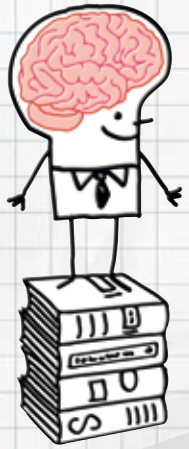
TechnoScope
by satw 4/21

Blockchain

Chances et opportunités

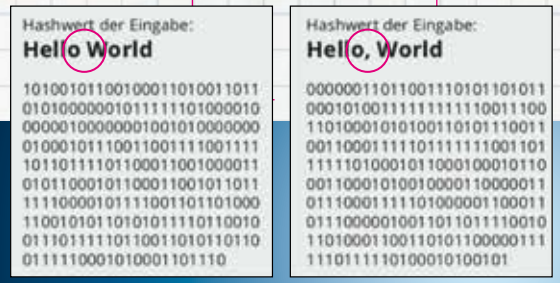
www.satw.ch/technoscope

À quel point la blockchain est-elle sûre?



La blockchain est considérée comme invulnérable car elle est répartie sur d'innombrables ordinateurs. De plus, divers procédés cryptographiques contribuent à sa sécurité. Le mot cryptographie vient du grec (kryptos: caché; graphein: écrire) et signifie «écriture secrète» ou chiffrement. La fonction de hachage joue un rôle essentiel dans la blockchain. Elle se compose d'un algorithme qui compresse un fichier numérique de n'importe quelle longueur et de nature diverse, par exemple un texte, une vidéo ou un fichier audio, en une chaîne de longueur fixe – le hachage (numéro de contrôle). Dans le SHA-256, l'algorithme de plus utilisé dans le monde des blockchains, le hachage se compose toujours de 256 caractères. Le moindre changement dans l'entrée génère une sortie totalement différente. L'exemple ci-dessous démontre ce qui se passe lorsqu'une seule virgule est ajoutée.

Enfin, tous ceux qui participent à la blockchain ont besoin d'un logiciel d'accès. Celui-ci se compose d'une clé publique et d'une clé privée. La clé publique permet de consulter toutes les données stockées dans une blockchain. Mais seule la clé privée permet de signer des transactions. La clé privée est une suite secrète de chiffres. Son détenteur a accès aux valeurs signées avec cette clé et peut les transmettre à d'autres personnes. La paire de clés est stockée dans un wallet, un «portefeuille numérique»: en ligne, à l'aide d'un logiciel ou hors ligne, sur un disque dur ou sous la forme d'un «portefeuille papier» imprimé sur une feuille de papier. Les wallets peuvent présenter une vulnérabilité dangereuse: ils peuvent être piratés, et les mots de passe et les disques durs peuvent être perdus. C'est alors le désastre absolu: si vous n'avez plus votre clé privée, vous ne pourrez plus jamais accéder à vos valeurs stockées sur la blockchain. Entre trois et cinq millions de bitcoins seraient ainsi bloqués dans le cyberespace.



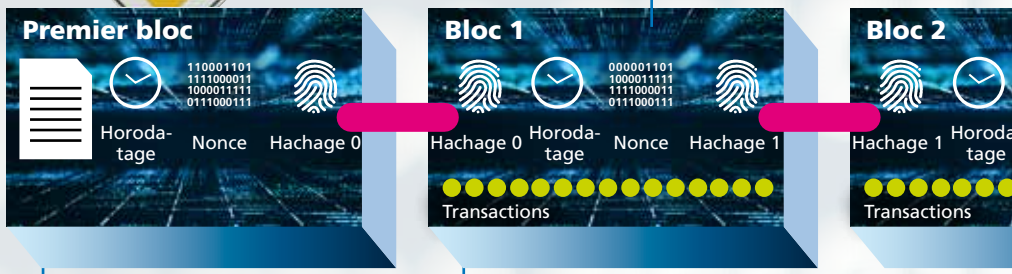
BLOCKCHAIN

La confiance numérique

La blockchain n'est rien d'autre qu'une base de données sous la forme d'une chaîne de blocs de données juxtaposés. Des informations sont enregistrées de manière cryptée dans chaque bloc. Chaque nouveau bloc fait référence au précédent. Chaque bloc ne peut donc être relié qu'à deux autres blocs: celui qui le précède dans la chaîne et celui qui le suit. Par conséquent, il est impossible de modifier, de manipuler ou de pirater les blocs a posteriori.

