



MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE

*Liberté
Égalité
Fraternité*

GUIDE DE SENSIBILISATION À LA BLOCKCHAIN

Pour mieux comprendre
les usages de cette technologie



Réalisation de l'étude : Blandine Dusser
et Hélicia Claude

Directeur de la publication : Thomas Courbe

Date de parution : avril 2022

Édition : bureau de la communication - DGE

Crédits photos : Peera_Sathawirawong,
imaginima / iStock / Getty Images Plus

ISBN : 978-2-11-162217-3 (en ligne)

À PROPOS DE CE GUIDE

Le présent guide est le fruit de la collaboration entre les acteurs de l'écosystème blockchain et la Direction générale des Entreprises.

Les différentes rubriques de ce site permettent de répondre aux questions récurrentes liées aux projets blockchain, de lever les idées reçues quant à cette technologie et de vous présenter des initiatives blockchain ayant été menées avec succès.

La finalité de ce guide est avant tout vulgarisatrice ; ainsi, l'utilisation d'expressions compréhensibles par le plus grand nombre a été privilégiée.

Bonne lecture.

TABLE DES MATIÈRES

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN	4
CAS D'USAGE THÉORIQUE : TRAÇABILITÉ	4
Exemple : les caves du Rauzan traçabilité du vin biologique de Bordeaux	5
Exemple : une compagnie aérienne la Blockchain pour se conformer aux exigences douanières	6
Exemple : Suez - la Blockchain pour instaurer une gestion efficace et sécurisée du cycle de vie du produit	7
CAS D'USAGE THÉORIQUE : <i>Non-fungible token (NFT)</i>	8
Exemple : le consortium aura le nft comme certificat d'authenticité d'un produit de luxe	9
Exemple : le nft associé à une œuvre artistique numérique	10
CAS D'USAGE THÉORIQUE : MONNAIES NUMÉRIQUES	11
Exemple : utiliser une monnaie numérique pour optimiser ses activités de chambre de compensation	12
Exemple : s'appuyer sur le stablecoin « lugh » pour créer une communauté d'utilisateurs	13
II. RECOURIR À LA BLOCKCHAIN : QUELQUES CRITÈRES DE CHOIX	14
LA TECHNOLOGIE BLOCKCHAIN RÉPOND-ELLE À VOS BESOINS ?	14
QUELLES SONT LES PRINCIPALES DIFFÉRENCES ENTRE LES TYPES DE BLOCKCHAIN ?	15
QUELS SONT LES POINTS COMMUNS ENTRE LES DIFFÉRENTS TYPES DE BLOCKCHAIN ?	15
QUELS TYPES DE BLOCKCHAIN POUR QUELS CAS D'USAGE ?	16
EST-IL POSSIBLE DE RÉDUIRE LA CONSOMMATION ÉNERGÉTIQUE DE SON RÉSEAU BLOCKCHAIN ?	17
QUE REPRÉSENTE LA CONSOMMATION ÉNERGÉTIQUE D'UNE TRANSACTION SUR UN RÉSEAU DE CRYPTOMONNAIES ?	18
QUE REPRÉSENTE LA CONSOMMATION ÉNERGÉTIQUE ANNUELLE DU RÉSEAU BITCOIN ?	18
FOIRE AUX QUESTIONS	19
CONTRIBUTEURS À CE GUIDE	21

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN

CAS D'USAGE THÉORIQUE : TRAÇABILITÉ

SITUATION INITIALE

BESOIN CLIENT

- Répondre à une obligation de conformité
OU
- Différencier son offre sur le marché.

OBSTACLES TECHNIQUES

- Une chaîne complexe d'informations à recueillir.
- Besoin de renforcer la confiance entre les différents partenaires sur les informations fournies.

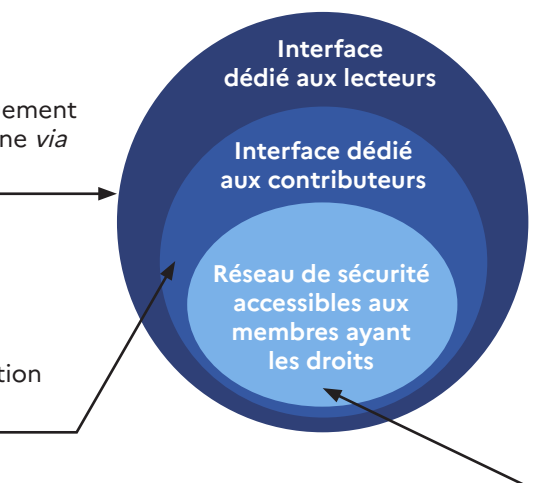
EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil.
- Partage sécurisé de l'information entre les partenaires sur la chaîne d'information.
- Fiabilité des données inscrites.
- Responsabilisation de tous les partenaires sur la qualité des données fournies.
- Confidentialité des données en dehors des ayant-droits d'accès.

LA BLOCKCHAIN COMME SOLUTION

Pour consulter l'information numériquement et facilement (exemple : sur smartphone *via* un QR code).

Pour transmettre numériquement les informations au réseau *via* une inscription dans la blockchain.



Pour assurer le bon fonctionnement de l'infrastructure numérique : ici sont situés les nœuds du réseau.

GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- **Périmètre** : choix du nombre de partenaires et de la taille du réseau (nombre de nœuds).
- **Choix des droits** : accès en lecture, ajout d'informations, validation.
- **Choix du public cible de l'information compilée** : qui accédera à la chaîne d'information de traçabilité sur le produit ?

Plus de précisions sur les différents types de réseau blockchain disponible dans la section (ajouter le numéro de la section sur les $\neq$ types de blockchains).



POINTS D'ATTENTION

- La mise en place du réseau blockchain requiert :
- la numérisation préalable des différents membres de la chaîne d'information ;
 - la standardisation des données des différentes bases d'où l'information est tirée.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : TRAÇABILITÉ

EXEMPLE : LES CAVES DU RAUZAN
TRAÇABILITÉ DU VIN BIOLOGIQUE DE BORDEAUXSITUATION
INITIALE

BESOIN CLIENT

- Différencier son offre sur le marché.
- Comment garantir au consommateur un respect des exigences BIO, de la vigne jusqu'à la bouteille ?

OBSTACLES TECHNIQUES

- Le cycle de production est composé de multiples acteurs.
- La chaîne logistique inclut des unités de volumes différentes : bouteilles, tonneaux, lots parcellaires...

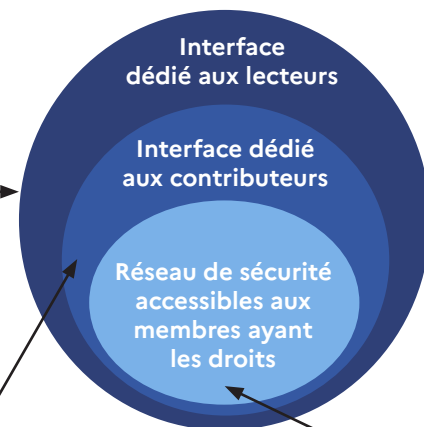
EXIGENCES TECHNIQUES
DE LA SOLUTION

- Accessibilité de l'outil par tous de manière intuitive.
- Partage sécurisé de l'information entre les partenaires sur la chaîne d'information.
- Fiabilité des données inscrites car forte auditabilité des informations fournies aux consommateurs.
- Cercle vertueux permettant le respect des exigences bio : si on inscrit une donnée fautive ou si on falsifie une donnée inscrite, cela apparaît dans un historique visible par tous.

LA BLOCKCHAIN COMME SOLUTION

Les consommateurs accèdent *via* un QR code sur la bouteille aux informations sur la vie du produit et ses labels.

