peer (P2P) comme celle proposée dans l'article fondateur de bitcoin [43] qui permet d'obtenir un véritable DLT. Ainsi, chaque nœud du réseau possède et maintient une copie cohérente et identique de la blockchain. Il est alors nécessaire 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 car toute modification d'un bloc de transactions dans la chaîne rend celle-ci incohérente : 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 **46**). 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 de bitcoin et le développements d'autres systèmes tels que Ethereum (*cf.* question **35**), Ripple, ou Litecoin (*cf.* question **27**). À travers 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 au domaine économique et monétaire. L'utilisation de la blockchain se répartit en trois cas, détaillés dans la partie 4 :

*voir par exemple : `en.bitcoin.it/wiki/Block_timestamp`.

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 une meilleure traçabilité des produits et des actifs ;
3. les contrats intelligents (*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* * émane d'un consortium d'instituts financiers de régulation comprenant plus de 70 des grandes banques et assureurs à travers 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 consortiums 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 ◇ 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**.

*www.corda.net
◇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)	*Permissionless* Anonyme & Publique	*Permissioned* Identifié & Autorisé	*Permissioned* 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, Multi-chain ...
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 (*Practical BFT*) ...	

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.

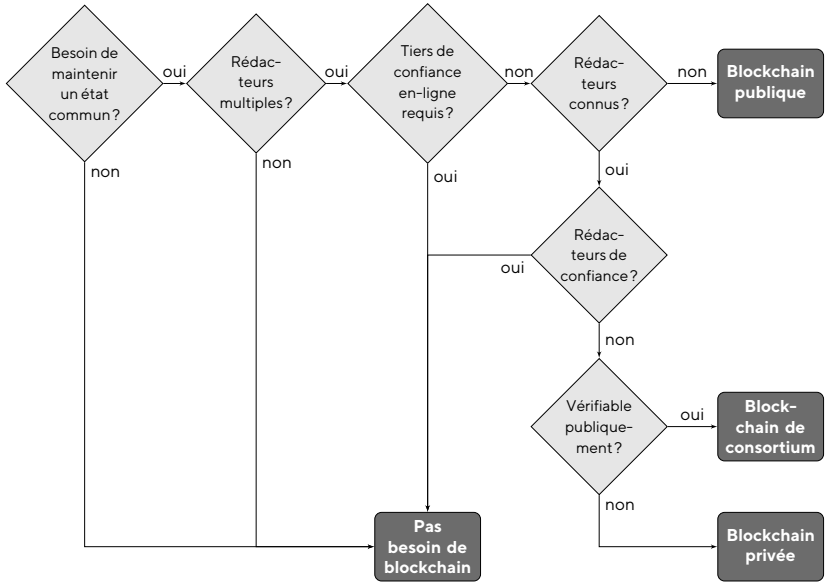

Figure 3.1 – Comment choisir son type de blockchain ? [55]

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 **44**), 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 :** il permet la création de nouvelles transactions au moyen d'un portefeuille – *wallet* en anglais –, ou porte-monnaie, électronique (*cf.* question **10**) ;
- **nœud simple** (*lightweight node*) : il fait la 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 6, 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 les 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 ;

2. 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 l'historique de la blockchain jusqu'au premier bloc, appelé *genesis*, et retracer les 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 faire en sorte que la création de blocs valides 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 rendant nécessaire 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**).

Il existe de nombreuses autres stratégies de consensus qui 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 en 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 ou 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 aient été envisagés dès le début dans l'article original de Satoshi Nakamoto (voir [43] §.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 93). 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**).

Le problème vient du fait que les communications dans un réseau P2P (*cf.* question **44**) 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 [38] 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 **45**). 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 anglais) offre une base pour un modèle de consensus pour les blockchains.

En outre, la mise en place d'un consensus pour des registres distribués suit quelques règles simples :

- D'abord, et dans la mesure où il est impossible de se fier aux autres pairs du réseau, il est vital que toute nouvelle information soit revue et confirmée avant d'être acceptée.

- Ensuite, lorsqu'un utilisateur rejoint une blockchain, il ne doit faire confiance qu'à l'état initial du système, c'est-à-dire celui publié dans le seul bloc préconfiguré et propre à chaque blockchain, le bloc *genesis* (voir Figure 2.1 page 6).

Ainsi, l'ajout de nouveaux blocs s'effectue à travers une stratégie n'exploitant que les informations présentes sur le réseau et que chacun peut consulter et contrôler. Au final, en combinant l'état initial, considéré comme fiable, et la possibilité de vérifier chaque bloc construit au-dessus, les utilisateurs peuvent se mettre d'accord sur l'état courant de la blockchain.

À noter que dans le cas peu fréquent où deux chaînes valides sont présentées à un utilisateur, le mécanisme par défaut utilisé dans la plupart des blockchains est de considérer que la chaîne la plus longue est « la plus valide » dans la mesure où les transactions qu'elle contient auront été vérifiées par un plus grand nombre de nœuds du réseau. Ce mécanisme sera approfondi dans la question **18** (voir en particulier la figure 18.2 page 92).

