

CORIO LAN STALENES

VIELLE TECHNOLOGIQUE

LA BLOCKCHAIN

CORIO LAN STALENES – BTS SIO
OPTION SLAM

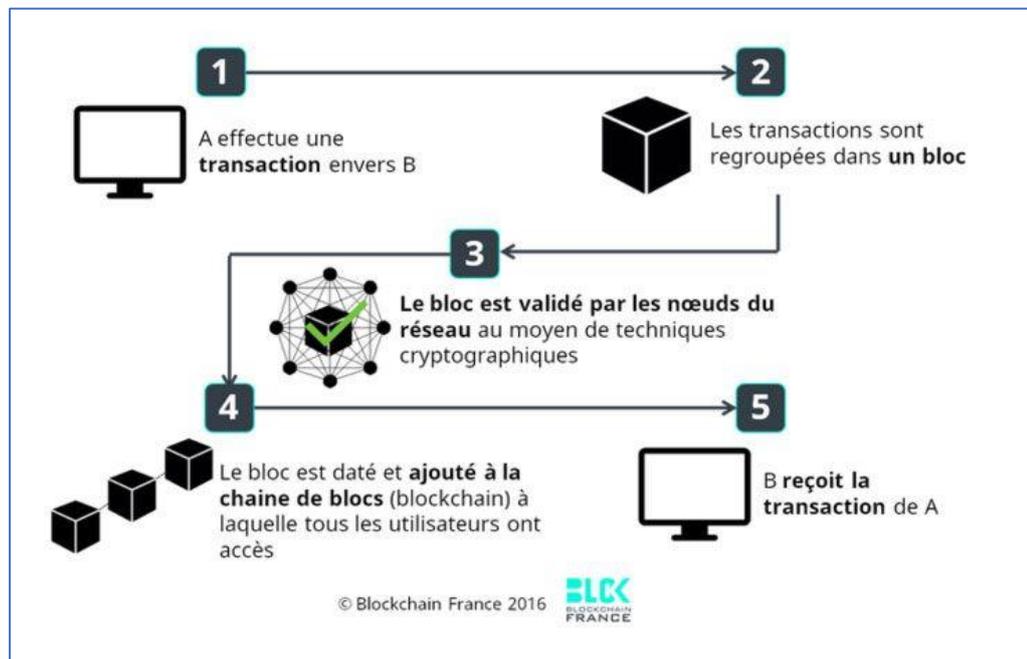
INTRODUCTION

Depuis son apparition public en 2009 la blockchain suscite beaucoup d'intérêt pour sa caractéristique inédite de permettre aux agents économiques de s'abstenir d'intermédiaire ou de tiers de confiance pour sécuriser leurs transactions. Son fonctionnement est fondé sur la cryptographie pour assurer la sécurité des transactions et s'appuie sur le développement exponentiel du nombre et de la puissance de calcul des machines raccordées à internet. C'est donc sur cette présentation que je vous présenterai son origine sans entrer dans des détails technique, ses applications dans de nombreux secteur d'activité ainsi que les enjeux d'une telle technologie qui bouleverse la décennie.

Table des matières

I. LA BLOCKCHAIN	1
A Définition.....	2
B Origine.....	2
C Les Applications.....	2
II. CARACTERISTIQUE DE LA BLOCKCHAIN	4
A Smart Contract.....	5
B Finance Décentralisé.....	5
C La Cybersécurité.....	5
III. REVOLUTION BLOCKCHAIN	6
A Les Avantages.....	7
C Les Inconvénients.....	7

I. LA BLOCKCHAIN



A Définition :

La Blockchain est un registre public dans lequel toutes les transactions sont enregistrées **de manière sécurisée, transparente** et définitive par un grand nombre d'ordinateurs participant volontairement au système ou réseau, appelés nœuds.

Ce registre, ou historique, débute lorsque la toute première transaction est émise et est alimenté en continu au fur et à mesure que les transactions ont lieu. Il présente la caractéristique majeure d'être décentralisé, c'est-à-dire qu'il n'existe pas d'autorité centrale validant et transmettant la transaction comme c'est par exemple le cas aujourd'hui lors d'un virement. Ce registre est enregistré en totalité en tous les nœuds du réseau, le rendant très difficilement altérable.

En effet, si un des nœuds est corrompu (à la suite d'une intrusion informatique par exemple) et tente de modifier l'historique des transactions, le résultat sera automatiquement rejeté par les autres nœuds possédant le véritable historique.