Les acteurs de la chaîne de production inscrivent numériquement : le lieu de récolte, le mode de production, le parcours du produit, les contrôles du label bio effectués et horodatés.



Pour assurer le bon fonctionnement de l'infrastructure numérique : plusieurs acteurs locaux portent les nœuds du réseau sur une blockchain privée.

GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- **Périmètre** : local. Le réseau est limité aux acteurs de la chaîne de production du vin AOC bio des caves du Rauzan, de la vigne jusqu'à la mise en bouteille.
- **Choix des droits** : producteur, transporteur, embouteilleur, etc ont le droit d'inscrire des informations dans le réseau.
- **Choix du public cible de l'information compilée** : les consommateurs.



POINTS D'ATTENTION

La mise en place du réseau blockchain requiert :

- l'accès à une interface (sur PC, tablettes, smartphones) pour les contributeurs sur laquelle ils inscrivent les données facilement ;
- la formation des acteurs à l'utilisation de cet interface.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : TRAÇABILITÉ

EXEMPLE : UNE COMPAGNIE AÉRIENNE LA BLOCKCHAIN POUR SE CONFORMER AUX EXIGENCES DOUANIÈRES

SITUATION INITIALE

BESOIN CLIENT

• Une compagnie aérienne doit répondre à une obligation de conformité en assurant la certification de ses processus de dédouanement d'actifs. La compagnie doit être en mesure de prouver que chaque actif dédouané est effectivement utilisé dans son activité industrielle aéronautique.

OBSTACLES TECHNIQUES

• Différents niveaux d'intégration des données sont nécessaires. L'infrastructure est une chaîne d'acteurs qui doivent tous contribuer à la collecte d'information mais dont les droits de lecture sont différents.

• Besoin de renforcer la confiance entre les différents partenaires sur les informations fournies.

EXIGENCES TECHNIQUES DE LA SOLUTION

• Interopérabilité permettant la collecte de données issues de différents acteurs et de différentes sources.

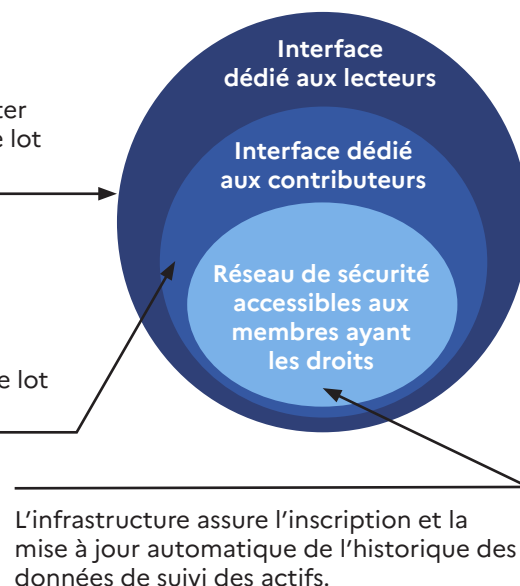
• Auditabilité de l'historique des données.

• Pleine responsabilité des acteurs individuels quand à ce qu'ils déclarent.

LA BLOCKCHAIN COMME SOLUTION

Pour que les autorités puissent consulter le suivi des consommations de chaque lot d'actifs.

Les différents systèmes d'information des parties prenantes fournissent les informations sur l'utilisation de chaque lot d'actifs.



GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- La compagnie aérienne a choisi une blockchain privée afin de réunir uniquement les parties prenantes impliquées dans le cycle de vie des actifs (transport, utilisation, revente...) et cela à une échelle internationale.
- **Choix des droits** : les accès de chacun sont strictement définis à la création du consortium de gestion du réseau. Les accès aux données confidentielles sont strictement réservés aux seuls membres autorisés.
- L'historique des données de suivi automatisé des consommations de chaque lot d'actifs est partagé de manière sécurisée avec les services des Douanes à la fin de chaque mois.



POINTS D'ATTENTION

Le recours à différentes sources d'information nécessite un travail de standardisation des données entre système d'information préalable.

La gestion des droits d'accès suppose la mise en place d'un consortium avec des règles de gouvernance précises.

L'utilisation d'un suivi automatisé permet ici de simplifier la compilation des données mais ne garantit pas la véracité des données inscrites : la responsabilité des membres du réseau est toujours engagée lors de la communication du bilan mensuel aux autorités.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : TRAÇABILITÉ

EXEMPLE : SUEZ - LA BLOCKCHAIN POUR INSTAURER UNE GESTION EFFICACE ET SÉCURISÉE DU CYCLE DE VIE DU PRODUIT

SITUATION INITIALE

BESOIN CLIENT

- Suez fait face à la nécessité de sécuriser la traçabilité des boues de ses stations d'épuration.
- Suez s'inscrit dans une démarche liée à l'économie circulaire : l'utilisation de la solution doit rendre possible in fine une réduction de l'empreinte environnementale de la fertilisation.
- Objectif : renforcer la confiance et la transparence dans la sécurité sanitaire et environnementale des boues.

OBSTACLES TECHNIQUES

- Une chaîne complexe d'informations à recueillir.
- Un pilotage simplifié de la gestion des flux de boues.

EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil.
- Partage sécurisé de l'information entre les partenaires sur la chaîne d'information : recours à un outil qui remplace les bases de données centralisées par Suez.
- Fiabilité des données inscrites.
- Responsabilisation de tous les partenaires sur la qualité des données fournies.
- Confidentialité des données en dehors des ayant-droits d'accès.

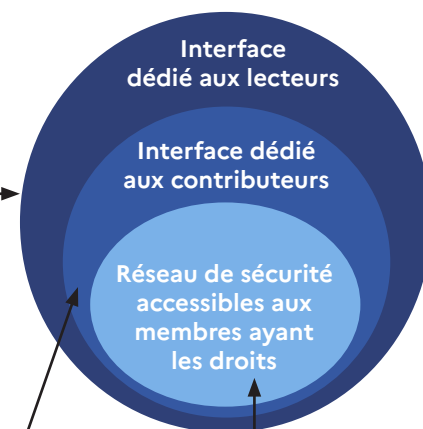
LA BLOCKCHAIN COMME SOLUTION

Pour consulter l'information sur un portail numérique de supervision, qui se substitue aux rapports périodiques statiques utilisés jusqu'alors.

Chaque acteur (producteur de boue, agriculteur, opérateur Suez) peut transmettre les informations au fil de l'eau au réseau via une inscription dans la blockchain :

- conformité de la gestion des flux et des opérations de valorisation effectuée par Suez ;
- suivi des stocks ;
- éventuels impacts liés à l'activité de valorisation du déchet organique (impact olfactif,...) ;
- apports de fertilisants sur les parcelles agricoles.

Cet interface succède aux documents papier et à la ressaisie des données.



Pour assurer le fonctionnement du réseau et la sécurité de l'historique des données d'exploitation collectées.

DÉROULÉ DU PROJET

La numérisation des données de terrain, la création du portail de supervision et l'étude des nouvelles technologies de traçabilité débutent en 2018. L'outil final est fonctionnel depuis le 1^{er} janvier 2020, avec un premier projet pour le compte d'une collectivité.

Résultats obtenus :

- en 2020, l'outil a permis de superviser la valorisation de 50 000 tonnes de boues, en partie épandues chez 150 agriculteurs et sur 20 000 ha. ;
- 400 tonnes d'azote et 320 tonnes de phosphore ont ainsi été apportées aux champs en substitution aux engrais de synthèse et issus de mines.