La blockchain est considérée comme un livre de comptes numérique incorruptible. Il en existe d'innombrables copies identiques, qui sont reliées entre elles. Lorsqu'une entrée est modifiée dans l'un des livres, cette modification est automatiquement enregistrée dans tous les autres. C'est pourquoi la technologie blockchain est également appelée «technologie des registres distribués» ou «Distributed Ledger Technology» (DLT).

Aucun instance centrale de contrôle n'est requise dans cette chaîne. Avec la blockchain, nul besoin de passer par des intermédiaires tels que des banques ou des assurances. Grâce à son inaltérabilité, la blockchain crée la confiance et la transparence. Certains y voient une grande promesse, d'autres, une menace pour les procédures et les mécanismes de contrôle en place. La question de savoir qui a raison n'est pas encore tranchée, d'où le battage médiatique actuel autour de la blockchain.



Bloc créateur: Le premier bloc d'une blockchain stocke le protocole de consensus. Celui-ci est négocié par la totalité des participant.e.s la blockchain et détermine la fréquence d'écriture d'un nouveau bloc dans la chaîne ainsi que sa taille, autrement dit le nombre de transactions qui peuvent y être enregistrées. Il précise également qui est autorisé à vérifier les nouveaux blocs et quelles tâches doivent être réalisées.

Bloc 1, 2, 3....: Le contenu de chaque bloc est constitué de la valeur de hachage (chiffre de contrôle ou empreinte numérique, voir AHA! pour plus de détails) de toutes les informations stockées dans le bloc. À cela s'ajoutent un horodatage et un nombre aléatoire (nonce) qui sont nécessaires pour valider le bloc, ainsi que la valeur de hachage du bloc précédent. Le hachage du nouveau bloc est calculé à partir de tous ces éléments. C'est en quelque sorte sa carte d'identité numérique qui garantit qu'il n'existe qu'une fois (par exemple, que les valeurs monétaires contenues ne peuvent pas être comptées plusieurs fois). Le hachage indique aussi l'ordre exact dans lequel un bloc est disposé dans la chaîne.

Mineurs: Avant qu'un nouveau bloc ne soit ajouté à la chaîne, les mineurs entrent en jeu. Ce sont les comptables de la blockchain: ils vérifient la validité des nouvelles transactions, les regroupent et les scellent de manière cryptographique. Le processus de vérification (proof of work) consiste à résoudre une énigme cryptographique. Chaque mineur est en concurrence avec d'autres pour résoudre une énigme mathématique complexe. Cela requiert une énorme puissance de calcul. Le premier qui résout la tâche peut attacher le bloc à la chaîne et reçoit une récompense. Dans la blockchain bitcoin, les mineurs reçoivent de nouveaux bitcoins. Dans les autres blockchains, d'autres formes de valeurs numériques (token) sont créées. C'est pourquoi ce processus est comparé à la prospection de l'or.

Accès réservé aux personnes autorisées: dans les blockchains privées, le nombre de participant.e.s est limité. Une instance centrale détermine qui est autorisé à participer, qui dispose de quels droits d'accès et quels processus de validation sont applicables. Les blockchains privées sont donc moins transparentes que les publiques. Mais leur objectif est généralement différent: elles utilisent la technologie pour protéger les données sensibles contre les falsifications. Les blockchains privées sont principalement utilisées par les entreprises et les pouvoirs publics.

Bien public: Sur les blockchains publiques, il suffit de télécharger le protocole open source. Aucune preuve d'identité n'est requise. Les participant.e.s ont les mêmes droits: ils peuvent consulter toutes les transactions et participer au processus de vérification. Une blockchain publique est entièrement transparente pour toutes les parties concernées.

Nœuds (nodes): Chaque ordinateur qui participe à la blockchain est un nœud. Chaque nœud stocke et gère une copie complète et constamment mise à jour de la blockchain. Le stockage multiple des données rend le réseau stable et fiable. Il permet de surmonter la défaillance d'un ou même de plusieurs nœuds.

