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

11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN 978-2-10-084141-7

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

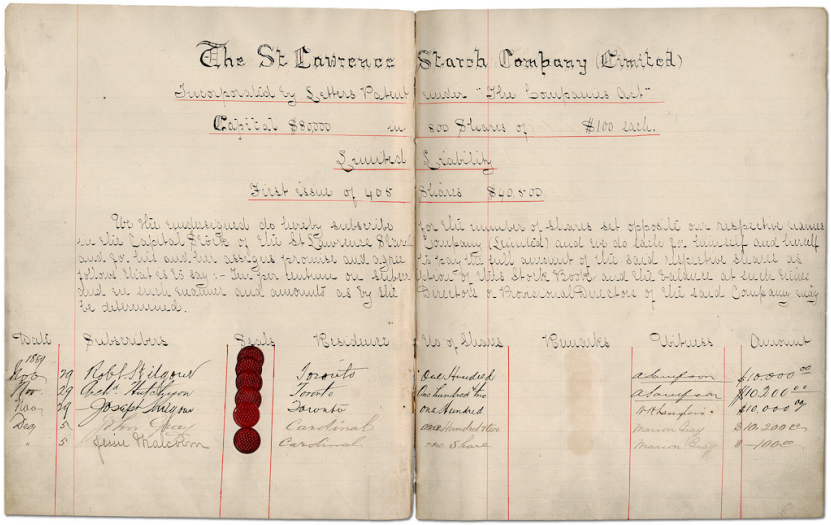

Figure 1.1 – Extrait d'un registre de souscriptions et transactions d'actions, 1889. Documents corporatifs officiels de St. Lawrence Starch Company. Archives publiques de l'Ontario.

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.

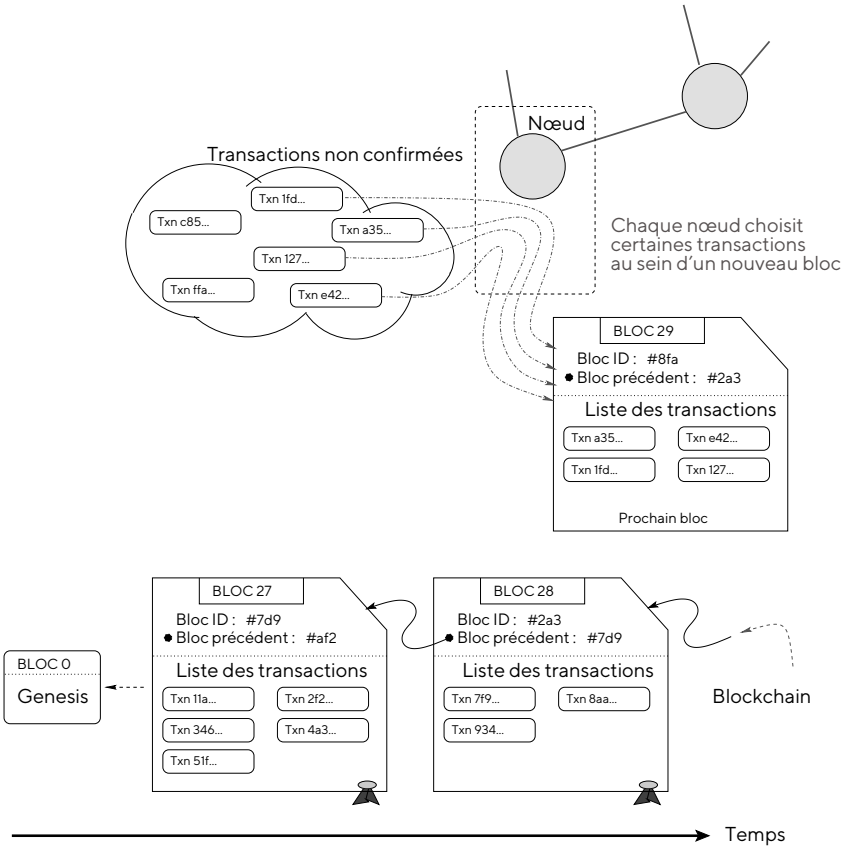

Figure 2.1 – Exemple simplifié d'une structure de données de type blockchain. Les transactions confirmées sont agrégées en blocs certifiés qui sont ajoutés en bout de chaîne à travers un pointeur vers le bloc précédent, formant ainsi une seule et unique chaîne répliquée à travers tout le réseau.

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