GOUVERNANCE

- **Périmètre** : à l'échelle acteur intervenant dans le cycle de gestion des boues et leur valorisation (producteur, agriculteur, opérateurs de Suez, autorité de contrôle) est engagé dans la fiabilité des informations qu'il partage.
- **Choix des droits** : accès en lecture, ajout d'informations, validation.
- **Choix du public cible de l'information compilée** : qui accèdera à la chaîne d'information de traçabilité sur le produit ?



POINTS D'ATTENTION

La mise en place du réseau blockchain requiert :

- la numérisation préalable des différents membres de la chaîne d'information ;
- la standardisation des données des différentes bases d'où l'information est tirée.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN

CAS D'USAGE THÉORIQUE : NON-FUNGIBLE TOKEN (NFT)

SITUATION INITIALE

BESOIN CLIENT

- Côté acheteur : avoir accès à une offre artistique/immobilière/ludique exclusive et numérique. Côté offreur : monétiser une œuvre ou un bien numérique en empêchant sa duplication.
- Stocker tout type de bien numérique sur la blockchain en y inscrivant également sa propriété sur ce bien.
- Garantir et valoriser l'authenticité d'un bien physique *via* une certification numérique même après sa vente. Ceci afin de limiter les risques de vol (chaque transaction étant traçable sur les réseaux blockchain) et de contrefaçon.

OBSTACLES TECHNIQUES

- Tracer le NFT au fil des transactions dont il est l'objet
- Dans le cas d'un NFT lié à un objet physique, assurer que cette association se fasse de manière sûre et inviolable.

EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil pour tous selon leurs droits d'accès.
- Fiabilité des données inscrites.
- Responsabilisation de tous les partenaires sur la qualité des données fournies.
- Délivrance d'une certification d'authenticité unique dans le cas d'un objet physique associé à un NFT.

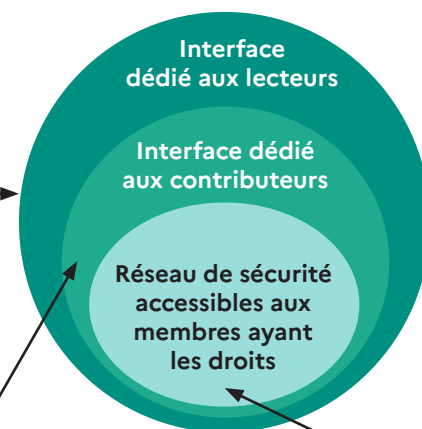
LA BLOCKCHAIN COMME SOLUTION

Pour consulter les informations sur le jeton non fongible (NFT) numériquement (exemple : sur smartphone *via* un QR code).

Pour enregistrer numériquement et de manière sécurisée l'objet physique sous un format non reproductible – le jeton non-fongible (NFT)

ET

Pour créer le jeton non-fongible NFT dans le cas d'un objet nativement numérique.



Pour assurer le bon fonctionnement de l'infrastructure numérique, celle-ci garantissant l'auditabilité des données sur la vie du jeton : création, achat, revente...

GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- **Périmètre** : choix du nombre de partenaires et de la taille du réseau (nombre de nœuds).
- **Choix des droits**
- **Choix du public cible de l'information compilée** : qui accédera à la chaîne d'information de traçabilité sur le produit ?

Plus de précisions sur les différents types de réseau blockchain disponible dans la section (*ajouter le numéro de la section sur les ≠ types de blockchains*).



POINTS D'ATTENTION

Les NFT soulèvent des enjeux de qualification juridique qui nécessitent d'être résolus pour instaurer plus de confiance pour les investisseurs et permettre l'émergence de nouveaux projets innovants.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : NFT

EXEMPLE : LE CONSORTIUM AURA

LE NFT COMME CERTIFICAT D'AUTHENTICITÉ D'UN PRODUIT DE LUXE

SITUATION INITIALE

- AURA : consortium entre LVMH, Prada, Richemont et des acteurs numériques (ConsenSys, Microsoft) pour créer une plateforme de certification des produits.

BESOIN CLIENT

- Se prémunir des contrefaçons .
- Garantir et valoriser l'authenticité de son produit même après sa vente.

OBSTACLES TECHNIQUES

- Une chaîne complexe d'informations à recueillir.
- Assurer un suivi à l'unité du produit même lors de sa revente entre particuliers.

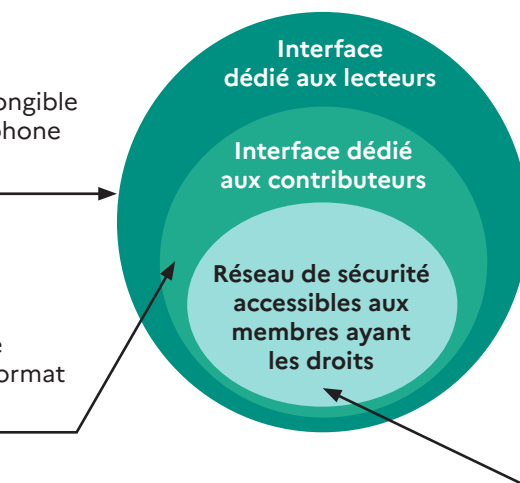
EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil pour tous les niveaux de contributeurs.
- Partage sécurisé de l'information entre les partenaires sur la chaîne d'information.
- Fiabilité des données inscrites
- Responsabilisation de tous les partenaires sur la qualité des données fournies.
- Délivrance d'un certification d'authenticité unique par produit.

LA BLOCKCHAIN COMME SOLUTION

Pour consulter les informations sur le produit, représenté via un jeton non fongible numériquement (exemple : sur smartphone *via* un QR code).

Pour enregistrer numériquement et de manière sécurisée le produit sous un format non reproductible : le NFT.



Pour assurer le bon fonctionnement de l'infrastructure numérique, celle-ci garantissant l'auditabilité des données inscrites.

GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- **Périmètre** : international, mais choix d'un nombre restreint d'acteurs pour gérer le réseau de sécurité, *via* une blockchain privée.
- **Choix des droits** : AURA est un consortium dans lequel toute marque de luxe peut devenir contributeur.
- **Choix du public cible de l'information compilée** : le consommateur peut utiliser l'application de la marque pour recevoir le certificat AURA lors de l'achat, contenant toutes les informations sur le produit. Il peut faire valoir le certificat d'authenticité dans le cas d'une revente.



POINTS D'ATTENTION

- La mise en place du réseau blockchain requiert :
- la numérisation préalable des différents membres de la chaîne d'information ;
 - la standardisation des données issues des systèmes d'informations des différentes marques de luxe contributrices.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : NFT

EXEMPLE : LE NFT ASSOCIÉ À UNE ŒUVRE ARTISTIQUE NUMÉRIQUE

SITUATION INITIALE

BESOIN CLIENT

- Monétiser une œuvre numérique en empêchant sa duplication.

OBSTACLES TECHNIQUES

- Empêcher la duplication de l'œuvre en lui associant un marqueur unique infalsifiable : le NFT.
- Tracer le NFT au fil des transactions dont l'œuvre est l'objet.

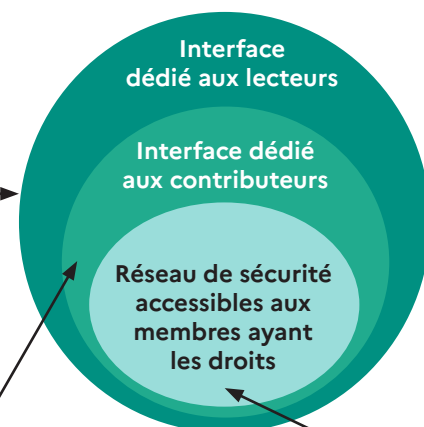
EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil pour tous les niveaux de contributeurs.
- Sécurisation du droit de propriété sur le NFT de son acquéreur et suivi de ce droit lors d'éventuelles reventes.