Le consensus pair-à-pair

Dans tous les cas, l'une des caractéristiques principales des blockchains est d'atteindre un consensus sur l'état du système sans avoir besoin de disposer d'un tiers de confiance – chaque utilisateur peut vérifier l'intégrité du système. Pour ajouter un nouveau bloc, tous les nœuds participants doivent arriver à un accord commun au bout d'un certain temps – en particulier si des désaccords occasionnels sont possibles. L'algorithme de consensus doit continuer de fonctionner en présence d'acteurs malveillants tentant de corrompre ou de prendre le contrôle sur l'état courant de la blockchain. En ce sens, les blockchains offrent de multiples solutions efficaces au problème des généraux byzantins (BGP) décrit dans l'encadré ci-dessous en plus de toutes les approches BFT valides telles que *Practical Byzantine Fault Tolerance (PBFT)* (*cf.* question **45**).

Le problème des généraux byzantins

Le problème des généraux byzantins est une métaphore illustrant la difficulté de *s'accorder* sur une décision commune entre plusieurs acteurs distants et communicants, sur la base d'informations contradictoires provenant de messages erronés voire malveillants.
Il peut se formuler ainsi : n généraux campent autour d'une cité fortifiée ennemie avec leurs divisions. Chaque général doit décider, sur la base de ses observations de la situation, s'il faut attaquer ou battre en retraite. Il a en outre une opinion initiale sur l'action à faire qu'il doit transmettre aux autres généraux. Or les communications ne peuvent s'effectuer que par le biais de *messagers* qui mettent un certain temps pour rejoindre un autre camp : les communications sont donc *asynchrones*. Selon le modèle, il est possible d'envisager que ces messagers soient éventuellement capturés, amenant ainsi à des pertes de messages. Il se peut également que des traîtres se soient glissés parmi les généraux, qui essayeront de semer la confusion parmi les autres généraux en transmettant des informations erronées, voire volontairement falsifiées. L'hypothèse suivante est faite : il y a d traîtres (en informatique, ces traîtres sont plutôt appelés des nœuds *défaillants*), mais il y a moins de traîtres que de généraux loyaux, soit $0 \leqslant d < \lceil \frac{n}{2} \rceil$.
Les généraux loyaux doivent alors s'accorder sur une décision raisonnable car seule une attaque coordonnée impliquant un nombre suffisant de divisions permettrait de vaincre la cité assiégée. À l'inverse, une attaque isolée ou sous-dimensionnée serait obligatoirement synonyme de défaite. Ainsi, et même à supposer les communications fiables, le problème BGP consiste à trouver une stratégie (c'est-à-dire un algorithme) de communication permettant à l'issue des échanges de messages :

- aux généraux loyaux de se mettre d'**accord** sur un plan de bataille commun, c'est-à-dire, soit attaquer, soit se retirer pour ne pas engager leurs troupes vers une mort certaine ;
- d'obtenir une **décision valide**, c'est-à-dire, correspondant au choix majoritaire initial parmi les généraux loyaux en dépit de la présence de d traîtres.

Bien entendu, les généraux loyaux suivront la stratégie de communication à la lettre, quand les traîtres peuvent se comporter de manière complètement arbitraire (par exemple, ne pas envoyer de messages, ou en envoyer un autre). La difficulté vient donc du fait qu'un message reçu

peut paraître plausible pour le receveur alors qu'il n'est en réalité pas correct, et qu'il n'existe pas de superviseur (fiable et informé) susceptible de centraliser et faciliter la prise de décision.
En supposant que chaque général connaît le nombre total de généraux n ainsi que l'action à appliquer en cas d'égalité, il est possible de montrer que BGP peut se réduire à la résolution du sous-problème CL dit de *diffusion cohérente* où il y a parmi les généraux le *commandant* en chef (C) qui diffuse son message aux *lieutenants* (L), qui eux-mêmes relaient ce message entre eux. Les traîtres peuvent se trouver indifféremment parmi les lieutenants et le commandant. Il s'agit alors de définir une stratégie où lorsque le commandant envoie un ordre aux $n-1$ lieutenants :

- Tous les lieutenants loyaux obéissent au même ordre ;
- Si le commandant est loyal, alors chaque lieutenant loyal obéit à l'ordre émis.

Il existe des cas où il est impossible de résoudre le problème CL, en particulier si les communications sont uniquement "orales", c'est-à-dire si leur contenu est sous le contrôle total de l'émetteur. Par exemple si $n = 3$, un seul traître ($d = 1$) peut confondre les deux autres acteurs loyaux dans le cas de messages oraux. De façon générale, une condition nécessaire et suffisante à l'existence d'une solution est que $n \geqslant 3d + 1$, *i.e.*, au moins $\frac{2}{3}$ des acteurs sont loyaux – la preuve est constructive et définit un algorithme récursif permettant ainsi de tolérer d fautes ou défaillances (*cf.* question **45**). Cela peut paraître rédhibitoire dans le contexte de blockchains. Heureusement l'utilisation de messages cryptographiques signés (*cf.* question **47**) permet de diminuer drastiquement le nombre de composants loyaux nécessaires à la résolution du problème : jusqu'à $d \leqslant n-2$ erreurs peuvent être tolérées sans risque au prix de quelques hypothèses supplémentaires [38].

Le tableau 5.1 offre une liste des modèles de consensus dominants au sein des blockchains. Chaque approche est ensuite exposée avec ses avantages et inconvénients principaux. Lorsque de plus amples renseignements sont nécessaires, un lien vers la question correspondante est proposé.

Consensus par autorité – Proof-of-Authority (PoA)

Une preuve par autorité ou *Proof-of-Authority (PoA)* est un algorithme de consensus dans lequel les transactions et les blocs ne sont validés que par des