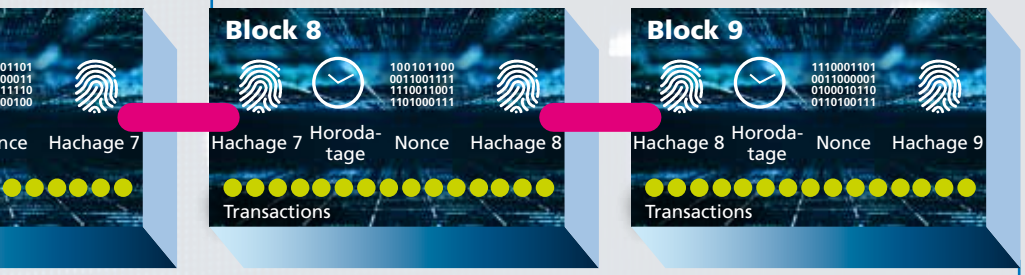
Opportunités de la blockchain:

- Comme toutes les informations sont enregistrées sous forme cryptée et que la blockchain est répartie sur de nombreux ordinateurs, elle est impossible à manipuler.
- La blockchain est entièrement transparente. Elle instaure la confiance entre des partenaires contractuels qui ne se connaissent pas ou peu.
- Les transactions sont réalisées directement entre les parties concernées. L'absence d'intermédiaires les rend plus rapides, moins coûteuses et moins sujettes aux erreurs.
- Dans les pays avec une faible sécurité juridique, la blockchain permet de garantir les droits de propriété.

Pseudonymat: Dans une blockchain publique, chaque transaction est attribuée à une adresse publique qui ne permet pas d'identifier les personnes. Toutefois, on ne peut pas exclure la possibilité de deviner leur identité à partir des transactions enregistrées, c'est pourquoi la blockchain n'est pas considérée comme anonyme, mais pseudonyme. Elle n'est donc pas appropriée aux malversations, bien que cette réputation lui colle encore à la peau.

Risques de la blockchain:

- La blockchain s'appuie sur l'énorme puissance de calcul d'un grand nombre d'ordinateurs en réseau. Elle consomme donc de grandes quantités d'énergie.
- Le fait que les utilisatrices et les utilisateurs participent aux blockchains publiques avec un pseudonyme peut être utilisé à des fins criminelles.
- Lorsque la personne utilisant un pseudonyme est identifiée, il est possible de suivre toutes les transactions qu'elle a effectuées sur la blockchain. Cela va à l'encontre du droit à l'oubli prévu par la protection des données.
- La blockchain promet plus de transparence, mais elle est tellement complexe qu'elle demeure opaque et énigmatique pour la plupart des gens.



Qui l'a inventée? En 2008, en pleine crise bancaire, une personne ou un groupe inconnu publie un article scientifique sous le pseudonyme de Satoshi Nakamoto, qui traite d'un nouveau système électronique appelé «bitcoin» et capable de transmettre des valeurs monétaires de manière anonyme et infalsifiable sans instance centrale de contrôle. À l'heure actuelle, on ne sait toujours pas qui est Satoshi Nakamoto ni même si cette personne existe. Mais beaucoup considèrent encore son idée comme révolutionnaire: un système de paiement libre, ouvert et autogéré par la société numérique. Une alternative au système financier souvent opaque et sensible aux crises.

QUELLES SONT LES AUTRES APPLICATIONS DE LA BLOCKCHAIN?

Le bitcoin et les autres cryptomonnaies (il en existe aujourd'hui plus de 6'000) ne sont qu'une application de la blockchain. En principe, il est possible d'utiliser le registre numérique incorruptible partout où les conditions de propriété doivent être documentées de manière transparente, publique et infalsifiable: cartes d'identité, diplômes, inscriptions au registre foncier, testaments. En voici un exemple concret: depuis un peu moins d'un an, l'entreprise horlogère suisse Breitling vend tous ses nouveaux modèles avec un passeport numérique basé sur la blockchain. Celui-ci documente toutes les informations importantes (modèle, date de fabrication, numéro de série, date d'achat, garantie, réparations, etc.) de manière sûre et inaltérable et garantit l'authenticité de la montre. Les solutions blockchain sont particulièrement efficaces lorsqu'elles sont combinées à des contrats intelligents (Smart Contracts). Ce sont des codes de programme «if-then» stockés dans la blockchain qui déclenchent automatiquement des actions convenues dès que certaines conditions sont remplies. Par exemple, la serrure intelligente de l'appartement de vacances reste verrouillée le jour de l'arrivée jusqu'à ce que le locataire ait payé la caution.