LA BLOCKCHAIN COMME SOLUTION

Pour consulter les informations sur le NFT (exemple : sur smartphone *via* un QR code) : l'œuvre, son artiste, son propriétaire actuel.

Pour transformer l'œuvre numérique en version unique et infalsifiable : l'ajout du NFT est demandé par l'artiste qui paye en cryptomonnaies pour cette action.



Pour générer un fichier digital unique et non-duplicable : il est estampillé avec un marqueur valant titre de propriété : le NFT. Lors de la revente de l'œuvre, le NFT change de main. Alors, un contrat intelligent peut enclencher le paiement d'un pourcentage du prix de revente à destination de l'artiste (en cryptomonnaies).

GOUVERNANCE

- Le réseau sur lequel s'opère la plupart des créations de NFT en 2021 est celui d'Ethereum, une blockchain publique.
- Lorsqu'un collectionneur acquiert une œuvre d'art NFT, il achète en réalité un certificat de propriété d'une œuvre d'art virtuelle.
- Il pourra céder ce NFT et sera alors rémunéré en crypto-monnaies.



POINTS D'ATTENTION

Les NFT soulèvent des enjeux de qualification juridique et il existe une incertitude sur le régime fiscal qui leur est applicable.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN

CAS D'USAGE THÉORIQUE : MONNAIES NUMÉRIQUES

SITUATION INITIALE

BESOIN CLIENT

• Accélérer les processus financiers assurés par les chambres de compensation que sont le KYC (*know your customer*), la réconciliation des données et de la gestion des risques.

OU

• Créer un écosystème de transactions rapides *via* une monnaie numérique. Les transactions devront être effectuées de manière moins coûteuse qu'avec un système centralisé *via* une banque, tout en ayant un haut niveau de sécurité garanti.

OU

• Bénéficier d'un outil pour réaliser des projets de finance décentralisée.

OBSTACLES TECHNIQUES

• La collecte rapide d'un grand nombre de données.
• Un besoin de transparence sur les actions réalisées dans les processus financiers tout en protégeant les données privées des parties prenantes.

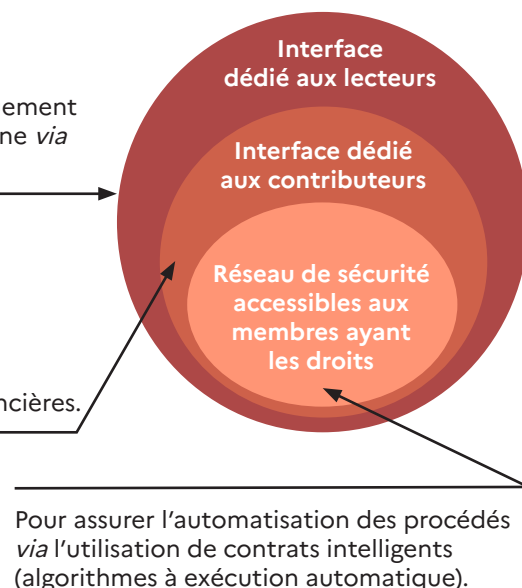
EXIGENCES TECHNIQUES DE LA SOLUTION

• Accessibilité de l'outil pour les contributeurs et lecteurs tout en assurant une confidentialité des données sensibles.
• Contrôle facilement réalisable par les organismes régulateurs.
• Fiabilité des données inscrites.

LA BLOCKCHAIN COMME SOLUTION

Pour consulter l'information numériquement et facilement (exemple : sur smartphone *via* un QR code)

Pour transmettre numériquement les informations financières nécessaires à l'automatisation des transactions financières.



GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

- **Périmètre** : choix du nombre de partenaires et de la taille du réseau (nombre de nœuds).
- **Choix des droits** : accès en lecture, ajout d'informations, validation des données inscrites.
- **Choix du public cible de l'information compilée** : qui accédera aux informations de transactions réalisées.

Plus de précisions sur les différents types de réseau blockchain disponible dans la section (*ajouter le numéro de la section sur les types de blockchains*).



POINTS D'ATTENTION

- La mise en place du réseau blockchain pour automatiser les transferts d'informations dans un cadre financier requiert :
 - l'anonymisation préalable des données ;
 - l'anticipation des droits d'accès aux différentes données entrées par les contributeurs ;
 - la formation des différentes parties prenantes au mode de gouvernance décentralisé d'un réseau blockchain ;
 - la bonne compréhension du contexte réglementaire, qui est encore en cours de création.
- Distinction entre cryptomonnaie à valeur intrinsèque et monnaie numérique adossée à une monnaie fiduciaire ou à un métal* : la seconde est appelée *stablecoin*, son atout principale est sa stabilité accrue, son défaut est le recours souvent nécessaire à un intermédiaire (centralisation).

Remarque : certains *stablecoins* sont adossés à des cryptomonnaies à valeur intrinsèque, le mécanisme pour contrer leur volatilité est un contrôle par contrat intelligents, lorsque le cours fluctue énormément, des jetons sont détruits pour le stabiliser.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : MONNAIES NUMÉRIQUES

EXEMPLE : UTILISER UNE MONNAIE NUMÉRIQUE POUR OPTIMISER SES ACTIVITES DE CHAMBRE DE COMPENSATION

SITUATION INITIALE

BESOIN CLIENT

- Chambres de compensation : accélérer et faciliter le processus de réconciliation des données lors d'une transaction financières.

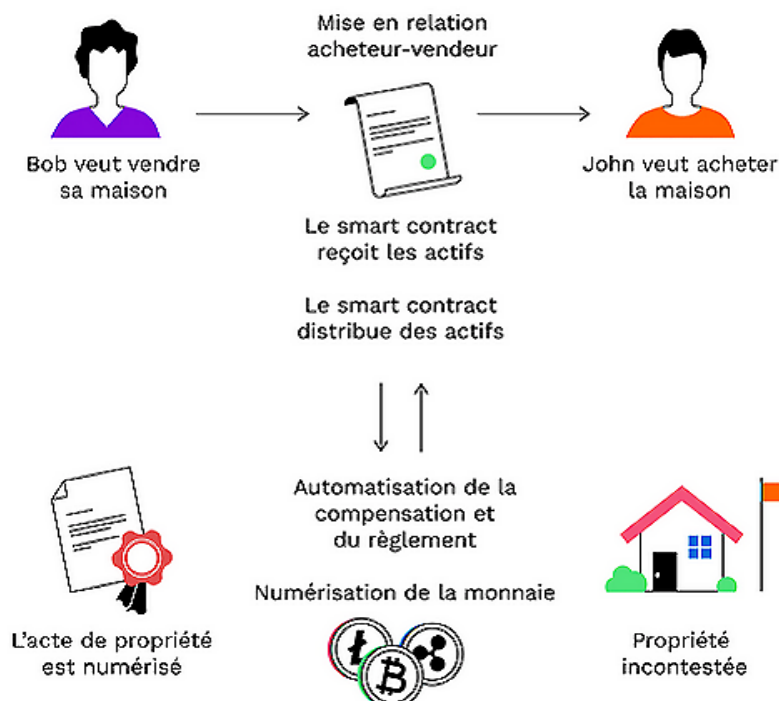
OBSTACLES TECHNIQUES

- La collecte rapide d'un grand nombre de données tout en réduisant le risque d'erreur.
- Un besoin de transparence sur les actions réalisées dans les processus financiers tout en protégeant les données privées des parties prenantes.

EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil pour les contributeurs et lecteurs tout en assurant une confidentialité des données sensibles.
- Contrôle facilement réalisable par les organismes régulateurs.
- Fiabilité des données inscrites.

LA BLOCKCHAIN COMME SOLUTION



GOUVERNANCE

DÉMARCHES POUR MONTER UN RÉSEAU

Le processus de compensation nécessite la réconciliation de données venant d'acteurs différents définis lors de la création du réseau.

- **Périmètre** : les contributeurs partagent leurs données sur un registre commun protégé et dont l'accès est limité aux ayant-droits ;
- Les opérations de réconciliation sont automatisées sur l'infrastructure blockchain *via* des smart contracts.
- Lecture et suivi en temps réel pour tous les acteurs autorisés des opérations réalisées.
- Accès aux données de reportings, audits réalisables pour les autorités régulatrices.



POINTS D'ATTENTION

La mise en place du réseau blockchain pour automatiser les transferts d'informations dans un cadre financier requiert :

- l'anonymisation préalable des données ;
- l'anticipation des droits d'accès aux différentes données entrées par les contributeurs ;
- la formation des différentes parties prenantes au mode de gouvernance décentralisé d'un réseau blockchain.
- la bonne compréhension du contexte réglementaire, qui est encore en cours de création.

I. CAS D'USAGE MÉTIERS DE LA BLOCKCHAIN CAS D'USAGE THÉORIQUE : MONNAIES NUMÉRIQUES

EXEMPLE : S'APPUYER SUR LE *STABLECOIN* « LUGH » POUR CRÉER UNE COMMUNAUTÉ D'UTILISATEURS

SITUATION INITIALE

BESOIN CLIENT

- Le projet Lugh est porté par le groupe Casino, la Société Générale et la plateforme d'échange Coinhouse. Il a pour buts de :
- créer un écosystème de transactions rapides via une monnaie numérique stable, le « Lugh ».
- créer de nouveaux usages innovants autour de nouvelles méthodes de paiement décentralisées.

OBSTACLES TECHNIQUES

- La collecte rapide d'un grand nombre de données
- Les transactions devront être effectuées de manière moins coûteuse qu'avec un système centralisé via une banque mais avec un haut niveau de sécurité

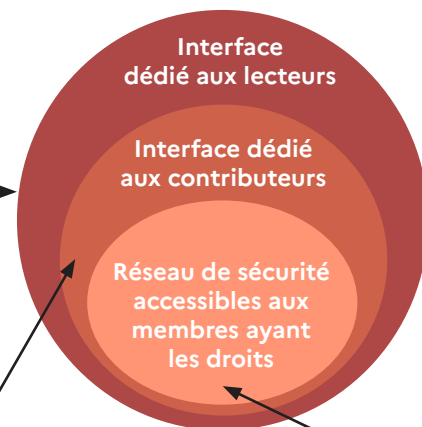
EXIGENCES TECHNIQUES DE LA SOLUTION

- Accessibilité de l'outil pour les contributeurs et lecteurs tout en assurant une confidentialité des données sensibles
- Assurer la stabilité du cours du stablecoin entre monnaies numérique et fiduciaire : pour un jeton « lugh » émis, un euro est conservé sur un compte bancaire dédié.
- Contrôle facilement réalisable par les organismes régulateurs
- Fiabilité des données inscrites

LA BLOCKCHAIN COMME SOLUTION

Pour que l'utilisateur puisse accéder aux informations sur le nombre de Lugh qu'il détient, ses transactions réalisées, le cours du Lugh, etc.

Pour transmettre numériquement les informations financières nécessaires à la création et aux transactions en Lugh.



Pour assurer la création des Lugh et leur circulation entre la communauté de détenteurs de manière automatisée et sécurisée. Chaque Lugh crée est adossé à un euro dans un compte dédié.

GOUVERNANCE

- **Périmètre** : il s'agit d'un réseau sur blockchain fermée, où la Société Générale est teneur des comptes en euros, le cabinet d'audit PwC atteste chaque mois du nombre de jetons Lugh émis ainsi que le solde du compte bancaire associé domicilié chez Société Générale. Casino et Coinhouse assurent quant à eux l'accès aux jetons Lugh pour leur utilisateurs.
- Dans la première phase du projet, le Lugh est proposé aux clients de la plateforme Coinhouse afin de faciliter les opérations sur cryptoactifs pour les investisseurs particuliers ou professionnels qui cherchent à se prémunir du risque lié à la volatilité de ces marchés.
- À terme, cela pourrait se concrétiser par la création d'un consortium d'acteurs *B2C* intégrant le Lugh au sein d'un programme de fidélité et de paiement décentralisé.
- Aujourd'hui, plus de 5M d'EURL ont été émis.



POINT D'ATTENTION

L'utilisation de la blockchain dans un contexte de réseau fermé restreint la décentralisation des échanges : les intermédiaires porteurs du projet deviennent ainsi la porte d'accès incontournables aux jetons numériques proposés.

II. RECOURIR À LA BLOCKCHAIN QUELQUES CRITÈRES DE CHOIX

LA TECHNOLOGIE BLOCKCHAIN
RÉPOND-ELLE À VOS BESOINS ?

Avez-vous besoin d'un système commun d'accès aux informations bénéficiant d'un haut niveau de sécurité ?



Y a-t-il plus d'une entité qui doivent fournir des données pour construire les enregistrements blockchain ?



Souhaitez-vous que vos données soient non modifiables et puissent être auditées à tout moment ?



Rencontrez-vous des problématiques de confiance avec vos partenaires ?



Voulez-vous disposer d'un répertoire inviolable de toutes les écritures inscrites dans le système ?

**NON**

La blockchain offre un accès à un stockage d'enregistrements cryptés. Si cela n'est pas votre besoin, utilisez plutôt : emails, feuilles de calcul.

NON

La blockchain est généralement utilisée par plusieurs organisations qui ont besoin d'échanger de l'information de manière sécurisée. Si vous souhaitez échanger en interne de votre organisation, utilisez plutôt : base de données.

NON

La blockchain ne permet pas de modifier les données historiques enregistrées ; elles sont fortement auditable car gage de transparence. Si cela ne vous convient pas, utilisez plutôt : base de données.

NON

S'il n'y a pas de problèmes de confiance ou de contrôle sur la personne qui dirige le système, le recours à la blockchain est moins pertinente. Dans ce cas, vous pouvez plutôt utiliser : base de données partagée.

NON

Si vous n'avez pas besoin d'auditer ce qui s'est passé et quand, la blockchain est moins pertinente.

II. RECOURIR À LA BLOCKCHAIN QUELQUES CRITÈRES DE CHOIX

QUELLES SONT LES PRINCIPALES DIFFÉRENCES ENTRE LES TYPES DE BLOCKCHAIN ?

Blockchain publique	Blockchain permissionnée - de consortium
Lecture et écriture ouvertes.	Écriture restreintes avec droit d'accès donné par les membres du consortium.
L'identité de l'utilisateur est protégée.	L'identité de l'utilisateur est connue des autres membres.
Chaque utilisateur a accès à tous les blocs.	Les membres du réseau peuvent choisir à qui ouvrir la lecture des informations inscrites.
Chaque utilisateur peut participer à la création d'un nouveau bloc.	Les membres peuvent participer à la création d'un bloc selon les règles qu'ils se sont fixés.

QUELS SONT LES POINTS COMMUNS ENTRE LES DIFFÉRENTS TYPES DE BLOCKCHAIN ?

Les réseaux sont décentralisés : le groupe de membres est garant de la solidité du réseau.

Le registre des transactions est commun : il n'y a pas de version originale et de copie, chacun dispose d'un original du registre.

