



# L'avenir des SII

Cloud Computing  
Blockchain



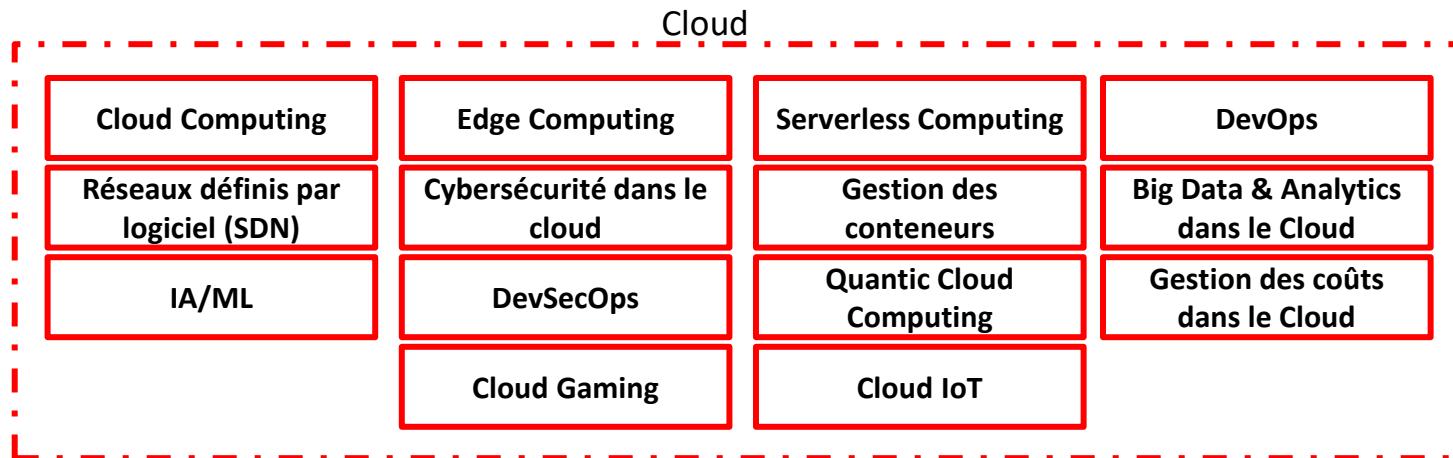
ÉCOLE  
**CENTRALE** LYON

# Cloud Computing Acteurs et stratégies

Module “Défis Informatique du Big Data”

Un cours de Yann FORNIER

# L'écosystème du Cloud



# Le Cloud Computing : Qu'est ce que c'est ?

Le Cloud Computing est un modèle de prestation de services informatiques via internet.

Plutôt que d'avoir des serveurs, des stockages et des applications physiquement présents sur site, les utilisateurs accèdent à ces ressources via des connexions Internet à partir de fournisseurs de services cloud.



Le **Cloud Computing** est la livraison **sur demande** de puissance de calcul, de bases de données, d'applications et diverses ressources informatiques **via Internet** et dont le paiement de ses ressources se fait **à l'utilisation**. ("pay-as-you-go")

# “Considérer l'infrastructure comme un logiciel”

Le Cloud Computing vous demande de considérer **l'infrastructure physique** comme une couche logicielle.



The screenshot shows the AWS CloudFormation console. On the left, the navigation pane includes sections like Home, Resources, Stack Requests, and Outputs. The main area displays the following details:

- Resources**:
  - Running instances: 1 - Elasti-01, 0 - Dedicated Hosts
  - Stacks: 0 - Instances, 1 - Load balancer, 0 - Lambda function, 0 - Function event source
  - Outputs: 0 - Service endpoint, 0 - Function endpoint
- Launch instance**: A button labeled "Launch instance" is present.
- Scheduled events**: Shows 100 items (0 copied).
- Service health**: Status: 0 services (0 failed), This service is operating normally.
- Zone status**: Shows 1 zone (0 failed), 0 zones (0 failed), 0 zones (0 failed), 0 zones (0 failed).
- Additional information**: Includes links to "Save to my AWS Lambda function", "Optimize price performance by combining RDS database options in a single RDS Multi-AZ cluster", and "Enable best Price Performance with AWS Lambda".

# Le modèle classique informatique



**Le modèle classique** (ou “on-premise”) en informatique demande pour fonctionner des solutions physiques (serveurs, data centers..)

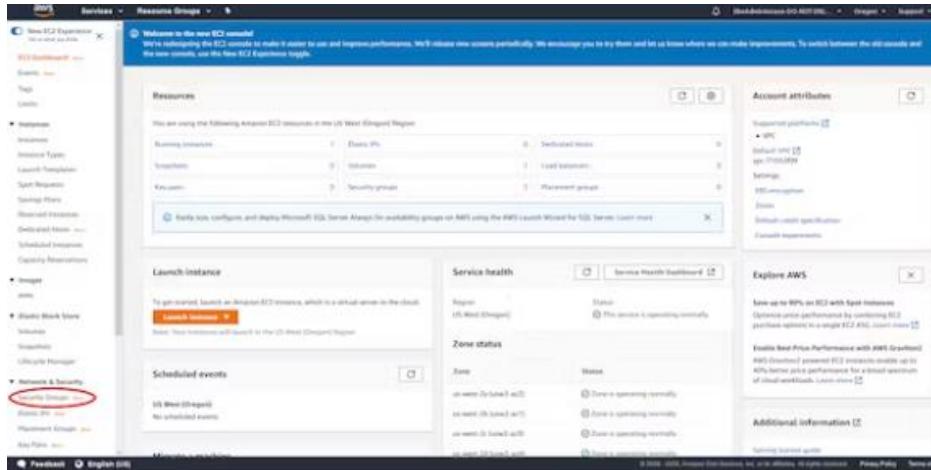
Les solutions physiques demandent notamment:

De la **place**, des **équipes humaines**, de la **sécurité physique**, une **gestion du temps et du capital**.

Des **cycles longs d'approvisionnement en matériel**.

Demande de **prévoir** du matériel en réserve en cas de pic de capacité.