Les crypto-monnaies sont comme les cartes Pokemon

Entretien avec Bernd Lapp, expert en blockchain

Payer avec des bitcoins

Dans la vie quotidienne, le paiement en cryptomonnaies est encore assez rare en Suisse. Seuls certains cafés, magasins en ligne ou compagnies d'assurance font exception. À Zoug, il est possible aussi de payer ses impôts en bitcoins depuis 2016. À Zermatt, l'administration communale accepte les bitcoins pour les opérations au guichet depuis le début de l'année – mais cela a encore peu d'écho. Une carte de crédit bitcoin sert de passerelle entre le monde de la monnaie numérique et celui des francs: elle permet de payer comme n'importe quelle autre carte prépayée rechargeable.

Technoscope: Pourriez-vous nous expliquer la blockchain le plus simplement possible?

Bernd Lapp: La blockchain est comme une feuille de papier sur laquelle vous écrivez. Lorsqu'elle est remplie, vous la classez dans un livre. Dès que la nouvelle page est classée, toute personne ayant le livre en main peut la lire. Et partout dans le monde, ceux qui disposent du même livre trouveront également cette page dans leur exemplaire.

Comment les blocs de la chaîne sont-ils reliés?

Toutes les informations d'une page sont cumulées. Le résultat est alors chiffré de manière cryptographique et le «hachage» obtenu devient la première entrée de la page suivante. Lorsque l'on connaît le mécanisme de chiffrement, ce hachage suffit à restaurer la page précédente et à remonter toute la chaîne jusqu'à son début. Cette transparence est le point fort de la blockchain.

Pourquoi?

Il existe de grandes sociétés d'audit dont la mission consiste à examiner les comptes des banques et d'autres entreprises et à vérifier que toutes les valeurs ont été correctement comptabilisées. Quand je leur explique en quoi consiste la blockchain, il arrive un moment où le silence se fait car elles réalisent

Comment faire?

Toute personne qui possède des bitcoins a besoin d'un portefeuille numérique ou «wallet». Jusqu'à récemment, en ouvrir un était assez compliqué mais désormais, c'est un jeu d'enfant grâce à différentes applications.

Économiser des bitcoins

La start-up suisse relai.ch est convaincue que le bitcoin est particulièrement adapté aux comptes d'épargne. Grâce son application, l'utilisation est facilitée.

Acheter des bitcoins

Le hall d'entrée du Parkhotel Beau Site à Zermatt abrite le premier distributeur de bitcoins des Alpes suisses. Car pour payer avec des bitcoins ou les acheter à titre d'investissement, il faut d'abord se les procurer. Cela est possible, par exemple, dans tous les distributeurs de billets des CFF. Selon les CFF, 1'500 personnes utilisent ce service chaque mois. Et depuis peu, Manor et Valora, ainsi que diverses stations-service, proposent des coupons en bitcoins qui peuvent être convertis de francs en bitcoins en ligne.

«Chacun peut accéder aux comptes, plus personne ne peut fausser quoi que ce soit.»

que cette nouvelle technologie rend leur modèle commercial obsolète. Ce qu'elles font, tout le monde peut le faire avec la blockchain: chacun peut accéder aux comptes, plus personne ne peut tricher ni fausser quoi que ce soit. C'est tout simplement impossible. Une fois cryptée, une page est comme gravée dans la pierre.

En quoi la blockchain se démarque-t-elle de l'e-banking?

Avec l'e-banking, vous êtes enregistré auprès d'une banque et vous lui donnez accès à votre argent. Avec la blockchain, vous êtes la seule personne à y avoir accès et, lorsque vous transférez une somme d'argent en bitcoins ou dans une autre cryptomonnaie, aucun tiers n'est impliqué. Cela permet également de réduire les frais et de rendre l'ensemble du processus plus efficace.

Les cryptomonnaies vont-elles s'imposer?