Elles exigent toutes que chaque **transaction** soit **signée numériquement et sécurisée par cryptographie**.

Les données « visibles » sont dans tous les cas chiffrées : voir le *hash* ne permet donc pas de voir la donnée réelle, même dans une blockchain publique.

Elles s'appuient toutes sur un cadre de fonctionnement : un protocole et un consensus.

II. RECOURIR À LA BLOCKCHAIN QUELQUES CRITÈRES DE CHOIX

QUELS TYPES DE BLOCKCHAIN POUR QUELS CAS D'USAGE ?

Blockchain publique

Exemple de cas d'usage correspondant

- Désintermédiation des transactions de monnaie virtuelle.
- Ancrage.
- Notarisation.
- Certification de documents officiels (exemple : diplôme).
- Traçabilité (contrefaçon des médicaments, œuvres, des droits d'auteur, etc.).

Atout de ce type de blockchain

- Est « prête à l'emploi ». Il n'est pas nécessaire de monter un consortium, ni de déployer de nœuds chez les acteurs de l'écosystème.
- Dispose d'un niveau de décentralisation très élevé, d'une forte résistance à la censure et aux collusions.
- Assure une transparence et une traçabilité des transactions en l'absence d'un tiers de confiance, donc un moindre coût de tenue de compte.

Inconvénients/limites

- Ne permet pas de créer une blockchain « sur-mesure ».
- La consommation énergétique est d'autant plus grande que le réseau accueille un grand nombre de membres.
- Les durées de traitement peuvent être allongées lorsque le nombre de membres grandit.
- Les transferts sont rarement modifiables après coup : une erreur de transaction est difficile à annuler.

Blockchain permissionnée dite de consortium

Exemple de cas d'usage correspondant

- Tout cas d'usage où une organisation décentralisée ou plusieurs organisations ont besoin de numériser et maîtriser les échanges entre les membres qui la composent.
- Audit.
- Traçabilité (transport, logistique dans les industries aéronautiques, automobiles, agroalimentaires).
- Transactions financières : *shared KYC* ; infrastructure de place pour simplifier l'émission et les transferts d'actifs.

Atout de ce type de blockchain

- Moins consommatrice en énergie que les blockchains publiques actuelles.
- Garantit une sécurité suffisante si le nombre de nœuds est adéquat, d'autant plus que, ses membres étant identifiés, ils sont moins enclins à frauder.
- Permet de définir un réseau blockchain miroir de l'organisation : lecture, écriture, révocation des membres, etc.
- Offre un système sécurisé avec une gouvernance stricte.
- Préserve la confidentialité des données (*privacy*).
- Permet l'ajout sous contrôle d'un nouveau membre.
- Assure un suivi adapté au format du produit (lot, parcellaire, etc) tout au long de son cycle de production.
- Permet de suivre les réglementations contraignantes rapidement sans modification complète du SI existant. Coût moins élevé qu'un multi cloud.

Inconvénients/limites

- Les protocoles peuvent rencontrer des problèmes d'interopérabilité avec d'autres systèmes blockchain.
- Les systèmes peuvent rencontrer des difficultés de passage à l'échelle.
- Les détenteurs des nœuds, en nombre limité, vérifient et valident eux-mêmes les transactions. La validité des informations délivrées aux personnes extérieures repose donc sur la confiance ; sans aucune possibilité de contrôle sur la bonne vérification des données par les membres.
- Avec moins de nœuds, il est beaucoup plus facile pour un hacker de prendre le contrôle du réseau et de manipuler les données qui y sont inscrites que dans le cas d'une blockchain publique.

II. RECOURIR À LA BLOCKCHAIN QUELQUES CRITÈRES DE CHOIX

EST-IL POSSIBLE DE RÉDUIRE LA CONSOMMATION ÉNERGÉTIQUE DE SON RÉSEAU BLOCKCHAIN ?

Les données ci-dessous sont issues d'études récentes mais les réseaux publics accueillant sans cesse de nouveaux nœuds, les chiffres sont ici un simple appui de démonstration.

Blockchain publique	Grand nombre de validateurs	Pistes de réduction de la consommation énergétique
Le réseau Bitcoin consommait 45,8 TWh en 2019.* Ceci correspond à la consommation d'un pays comme le Sri Lanka ou la ville de Kansas City en un an. À titre comparatif, la consommation énergétique des datacenters du cloud de l'UE28 est de 76,8 TWh/an en 2018.* * étude de l'Université technique de Munich, 2019. * Étude PIPAME : Blockchain : État de l'art et perspectives pour la France, 2019 ; Etude Datalab, chiffres de l'énergie en France, 2020.	La validation des transactions selon la méthode du consensus par preuve de travail, entraîne des grands temps de traitement informatique. Une pression supplémentaire sur les ressources se produit à chaque fois qu'un nouveau nœud complet est créé. Ce fonctionnement est utilisé en l'absence de confiance entre les utilisateurs qui ne se connaissent pas.	Fonctionnement « preuve d'enjeu » : la validation des transactions consommerait 99 % moins d'énergie qu'avec un fonctionnement en preuve de travail selon ses défenseurs. Mais cela représenterait tout de même plus du double de la consommation énergétique d'une transaction bancaire traditionnelle (cf. <i>graphique comparatif ci-après</i>). Développement des <i>lighting networks</i> visant également à réduire la consommation énergétique et l'engorgement des réseaux.

Blockchain permissionnée – de consortium	Nombre réduit de validateurs	Pistes de réduction de la consommation énergétique
Les membres accèdent et agissent sur le réseau <i>via</i> des droits d'accès.	Fonctionnement « preuve de travail » parfois maintenu, ce qui induit une consommation énergétique importante mais réduite par rapport à une blockchain publique car le nombre de validateurs est restreint : le réseau est plus petit.	À la limitation de la taille du réseau peut s'ajouter le fonctionnement par « preuve d'enjeu ». Cette combinaison permet une réduction importante de la consommation énergétique induite par rapport à une blockchain publique fonctionnant sous preuve de travail.

➔ Quel que soient le type de réseau et le type de protocole choisis, la consommation énergétique demeure un point clé à prendre en compte dans l'élaboration d'un projet blockchain.

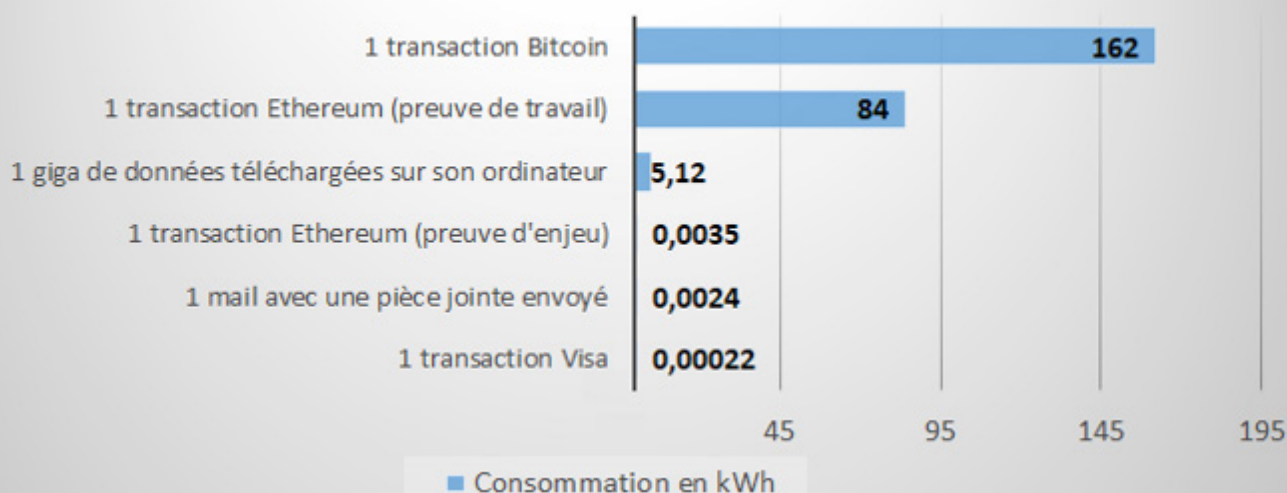
II. RECOURIR À LA BLOCKCHAIN QUELQUES CRITÈRES DE CHOIX

QUE REPRÉSENTE LA CONSOMMATION ÉNERGÉTIQUE D'UNE TRANSACTION SUR UN RÉSEAU DE CRYPTOMONNAIES ?