# Modèle du Cloud Computing



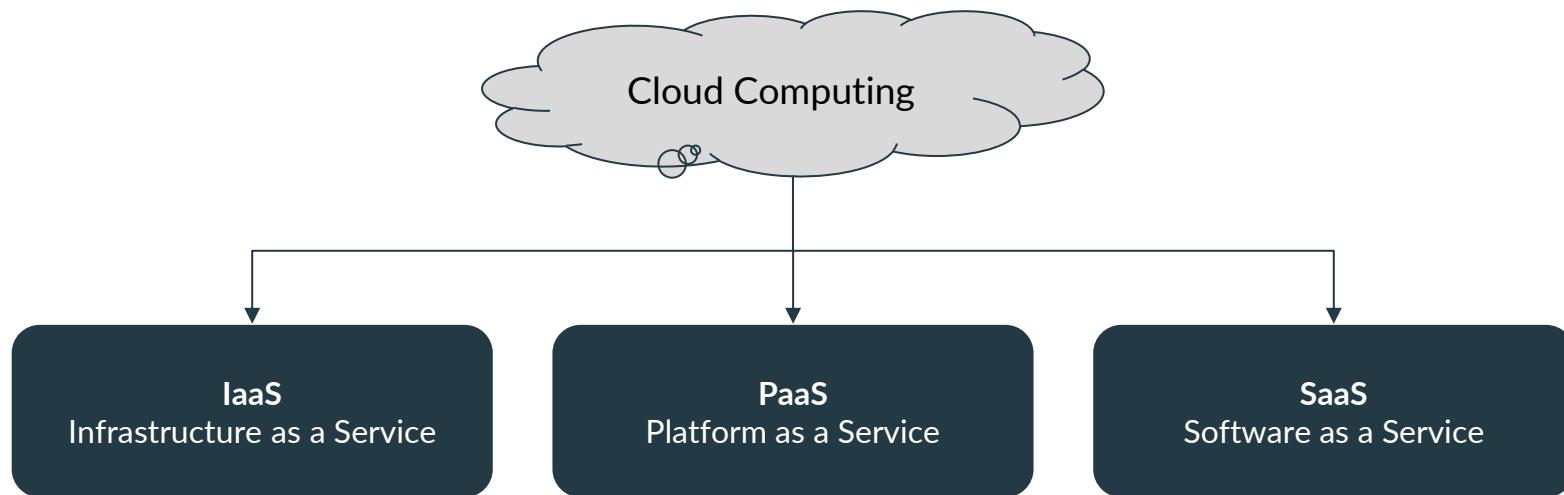
## L'infrastructure comme logiciel

Les solutions logicielles sont **flexibles**, peuvent être **modifiées facilement**, rapidement et sont **plus rentables** que des solutions matérielles.

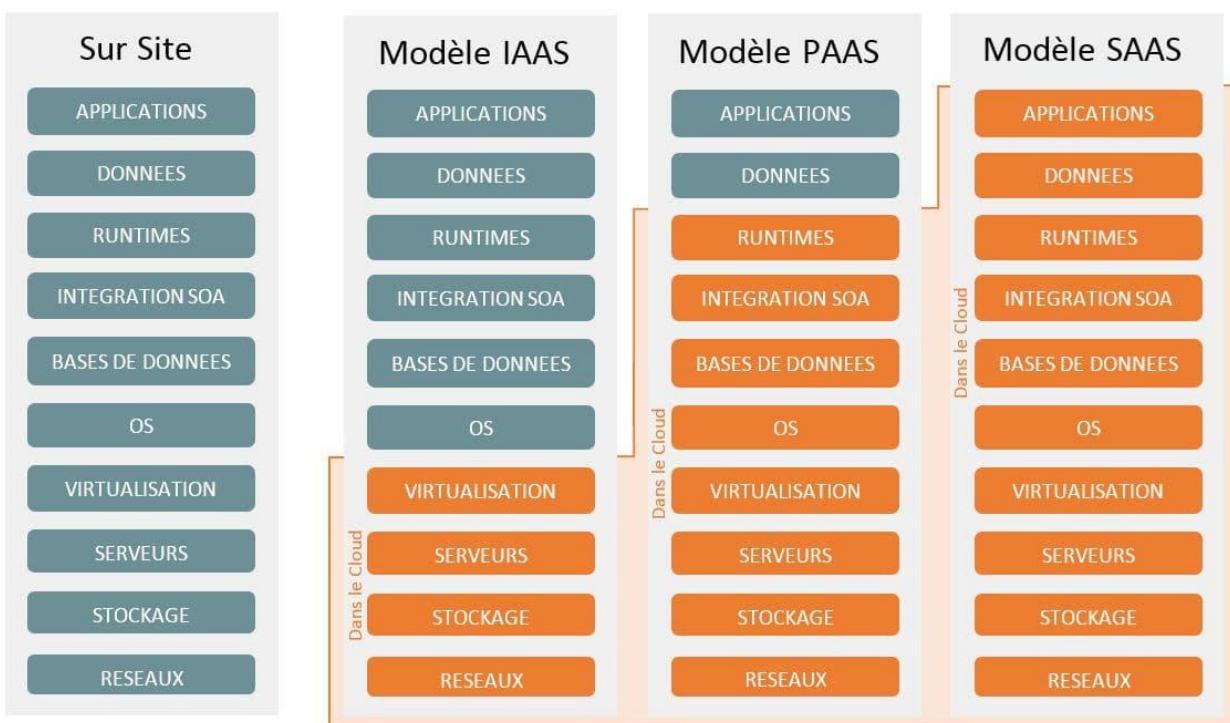
Elles éliminent les solutions lourdes qui ne font pas la différence.

# Les modèles de service dans le CC

Le Cloud Computing se décline en plusieurs modèles de service



# Les modèles de service dans le CC



# Les modèles de service dans le CC

## Sur Site

APPLICATIONS

DONNEES

RUNTIMES

INTEGRATION SOA

BASES DE DONNEES

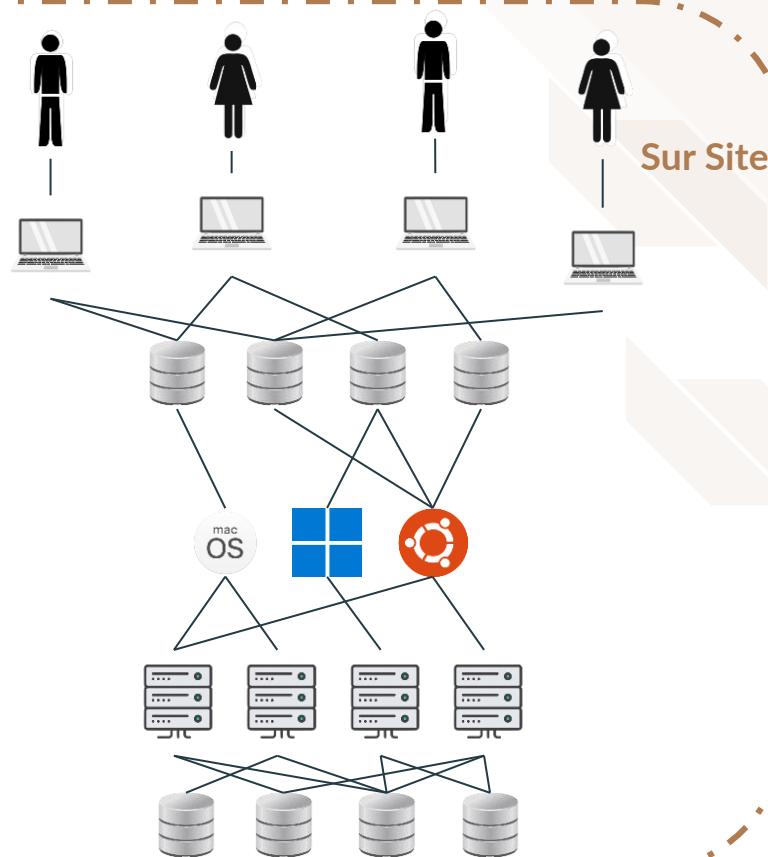
OS

VIRTUALISATION

SERVEURS

STOCKAGE

RESEAUX



On Premise (ou "Sur Site")

Rien dans le Cloud.