CORIO LAN STALENES

Une de ses caractéristiques principales est qu'elle ne peut pas être modifiée. Les blocs sont protégés par plusieurs procédés cryptographiques innovants qui rendent la modification impossible a posteriori. C'est ce qui donne à cette technologie son caractère transparent : on peut uniquement ajouter des opérations, mais pas les modifier ni les supprimer, elles sont infalsifiables.

Cette technologie repose sur un **système de pair-à-pair** décentralisé : les données ne sont pas hébergées par un serveur unique mais distribuées entre les utilisateurs, sans intermédiaire. Une partie des utilisateurs détient des copies de la blockchain, qui se trouve donc présente partout dans le monde.

Ces centaines de copies sont sans cesse mises à jour simultanément. Contrairement aux bases de données traditionnelles, qui sont administrées par des opérateurs centralisés, la blockchain est administrée collectivement, par tous les nœuds du réseau.

Ces nœuds obéissent tous à un même protocole informatique, qui définit les procédures à suivre, ainsi que les conditions à respecter pour mettre à jour la base de données.

B Origine :

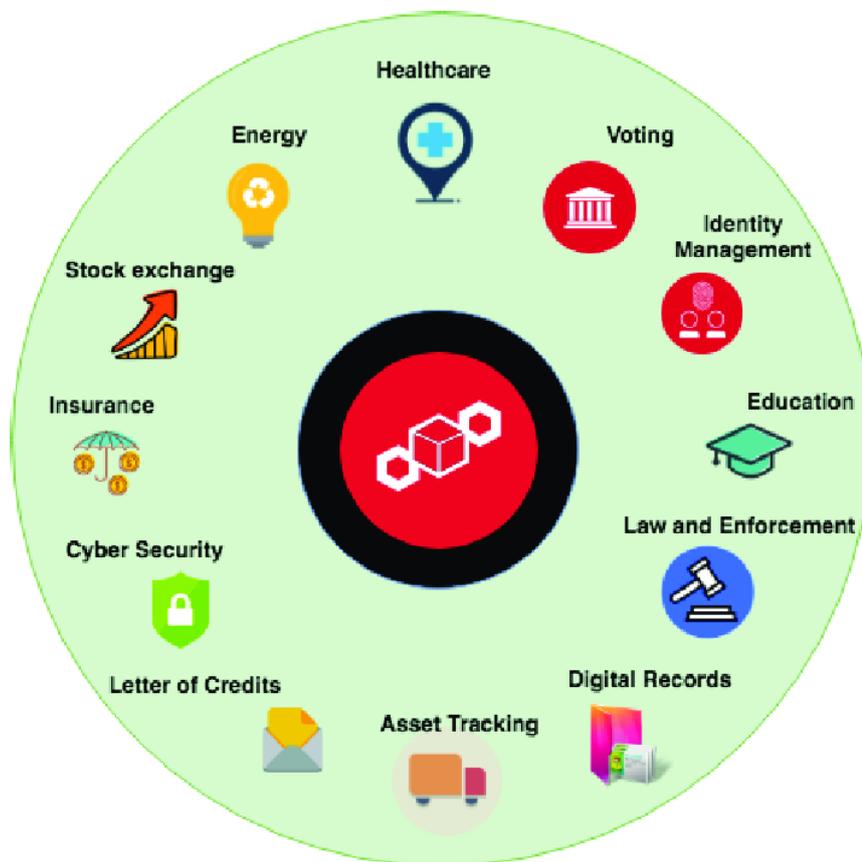
Pour mieux comprendre la démarche, il est nécessaire d'explorer le contexte dans lequel elle a été développée. À l'origine, les utilisateurs recherchaient un système efficace, rentable, fiable et sécurisé pour effectuer et enregistrer des transactions financières. Les volumes de transactions à l'échelle mondiale progressent de manière exponentielle et vont à l'évidence amplifier la complexité, les vulnérabilités, l'inefficacité et les coûts des systèmes de transactions actuels. Le développement du commerce électronique, les activités de banque en ligne et les achats au moyen d'applications, ainsi que la mobilité croissante des utilisateurs dans le monde, ont contribué à l'augmentation des volumes de transactions. Le bitcoin est l'une des solutions développées pour répondre aux problèmes de complexité, de vulnérabilité, d'inefficacité et de coût des systèmes de transactions.

CORIOLAN STALENES

Il s'agit d'une crypto-monnaie, lancée en 2009 par une ou plusieurs personnes dont l'identité reste mystérieuse, puisqu'elle n'est connue que par un pseudonyme : **Satoshi Nakamoto**.