Avec 1 kWh, on peut regarder la TV entre 3 et 5 heures selon la taille et la technologie de son téléviseur.

Consommation en kWh (données 2021)

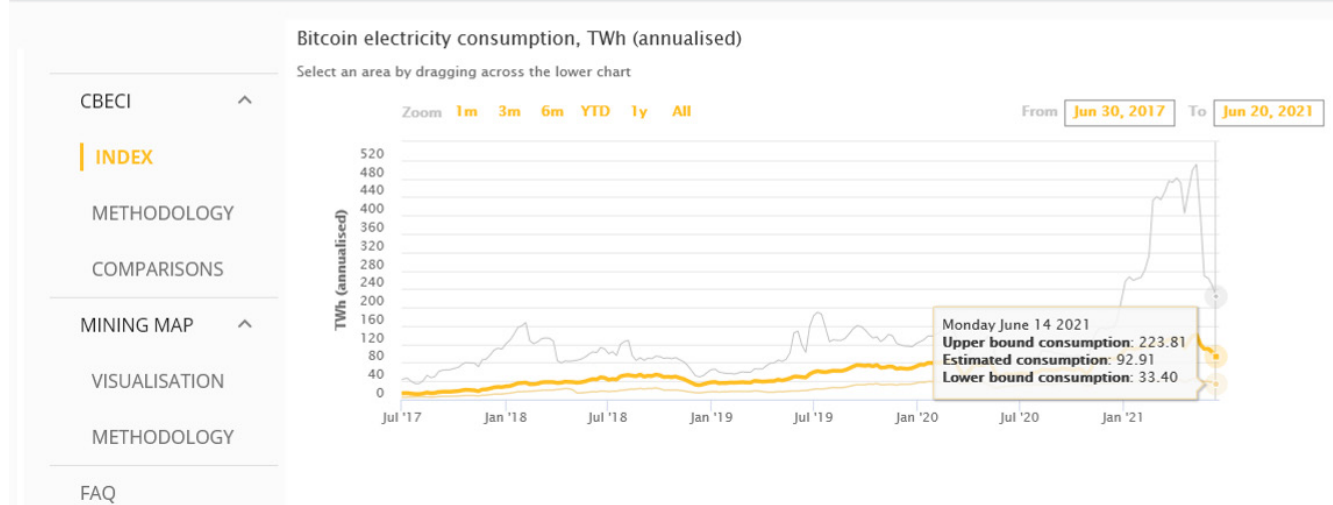


QUE REPRÉSENTE LA CONSOMMATION ÉNERGÉTIQUE ANNUELLE DU RÉSEAU BITCOIN ?



Cambridge
Centre
for Alternative
Finance

Cambridge Bitcoin Electricity Consumption Index



- La consommation énergétique d'un réseau tel que celui du Bitcoin représentait 32 TWh fin 2018, 67 TWh fin 2019 et 93 TWh en juin 2021 (étude de l'université de Cambridge, cf. ci-dessus).
- Ce réseau a entraîné l'émission de 3 à 15 millions de tonnes de CO₂ sur 2016-2018 (étude de M. J. Krause, T. Tolaynet, 2018), les émissions de gaz à effet de serre des grandes banques françaises seulement en 2018 représentaient 2 milliards de tonnes de CO₂ (étude Les Amis de la Terre France et Oxfam France, 2019).

FOIRE AUX QUESTIONS

LA BLOCKCHAIN REND-T'ELLE LES INFORMATIONS INSCRITES INFALSIFIABLES OU VÉRIDIQUES ?

Sous conditions, la blockchain garantit que les données soient infalsifiables. Cette propriété dépend de la qualité du réseau qui supporte la blockchain, mais n'est pas une propriété intrinsèque de la technologie.

La blockchain ne garantit pas que les données inscrites soient vraies. Cependant, la possibilité d'un audit incite les acteurs à mettre à disposition des informations exactes.

Condition d'infalsifiabilité : il faut s'assurer que les nœuds du réseau sont réellement distribués entre plusieurs acteurs. Si un acteur possède tous les nœuds ou accède à tous les nœuds (ex opérateurs techniques) alors modifier les données ne présente aucune difficulté pour lui.

À noter : en cas de donnée erronée, une nouvelle information peut être enregistrée en lieu et place de celle-ci. Cette nouvelle saisie est enregistrée avec une signature électronique différente de la précédente. L'ajout est rendu visible et peut être audité.

QU'EST-CE QU'UN CONSORTIUM AUTOUR DE LA BLOCKCHAIN ?

Un groupe d'entreprises ayant fixé ensemble une règle de gouvernance sur les données qu'elles vont partager *via* l'inscription d'empreintes sur la blockchain.

PUIS JE DÉVELOPPER UN PROJET BLOCKCHAIN AVEC DES CONCURRENTS TOUT EN GARDANT UNE TOTALE CONFIDENTIALITÉ DES DONNÉES INSCRITES ?

Oui, car les règles du jeu sont définies par les membres : choix de gouvernance du consortium et choix du mécanisme de consensus adopté.

Ainsi, il est possible de définir des données partagées, éventuellement encryptées par des clefs communes, et des données privées, encryptées par des clefs confidentielles accessibles à plusieurs membres choisis. La technologie blockchain permet ces transactions confidentielles.

LA BLOCKCHAIN PERMET T'ELLE DE STOCKER DES DONNÉES PARTAGÉES ? QUELLE EST LA DIFFÉRENCE AVEC UNE BASE DE DONNÉES ?

Non, sur la blockchain on stocke de manière décentralisée des preuves – ou empreintes – numériques qui correspondent à des transactions.

La possession de la seule empreinte numérique n'est pas suffisante pour reconstituer les données d'origine.

La différence avec la base de données réside principalement dans sa décentralisation et son immutabilité. Alors que tous les enregistrements sécurisés sur une base de données sont centralisés, chaque participant à une blockchain dispose d'une copie sécurisée de tous les enregistrements et de toutes les modifications afin que chaque utilisateur puisse visualiser la provenance des données.

EST-IL COMPLIQUÉ ET CÔUTEUX DE METTRE EN OEUVRE UN PROJET BLOCKCHAIN ?

L'enregistrement d'empreintes de données dans la blockchain n'est ni très compliqué ni très coûteux opérationnellement.

En revanche, un travail amont conséquent peut être nécessaire pour préparer les données (numérisation, standardisation, liaison des données unitaires les unes aux autres, etc.). De même, un portail de restitution peut s'avérer utile pour présenter les empreintes de données enregistrées.

Plusieurs prestataires du cloud ou prestataires blockchain offrent aujourd'hui des solutions à des coûts opérationnels équivalents à des prestations sur base de données standard.

QUELS SONT LES AVANTAGES DE LA BLOCKCHAIN PAR RAPPORT AUX SOLUTIONS / TRADITIONNELLES ?