Tout est présent  
dans l'entreprise.

# Les modèles de service dans le CC

## Modèle IAAS

APPLICATIONS

DONNEES

RUNTIMES

INTEGRATION SOA

BASES DE DONNEES

OS

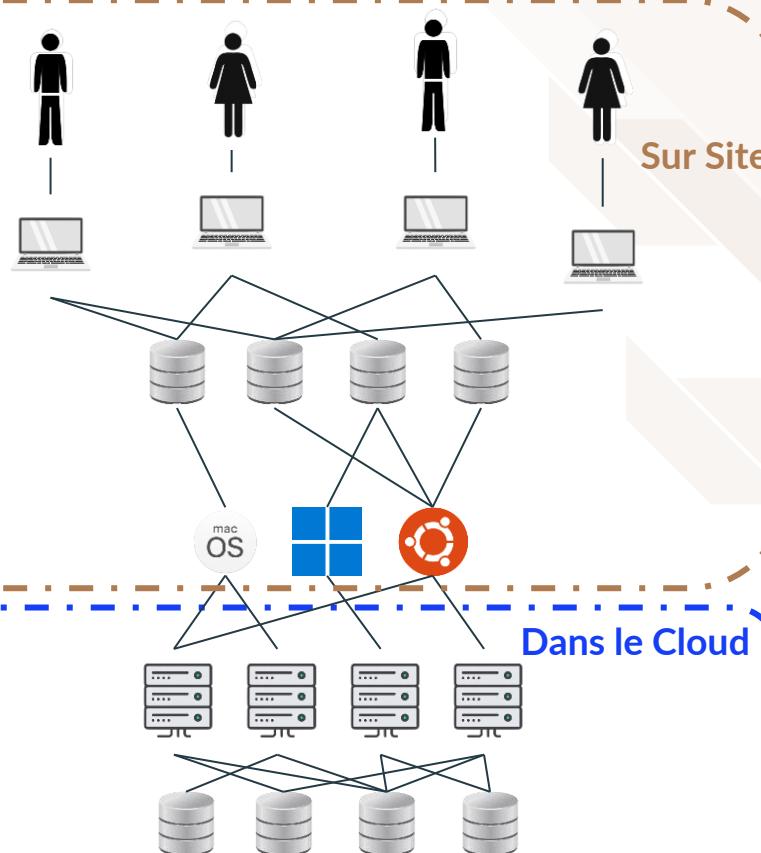
VIRTUALISATION

Dans le Cloud

SERVEURS

STOCKAGE

RESEAUX



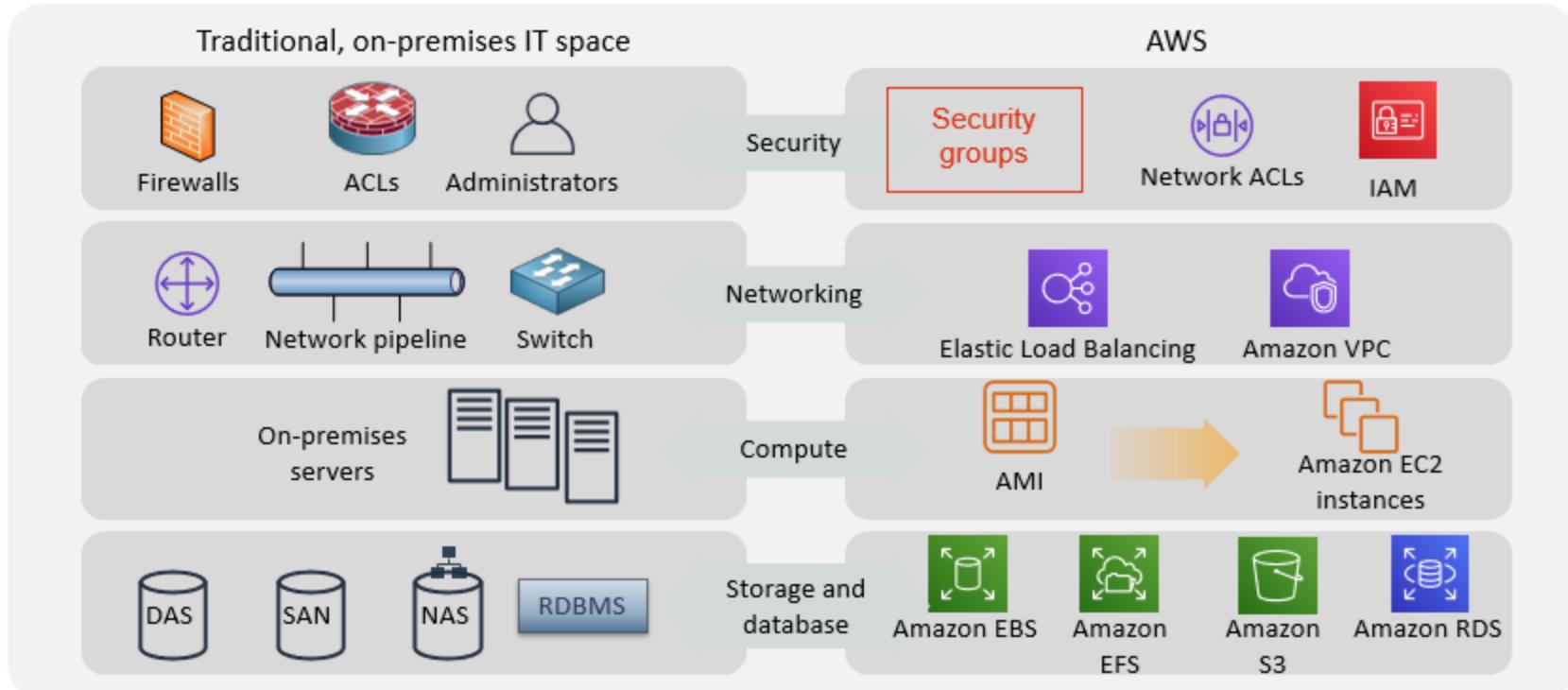
## Infrastructure as a Service

Il s'agit de la fourniture d'infrastructures informatiques virtuelles (machines virtuelles, réseaux, stockage)