Contrairement aux monnaies traditionnelles, émises par les banques centrales, le bitcoin ne dépend d'aucune autorité monétaire centrale.

C Les Applications :



CORIO LAN STALENES

Cloud Storage : Le stockage sur le cloud conventionnel implique que les données soient centralisées en un point de stockage central, avec les risques de pertes de données qui en découlent. On peut donner comme exemple le cas de Megaupload. A l'heure actuelle, aucun utilisateur n'a pu récupérer ses données hébergées sur Megaupload.

L'idée d'un stockage de données décentralisé et passant par la Blockchain a donc émergé. Elle part du constat que tout le monde possède de l'espace disque libre sur son ordinateur, et que dans le même temps de plus en plus de centres de données sont construits. Les utilisateurs peuvent ainsi louer leur espace disque non utilisé à ceux en ayant le besoin. Lorsqu'un fichier nécessite d'être stocké sur le cloud, il va être crypté et divisé en infimes morceaux qui seront répartis entre les différents utilisateurs, et ce afin que ces derniers ne puissent avoir accès au document dans son intégralité. Pour la récupération du fichier, le système va collecter les différentes parties auprès des loueurs d'espace et l'assemble

Banque : la technologie ouvre la possibilité de valider des transactions sans l'intermédiaire d'une chambre de compensation, ce qui devrait permettre de certifier des opérations dans des délais beaucoup plus courts. La blockchain peut aussi favoriser le **partage d'informations entre acteurs concurrents** d'une place financière dans le respect du secret de leurs données commerciales et, ce faisant, faciliter la gestion de structures ou d'instruments communs en réduisant les coûts de contact et les frais d'administration.

Assurance : l'apport de la blockchain tient par exemple à l'automatisation des procédures de remboursement et à l'allégement de certaines formalités à la charge des sociétés comme de leurs clients, sous réserve que les hypothèses et les conditions d'indemnisation et de préjudice soient clairement établies.

CORIO LAN STALENES

Logistique : la blockchain présente deux intérêts :

- **assurer une traçabilité des produits**, ainsi que la mémoire des différentes interventions sur une chaîne de production et de distribution
- **alléger les formalités** et créer les conditions d'une coopération entre les acteurs d'une filière, notamment en matière d'échange d'informations. Cet usage pourrait trouver aussi une application dans le secteur **agro-alimentaire** pour la traçabilité des aliments, particulièrement intéressante en cas de crise sanitaire.

Jeu Vidéo : Les « gamers » connaissent le problème par coeur : ce qui est dans un jeu vidéo reste dans le jeu. L'exemple le plus connu est celui de Fortnite. Le jeu à succès, s'il est disponible gratuitement, a amassé 2,5 milliards de dollars en 2018 grâce aux achats de « features » (déguisements, habits) pour les personnages. Or aucun de ces éléments n'appartient aux joueurs ; ces achats sont pour eux comme perdus. C'est justement pour remédier à cette frustration que des sociétés comme Ubisoft travaillent sur la blockchain. Grâce à elle, tous les équipements peuvent être digitalisés et avoir une existence propre en dehors du jeu, avec un système de tokens (jetons). Les « gamers » peuvent les acheter, les vendre, se les échanger.

II. CARACTERISTIQUE DE LA BLOCKCHAIN

A Smart Contrat :

Un contrat intelligent ou « **smart contract** » est un accord ou un ensemble de règles régissant une transaction entre entreprises. Il est stocké dans la Blockchain et mis en œuvre automatiquement dans le cadre d'une transaction. Les contrats intelligents peuvent comporter différentes clauses contractuelles susceptibles d'être, en tout ou partie, directement applicables et/ou exécutoires de manière automatique. Leur finalité est d'apporter une sécurité supérieure, mais aussi de **diminuer les coûts et les délais par rapport aux contrats traditionnels**. À titre d'exemple, un contrat intelligent peut définir les conditions contractuelles régissant le transfert d'un titre d'obligation d'entreprise.