La blockchain permet de casser les silos existants dans l'enregistrement des transactions. Cet enregistrement s'effectue en s'appuyant sur la sécurité et la rapidité du protocole. Les données enregistrées sont traçables et auditable, ce qui les rend hautement fiables. La solution blockchain permet ainsi d'adresser de nouveaux cas d'usage que l'IT traditionnel ne couvre pas ou peu.

DOIS-JE MODIFIER MON SYSTÈME D'INFORMATIONS POUR INTÉGRER DE LA BLOCKCHAIN ?

La blockchain vise la collecte d'information auprès de multiples acteurs. En cela, c'est bien souvent un système inter-organisations.

Si l'état initial de votre SI permet un interfaçage aisé avec un tel système (via des API) alors les modifications induites seront réduites.

Toutefois, il peut être nécessaire de mener un travail de numérisation, standardisation et uniformisation des données avant de lancer le projet de blockchain.

FOIRE AUX QUESTIONS

LE SYSTÈME EST-IL **PÉRENNE** ? QUELS SONT LES RISQUES DE DÉFAILLANCE DE LA TECHNOLOGIE ?

La technologie blockchain repose sur des éléments technologiques éprouvés, qu'on retrouve dans d'autres domaines tels que la signature électronique et le chiffrement des données.

Les risques associés sont donc de même ordre que pour des cas d'usages utilisant traditionnellement ces solutions.

QU'EST-CE QU'UN **SMARTCONTRACT** ?

Un smart contract est un programme informatique qui garantit l'exécution automatique d'un contrat lorsque les conditions convenues sont remplies.

C'est un protocole numérique enregistré de manière distribué et donc non modifiable.

QU'EST CE QU'UN **JETON** ? COMMENT L'UTILISE-T-ON ?

Un jeton est une représentation numérique d'un actif, d'un droit ou d'un objet.

Ce jeton peut être échangé entre deux parties sur Internet sans avoir besoin, pour cela, de l'autorisation d'un tiers.

QUELLE EST LA DIFFÉRENCE ENTRE **BLOCKCHAIN** ET **CRIPTOACTIF** ?

On appelle communément blockchain la mise en œuvre d'une combinaison de technologies permettant de faire de l'horodatage de transactions. Un crypto actif est un jeton financier émis et échangé sur une blockchain.

Un crypto actif est un cas d'usage de la blockchain ; d'autres cas d'usage existent et ne nécessitent pas de crypto actif.

EST'IL VRAI QUE LA BLOCKCHAIN ENTRAÎNE UNE **FORTE CONSOMMATION ÉNERGÉTIQUE** ? COMMENT LA **LIMITER** ?

La principale caractéristique d'une blockchain publique est l'anonymat des nœuds/miners et leur nombre, souvent important. La preuve de travail, une des caractéristiques techniques des blockchain actuelles, fonctionne alors en entraînant une consommation énergétique très élevée. En identifiant les nœuds et en limitant le nombre, on limite mécaniquement les consommations énergétiques.

De plus, de nombreux travaux de recherche sont actuellement menés pour trouver des alternatives au mécanisme de preuve de travail.

Pour en savoir plus, consulter l'article dédié du cnrs : <https://ecoinfo.cnrs.fr/2020/02/11/consommation-energetique-des-technologies-blockchain/>



CONTRIBUTEURS À CE GUIDE

Pour leur grande contribution aux différentes consultations, merci à :

Frédéric	BAUD	De : Primis Finance	Matthieu	HUG	De : Tilkal
Kheira	BENMERIDA	De : Palico	Julie	KLEIN	De : Suez
Mathieu	BORGÉ	De : Foodgates	Najah	NAFFAH	De : Systematic PR
Xavier	CHARPENTIER	De : Trido tech	Odile	PANCIATICI	De : groupe renault
Sébastien	DUPLAN	De : Groupe Renault	Bertrand	PEAUDECERF	De : Tessi
Laure	DURAND	De : Caves du Ranzan	Patrice	VAN DE VELDE	De : Unblocked
Mona	EL JADAOUI	De : Systematic Paris région	Alban	VENDEUVRE	De : Lugh -Groupe Casino
Benjamin	FARAGGI	De : Spuro			

Merci aux membres du groupe de travail dédié à l'élaboration de ce guide :

Irène	ALLAIS	De : Ministère de l'Agriculture et de l'Alimentation - DGPE 6 BEI
Emmanuelle	ANCEAUME	De : CNRS
Daniel	AUGOT	De : INRIA école polytechnique
William	AURIOL	De Unbank
Quentin	BARLUET DE BEAUCHESNE	De : Ownest
Juliette	BERTHIER	De : Ministère de la Culture - DGMIC
Élodie	BOUDOUIN	De : DGE
Timotheé	BRUGIÈRE	De : Trabschain
Gilles	CADIGNAN	De : Woleet
Jean-François	CESARINI	De : Député de l'Assemblée nationale
Benoît	CHAMBON	De : Maarkt
Ariane	CHÉREL	De : Université Paris-Saclay
Amel	CHERFAOUI	De : BYOM
Carole	CHERRIER	De : CAPIMMAT
Fabrice	CROISEAUX	De : InTech
Loÿs	DE LA SOUDIÈRE	De : GoodsID
Amandine	DOAT	De : Ledger
Vincent	DORUT	De : Vdorut
Marc	DURAND	De : Kapalt
Benjamin	GAYRAUD	De : Axiane Meunerie
Françoise	GORGA	De : ANIA
Delphine	GUILLAUME	De : EY
Corentine	HOLDSWORTH	De : Vicat
Xavier	HUA	De : Institut du Commerce
Céline	ISSARD-GUILLOT	De : Dirrecte AURA
Maxime	JEANTET	De : Kapalt
Luc	JODET	De : Arianee
Mikael	KAIS	De : TenChains SAS
Jihane	KHOUZAIMI	De : Fédération Française de l'Assurance
Yoni	LASRY	De : Cabinet d'avocats
Florian	LE GOFF	De : Synaps.io
François	LECOMTE-VAGNIEZ	De : LILLUP
Philippine	LEFÈVRE-ROTTMANN	De : Syntec Numérique
Alexandra	LEGRIS	De : MEF/DGE
Christophe	LEMEE	De : Deep Block
Mathieu	LESUEUR	De : Talan
Romain	MENETRIER	De : Emblock
Maxime	MICHELOT	De : Crystalchain
Cesare	MIGLIACCIO	De : ADSN
Nelly	MOFFETT	De : TAAL project
Nazim	MORERA	De : maarkt
Patrick	MULLER	De : CRCC de Colmar
Najah	NAFFAH	De : Blockchain Secure
Philippe	OGIER	De : DROON
Milan	ORBAN	De : Havas Blockchain
Margot	PAGES	De : Blockchain Xdev
Bertrand	PEAUDECERF	De : tessi
Isabelle	PEREIRA	De : De: SACEM
Alexandre	QUERTAMP	De : EY
Michel	RAYNAL	De : IRISa, Université Rennes 1
Patrice	REMEUR	De : Good info
Alain	ROSET	De : La Poste
Jordane	RUIZ	De : IBM Interactive
Sk	SOHEIL	De : The Blockchain Group
Salim	TALOUT ZITAN	De : Sia Partners
Clément	TÉQUI	De : eleven strategy
Pascal	URIEN	De : Telecom ParisTech
Lou	VETTIER	De : MEFR
Frédéric	VOLLE	De : In Vivo (Bioline)
Vincent	WAHL	De : Ministère de l'agriculture et de l'alimentation/DGPE/DMEA
Yanyan	YANG	De : GS1 France