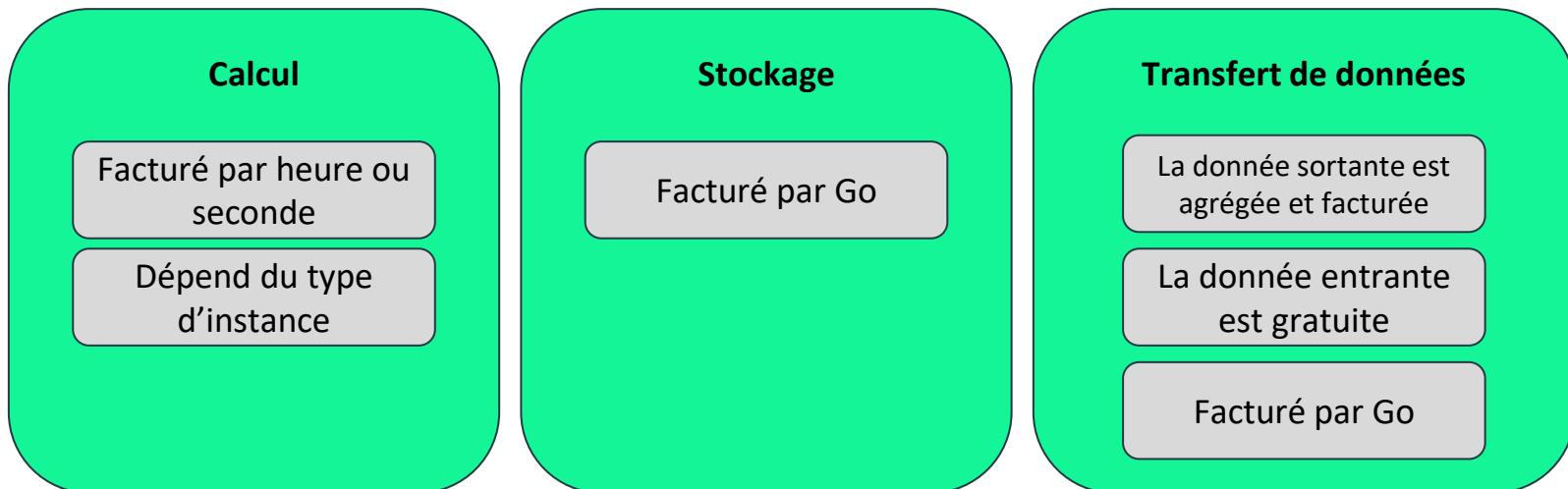
Les utilisateurs peuvent gérer ces ressources de manière flexible.

# Exemple de IaaS





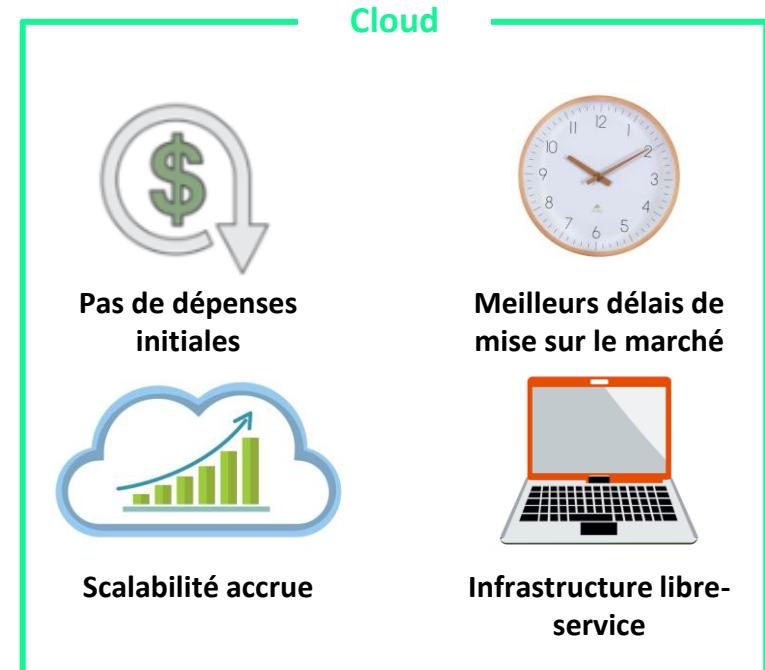
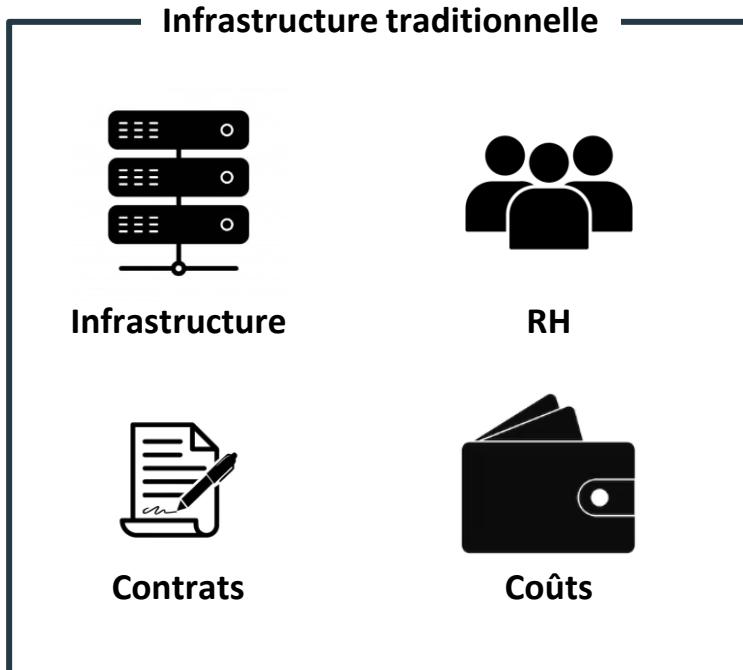
# Les modèles de facturation des Cloud Providers



ÉCOLE  
CENTRALE LYON

inspiré du cours "Cloud Foundations"

# Sur site vs Cloud





Gagner sur le **Coût Global de Possession** (TCO en anglais : Total Cost of Ownership)

# Qu'est ce que le TCO ?

Le TCO est une estimation financière qui permet de déterminer les **coûts directs et indirects** d'une système.

On l'utilise notamment pour comparer le prix d'une infrastructure entièrement sur site face à une infrastructure cloud.

On l'utilise également pour budgéter et construire les cas pratiques dans le cas d'une migration dans le cloud.

## Infrastructure IT

Coûts des serveurs

Hardware : Serveurs, châssis, unités de distribution (PDU) , top-of-rack (TOR) + maintenance

Software : OS, licences de virtualisation + maintenance

Coût des installations

Espace

Energie

Refroidissement

Coûts du stockage

Hardware : Disques de stockage, Zones de stockage (SAN), Commutateur fibre channel

Coûts d'administration du stockage

Coût des installations

Espace

Energie

Refroidissement

Coûts des réseaux

Network Hardware : LAN, Load Balancer avec bande passante

Coûts d'administration des réseaux

Coût des installations

Espace

Energie

Refroidissement

Main d'oeuvre Informatique

“Administre tout ce qu'il y a au dessus ..”