CORIO LAN STALENES

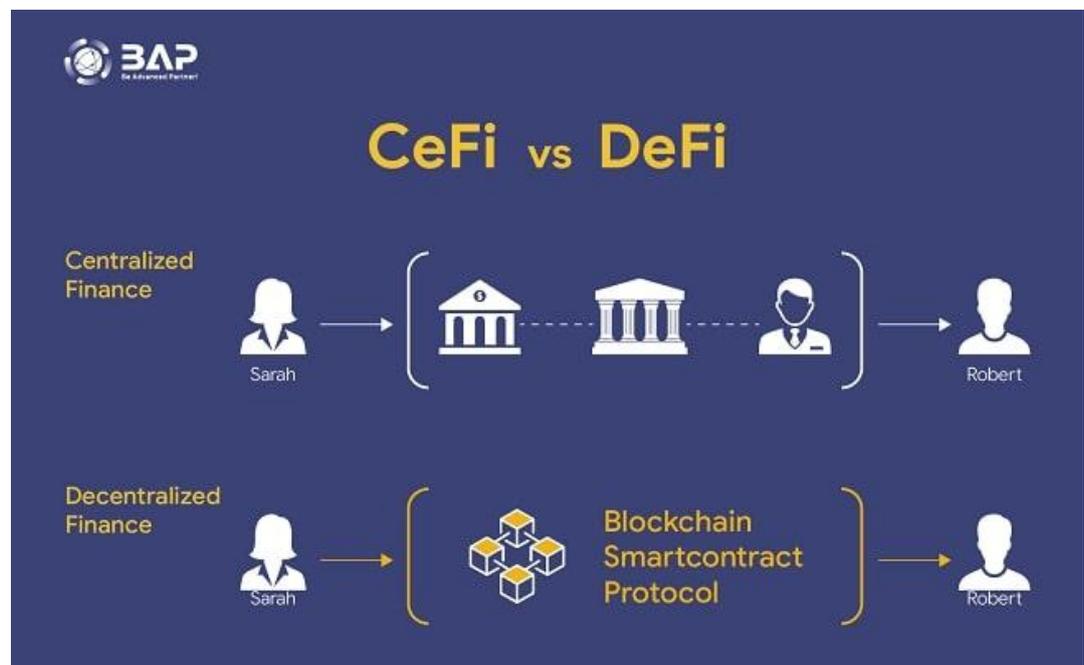
Il peut aussi définir les conditions générales d'une assurance voyage, qui peuvent être automatiquement applicables lorsque, par exemple, un vol est retardé de plus de six heures.

B Finance Décentralisé :

La DeFi, Decentralized Finance ou Finance Décentralisée, regroupe de nombreuses applications décentralisées (DAPPS) reposant sur la [blockchain](#) et ayant pour but de remodeler l'accès et l'utilisation d'outils et services bancaires et financiers traditionnels.

L'idée centrale est de créer un système financier et monétaire alternatif décentralisé et transparent permettant de transcender les limites du système actuel en redonnant le contrôle aux utilisateurs via la suppression d'intermédiaires ou d'organes de contrôle central.

Puisqu'elle repose sur la blockchain, la DeFi propose des services bancaires et financiers de pair-à-pair et décentralisés. Ils sont donc **sans intermédiaire, instantanés, immuables, transparents, bien plus rapides et moins chers que les services classiques.**



C La Cybersécurité :

La blockchain peut également être un outil stratégique pour la cybersécurité. En effet, la vague actuelle de cyberattaques est de plus en plus pointue, dopée à la fois par des mécanismes sophistiqués et une multiplication des appareils qui offrent de très nombreuses portes d'entrée aux hackers. Si les solutions se développent en écho à l'évolution des attaques, elles pourraient toutefois atteindre leurs limites face à un certain type d'actes malveillants.

C'est par exemple le cas des certificats de sécurité des sites web. Les utilisateurs font confiance à l'entreprise tierce qui certifie la sécurité du site. Mais si l'entreprise est compromise, le certificat de sécurité peut également l'être et, alors, tromper l'utilisateur.

Aujourd'hui, la blockchain peut-être est une clé centrale pour lutter contre la cybercriminalité.



III. REVOLUTION BLOCKCHAIN

A Les Avantages :

- Donné infalsifiable, traçabilité et propriété
- Suppression des intermédiaires avec les smart contract
- Sécurité et rapidité du protocole
- Création de la nouvelle économie Defi

B Les Inconvénients :

- Une technologie à ses débuts qui est imparfaite et qui demande à être plus exploité et connu du public
- Une technologie très énergivore vue du nombre de calcul et transaction effectué
- Risque de piratage exemple DAO

CONCLUSION

La blockchain est une technologie qui a bouleversé notre décennie tant ces applications dans divers secteurs de tout type son remarquable et très intéressante pour faciliter et optimiser notre digitalisation dans le monde. Elle est certes assez récente et incomplète mais il est certain que dans les prochaines décennies à venir elle sera au cœur de nos vies pour chaque utilisation d'objet connecté, de paiement instantané, de remboursement, de sécurisation de donné, de traçabilité de produit et de transparence.