Les cryptomonnaies sont comme les cartes Pokemon. Certaines d'entre elles valent plus cher parce qu'elles arborent un personnage spécial que tout le monde aimerait avoir, d'autres sont plus communes et donc moins convoitées. Il en va de même avec les cryptomonnaies. De plus en plus de personnes et même des pays entiers reconnaissent leur valeur: elles permettent des transactions financières plus simples et moins coûteuses, car elles nécessitent moins de technologie, moins d'étapes et moins d'intermédiaires. C'est pourquoi les cryptomonnaies sont de plus en plus acceptées. Récemment, le Salvador est devenu le premier pays à reconnaître le bitcoin comme un moyen de paiement officiel.

Vous vivez et travaillez dans la Cryptovalley de Zoug. Pourquoi la Suisse attire-t-elle autant d'entreprises blockchain?

La blockchain s'accommode très bien du système fédéral décentralisé et de l'autonomie des citoyennes et citoyens qui ont l'habitude de participer aux processus de décision. C'est précisément la philosophie qui sous-tend la blockchain.

À: **Corinne Giroud**

Copie:

Objet: **Choix d'études et de carrière**

Les évolutions technologiques me fascinent et je m'intéresse en particulier aux solutions innovantes liées au numérique. Existe-t-il par exemple des formations dans le domaine de la cryptographie et des blockchains? Leslie, 18 ans

Bonjour Leslie,
Internet a bouleversé notre société de l'information et notre manière de communiquer; la technologie de la blockchain pourrait révolutionner notre économie. Des transactions sûres, inaltérables et décentralisées, c'est ce que permet cette approche innovante où la cryptographie – le chiffrement garantissant la confidentialité des données – joue un rôle prépondérant. Les blockchains sont une technologie prometteuse, et l'un des défis de demain sera d'en réduire la consommation énergétique.

Corinne Giroud, Office cantonal d'orientation scolaire et professionnelle – Vaud

Un outil au service de l'innovation dans de nombreux domaines

Les domaines d'application de la blockchain sont nombreux: économie (banques, assurances), cyberadministration (registre foncier, cadastre, registre des poursuites, vote électronique, etc.), industrie 4.0 (traçabilité de la chaîne alimentaire, authentification de produits), santé (suivi des soins) ou encore juridique (droit d'auteur, exploitation et reproduction d'œuvres, etc.). En tant qu'objet d'étude et de recherche, la blockchain et la cryptographie sont le domaine des physicien.ne.s, des mathematicien.ne.s et des informaticien.ne.s. Technologie très récente, la blockchain ne fait pas encore l'objet de formation dédiée au niveau bachelor. En revanche quelques-uns de ses domaines d'application sont exploités dans des masters innovants organisés par l'École polytechnique fédérale de Lausanne (EPFL). Sécurité informatique, finances de l'ingénieur, données numériques: ces trois domaines d'application de la blockchain sont au cœur de masters spécifiques accessibles aux titulaires d'un bachelor en ingénierie ou en économie (pour l'ingénierie financière).

Si la technologie et l'innovation te passionnent dans une perspective de développement durable, le master conjoint en management durable et technologie proposé par l'Université de Lausanne, l'École polytechnique fédérale de Lausanne et l'Institut pour le management et le développement IMD propose une formation interdisciplinaire qui invite à réfléchir à des solutions durables, en particulier pour la blockchain, si énergivore.

Liens

Formations à retrouver sur **www.orientation.ch**
- EPFL Master en cybersécurité, en data science, ingénierie financière
- UNIL Master en management durable et technologie
- UNIGE CAS Développement d'applications décentralisées avec blockchain et Distributed Ledger Technologies

Impressum
SATW Technoscope 04/21 | Décembre 2021 | www.satw.ch/technoscope
Concept et rédaction: Ester Elices | **Collaboration rédactionnelle:** Christine D'Anna-Huber | **Graphisme:** Andy Braun | **Photos:** Adobe Stock, Bernd Lapp | **Photo de couverture:** Adobe Stock | **Traduction:** Ars Linguae | **Relecture**: Edith Schnapper | **Impression:** Egger AG

Abonnement gratuit et commandes supplémentaires
SATW | St. Annagasse 18 | CH-8001 Zürich | technoscope@satw.ch | Tel +41 44 226 50 11

Le prochain Technoscope paraîtra en avril 2022 sur le thème de la «Musique»

satw it's all about technology

Tu as des questions ou des suggestions pour l'équipe de Technoscope? Alors n'hésite pas à nous les envoyer! **technoscope@satw.ch**