# Exemples de clients IaaS (AWS)



JCDecaux

france.tv



Pernod Ricard

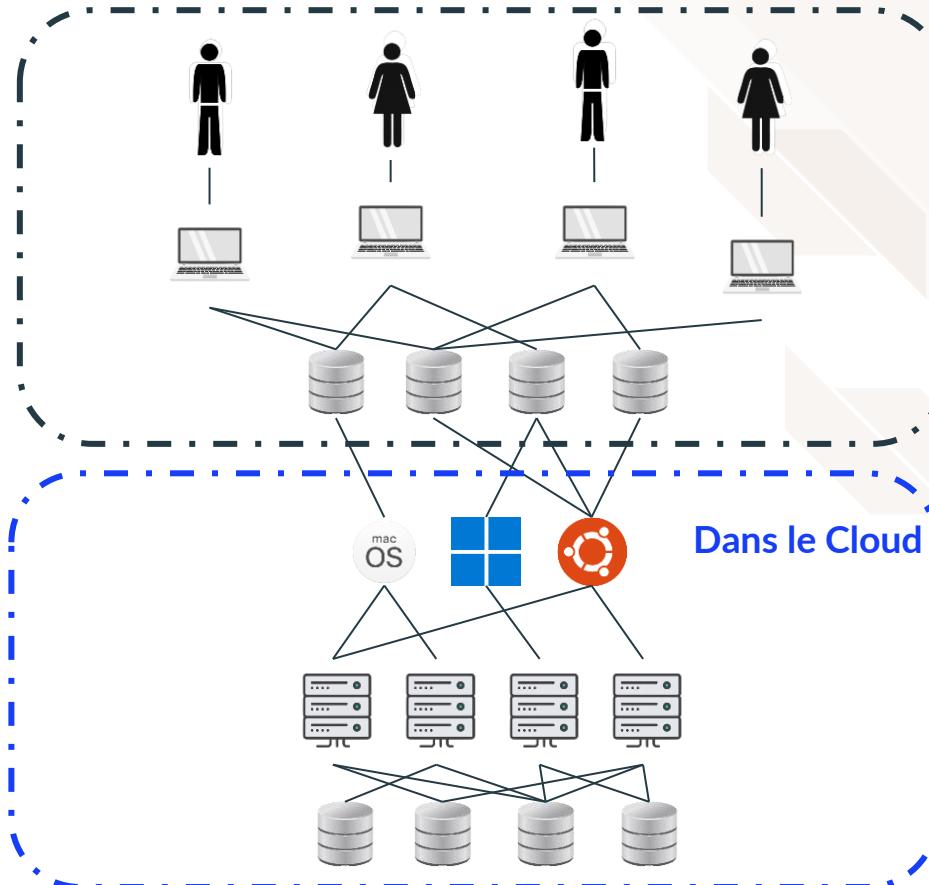
Doctolib

ZADIG & VOLTAIRE

# Les modèles de service dans le CC

## Modèle PaaS

- APPLICATIONS
  - DONNEES
  - RUNTIMES
  - INTEGRATION SOA
  - BASES DE DONNEES
  - OS
  - VIRTUALISATION
  - SERVEURS
  - STOCKAGE
  - RESEAUX
- Dans le Cloud



## Platform as a Service

Le PaaS fournit une plate-forme de développement qui inclut des outils, des bibliothèques et des services pour créer, tester et déployer des applications.

L'objectif est d'éliminer la gestion de l'infrastructure sous-jacente.

# Exemple de PaaS



Google  
App Engine

# Les modèles de service dans le CC

Sur Site ou en Distanciel

Modèle SAAS

APPLICATIONS

DONNEES

RUNTIMES

INTEGRATION SOA

BASES DE DONNEES

OS

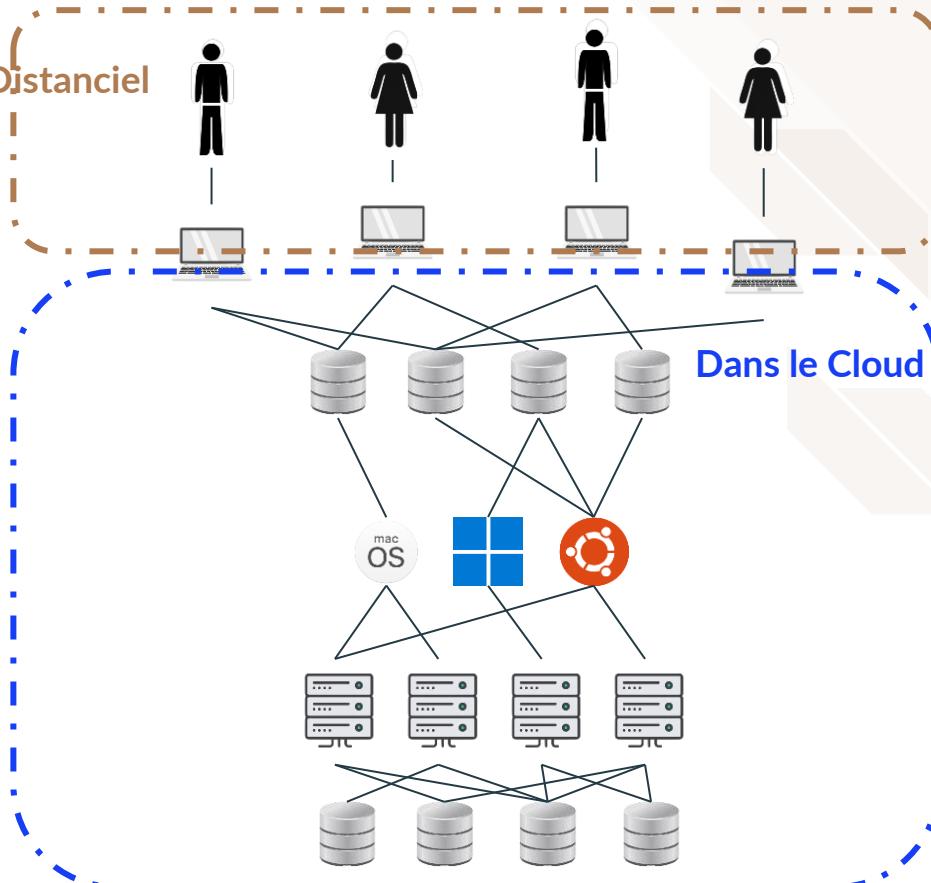
VIRTUALISATION

SERVEURS

STOCKAGE

RESEAUX

Dans le Cloud



## Software as a Service

Le SaaS offre des applications logicielles complètes accessibles via un navigateur web.

Les utilisateurs n'ont pas à se soucier de l'infrastructure ou de la maintenance logicielle.

# Le lecteur MP3



Télécharger de la musique sur Internet

La placer dans votre lecteur

Ecouter de la musique

Impossibilité d'écouter de la musique  
sans l'avoir téléchargée.

# Les solutions SaaS de streaming



Payer un abonnement mensuel pour avoir accès depuis toutes vos plateformes à un catalogue de musique étendu

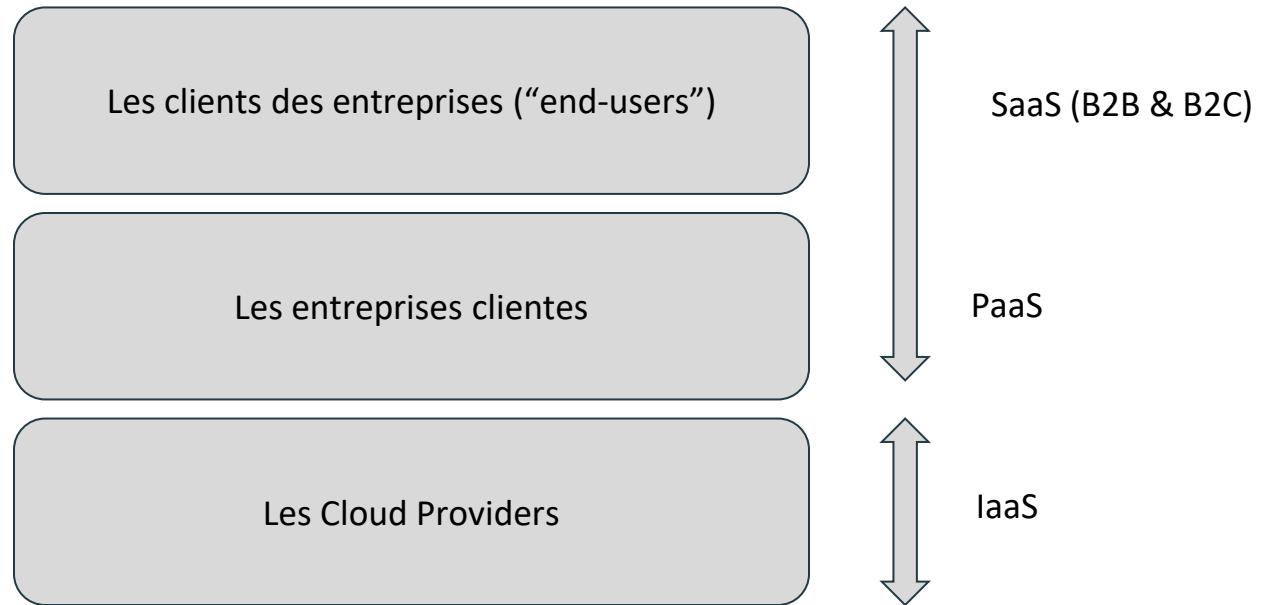
# SaaS

“Service basé sur le Cloud où, au lieu de télécharger un logiciel sur votre PC de bureau où votre réseau professionnel peut exécuter et mettre à jour, vous accédez à une application via un navigateur internet.”

Oracle Cloud



# Présentation des acteurs du Cloud



# Le Cloud Computing : Les Cloud Providers

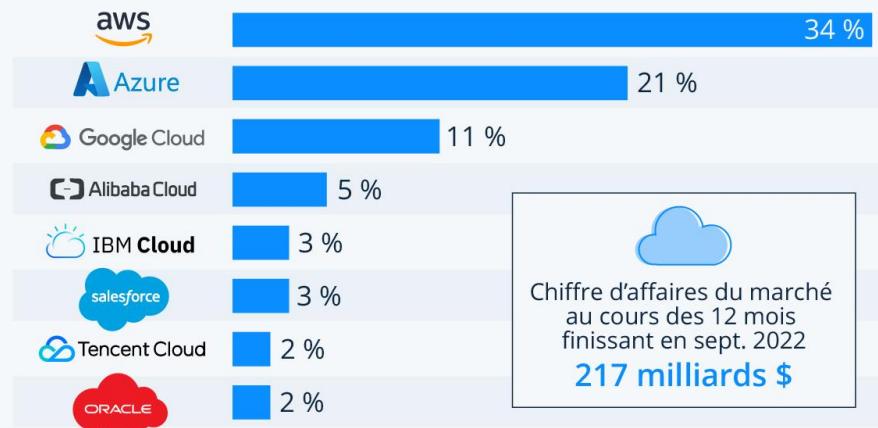
## Top 10 Cloud Providers



# Parts de marché des Cloud Providers

## Cloud : les géants de la tech se partagent le marché mondial

Part de marché mondiale des principaux fournisseurs de services cloud au troisième trimestre 2022 \*



\* inclut les services PaaS (platform as a service), IaaS (infrastructure as a service), ainsi que les services de cloud privé hébergé.

Source : Synergy Research Group



# Stratégie d'accélération Cloud

## STRATÉGIE D'ACCÉLÉRATION CLOUD

• • • •



© Da Kuk / Getty Images

La numérisation de la société s'accompagne d'un recours massif aux technologies du Cloud pour héberger et traiter nos données. La maîtrise de ces technologies est impérative pour garantir notre souveraineté numérique et permettre à la France de prendre part aux innovations à venir.

APP. A PROJETS
PRESSE
FAQ
CONTACT
ETUDES
EVENEMENTS
AUTRES SITES DGE

Dans le cadre du Plan « France Relance » et du Programme d'investissements d'avenir, le Gouvernement lance une stratégie d'accélération « Cloud ».

Dans le cadre du 4ème programme d'investissements d'avenir, le Cloud fait partie des marchés identifiés comme prioritaires, à fort potentiel de croissance et répondant à des enjeux sociétaux majeurs. Une stratégie d'accélération est en cours d'élaboration, sous le pilotage de la direction générale des entreprises et en lien avec toutes les administrations compétentes sur le sujet, afin d'identifier les chantiers prioritaires à mettre en œuvre.



# Sécurité, performance et souveraineté : les enjeux de la stratégie cloud du Gouvernement

06/04/2023

Le recours au cloud (« l'informatique dans les nuages ») est devenu incontournable et concerne tous les secteurs d'activité. En pleine expansion, le marché du stockage des données est dominé par des prestataires étrangers et soumet ses utilisateurs à différentes menaces. Face à ce constat, le Gouvernement développe une stratégie cloud en trois axes pour accroître le niveau de sécurité, la qualité des services et son indépendance technologique.



©BillionPhotos.com / Stock.Adobe.com

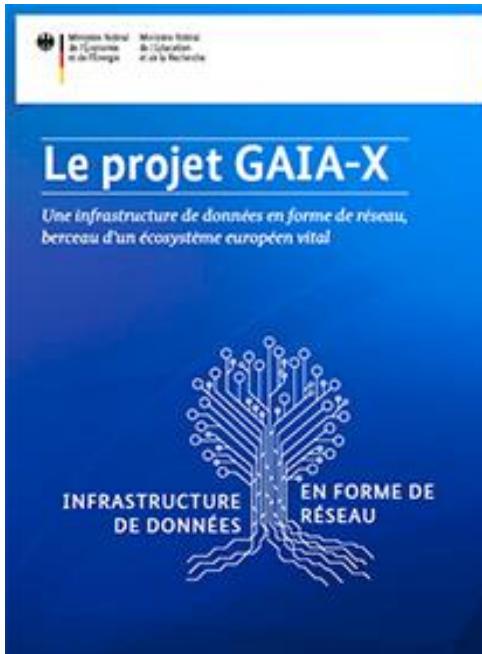
# Souveraineté du Cloud ?

Souveraineté Organisationnelle ou  
Opérationnelle

Souveraineté Logicielle

Souveraineté des Données

# Les projets Européens



[Contact Us](#)   [FAQ](#)   [News](#)   [Publications](#)   [Members](#)   [Background](#)

## EUCLIDIA: the European Cloud Industrial Alliance

Fostering innovation in the European cloud space.

# Le Projet GAIA-X

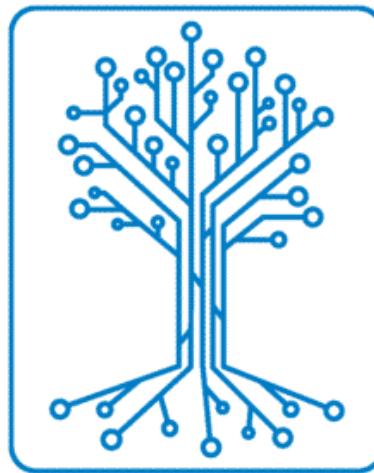
Annoncé le 4 juin 2020

Géré par une association internationale

Organisé sous la forme de “hubs” nationaux

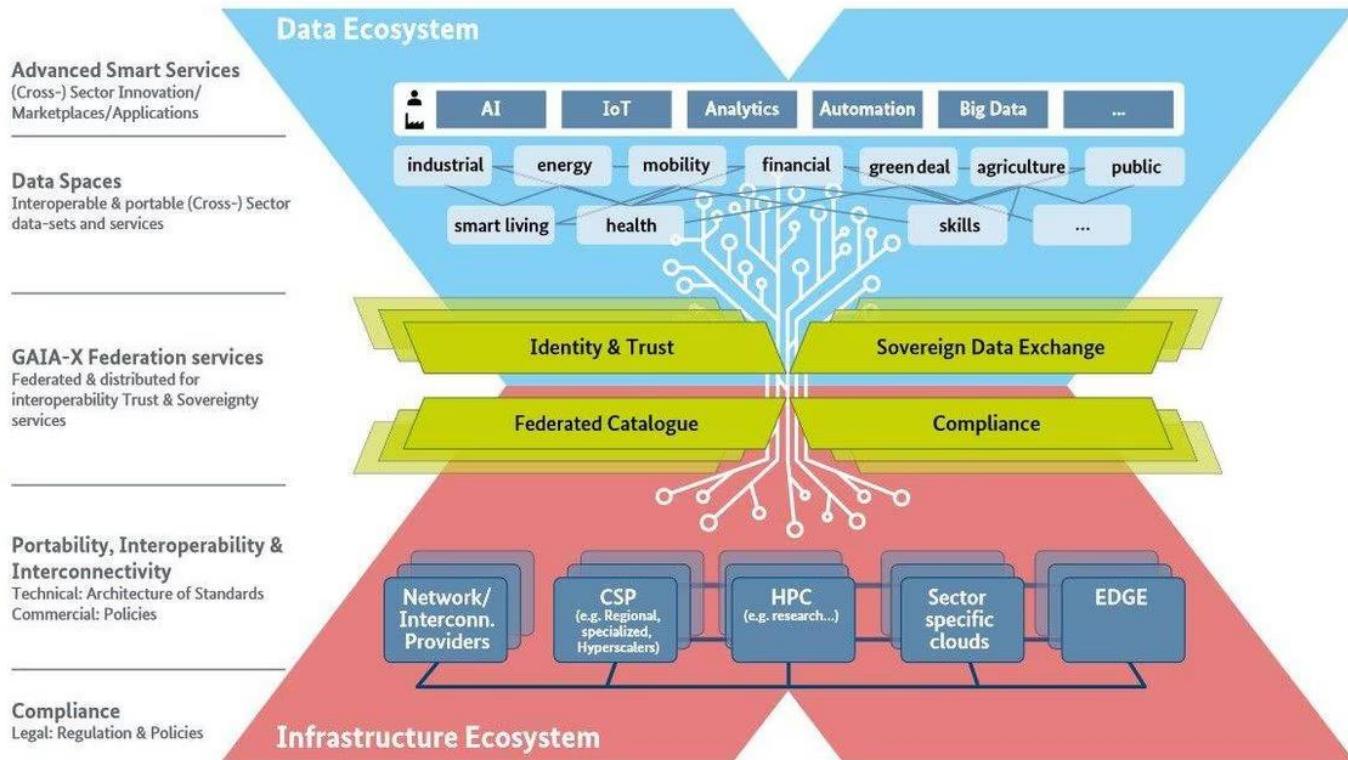
France : Lancé et coordonné par le CIGREF (Club Informatique des Grandes Entreprises Françaises)

Soutenu par le ministère de l'Economie



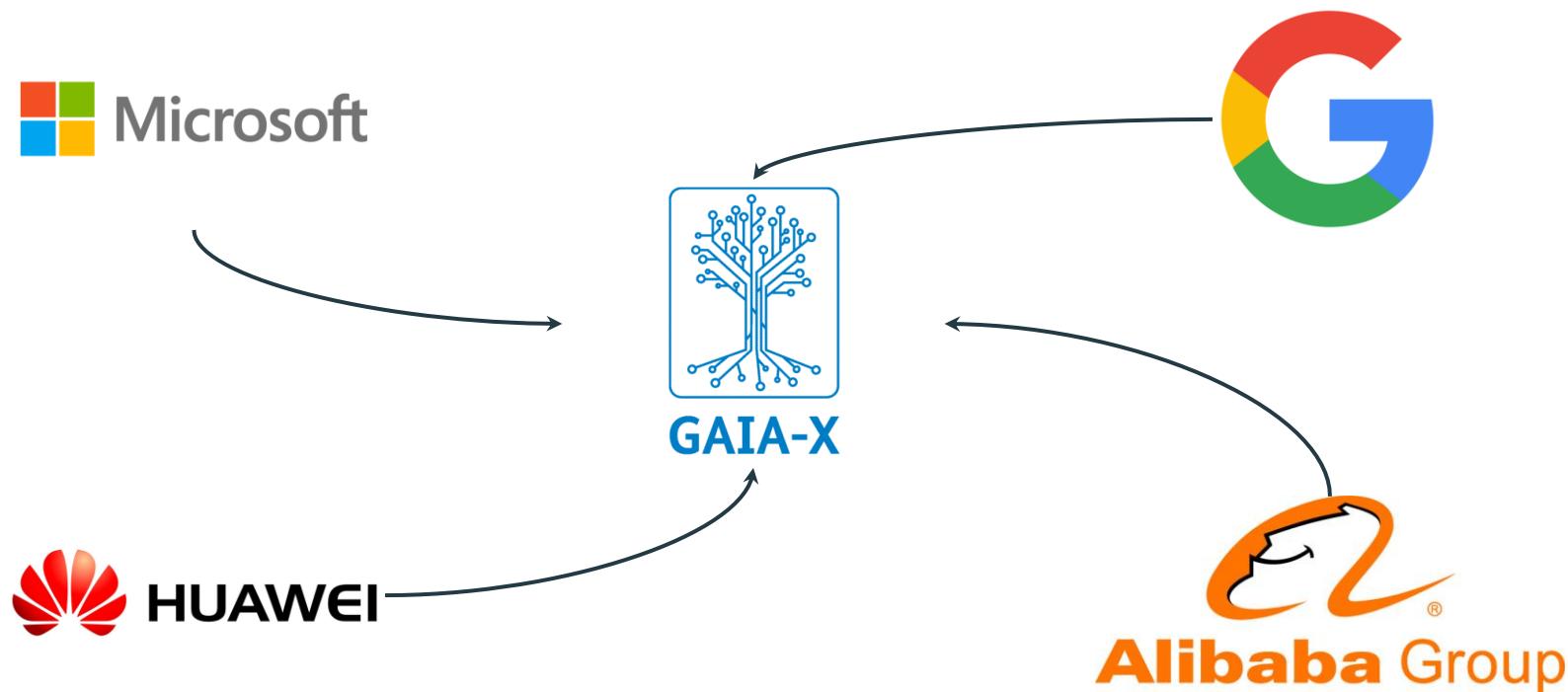
**GAIA-X**

Figure 1: Architectural concept with GAIA-X federated services



Source: BMWi

# Une gouvernance parfois difficile..



# Survivre à tout prix..

Francesco Bonfiglio, PDG de Gaia-X : “Le marché Européen n'a pas d'alternative et doit survivre à un marché concurrentiel (...) Nous essayons donc de construire une initiative qui soit compétitive sur le marché mondial. Et pour cela, nous avons besoin d'acteurs non-européens.”

# Euclidia, la solution anti-Gaia-X ?

Rassemble uniquement des sociétés dont le capital est européen.

<https://www.euclidia.eu/>



Contact Us    FAQ    News    Publications    Members    Background

**EUCLIDIA:**  
**the European Cloud Industrial Alliance**

Fostering innovation in the European cloud space.

# Et la France ?



# Et la France ?



# Les autres projets

Google Cloud

THALES

[https://www.thalesgroup.com/fr/group/investisseurs/press\\_release/thales-et-google-cloud-annoncent-partenariat-strategique](https://www.thalesgroup.com/fr/group/investisseurs/press_release/thales-et-google-cloud-annoncent-partenariat-strategique)

# Les autres projets



AWS European Sovereign Cloud

Nous sommes heureux d'annoncer le lancement de l'AWS European Sovereign Cloud, un nouveau cloud indépendant pour l'Europe, conçu pour aider les organisations du secteur public et les clients des industries régulées à répondre à leurs besoins évolutifs en matière de souveraineté. Nous concevons l'AWS European Sovereign Cloud de manière à ce qu'il soit distinct et indépendant de nos [Régions existantes](#), avec une infrastructure entièrement située dans l'Union européenne.



# Le Data Governance Act

Le **Data Governance Act** et le **Data Act** s'inscrivent dans le cadre de la **stratégie européenne pour les données**, présentée par la Commission européenne en février 2020. Cette stratégie vise à développer un marché unique de la donnée en soutenant **l'accès, le partage et la réutilisation responsables**, dans le respect des valeurs de l'Union européenne et notamment la **protection des données personnelles**.

Elle s'inscrit dans le contexte plus large du plan d'action de la Commission européenne visant à assurer la **souveraineté numérique** de l'Europe à l'horizon **2030**, et est complémentaire de la stratégie européenne en matière d'intelligence artificielle.

# Le Data Governance Act

Première brique de la série de mesures annoncées dans le cadre de la stratégie européenne des données, le Data Governance Act a été adopté en **mai 2022**, et sera applicable en **septembre 2023**. Il vise à favoriser le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation. Ce règlement comporte 4 grandes mesures.

# Le Data Governance Act

Un encadrement ainsi qu'une assistance technique et juridique facilitant la **réutilisation** de certaines catégories de données protégées du secteur public (informations commerciales confidentielles, propriété intellectuelle, données personnelles)

Une certification **obligatoire** pour les fournisseurs de services d'intermédiation de données.

Une certification **facultative** pour les organismes pratiquant l'altruisme en matière de données.

La création du  
**“Conseil Européen de l’innovation en matière de données”**

# Le Data Act (Le règlement sur les données)

La proposition législative de la Commission européenne, présentée le **23 février 2022**, a pour objectif d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs de l'économie de la donnée, notamment liées à l'utilisation des objets connectés et au développement de l'Internet des objets.

# Le Data Act

Faciliter le partage entre entreprises (B2B) et avec le consommateur (B2C) des données, en fixant notamment une obligation de rendre accessibles les données générées par l'utilisation des objets connectés et services connexes, en contrepartie d'une compensation juste et équitable.

Permettre l'utilisation des données détenues par les entreprises et, sous réserve de justifier d'un besoin exceptionnel, par les organismes publics des États membres et les institutions, agences ou organes de l'Union.

Faciliter le changement de fournisseur de services de traitement de données (cloud et edge computing) par l'encadrement des relations contractuelles entre les fournisseurs de services et les consommateurs, et notamment par la suppression progressive des frais liés au changement pour le consommateur.

Prévoir l'élaboration de normes d'interopérabilité pour les données et leurs réutilisations entre les secteurs.

Mettre en place des garanties contre les accès illicites de gouvernements de pays tiers aux données non-personnelles contenues dans le cloud.

# Amendes des GAFAM

Les plus grosses amendes reçues pour non respect des réglementations :

Meta : 2023 - Par l'autorité de contrôle irlandaise : 2,5 milliards d'euros pour un transfert de données de l'UE vers les USA

Janvier 2023 : Meta - 390 millions d'euros - utilisation de données personnelles dans le cadre de contacts publicitaires.

Amazon : 2021 746 millions d'euros.

Google : 2021 - 90 millions d'euros et 60 millions d'euros.

# Références

<https://afee-cedece.eu/gaia-x-un-projet-europeen-trop-ambitieux/> Lamprini Xenou, Maître de conférences en droit public, Université Paris-Est Créteil

<https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2021/euclidia-un-cloud-europeen-rival-de-gaia-x/> “Euclidia, un cloud européen rival de Gaia-X ?” Nathan Crouzevialle



# Introduction à la Blockchain



# Historique

Revenons au début...





Historique

2008

# Historique

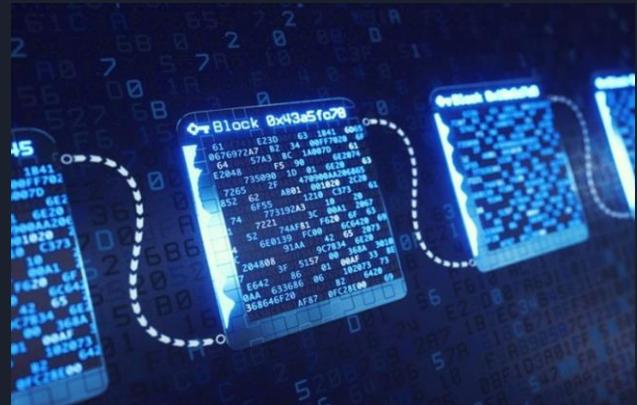
En 2008, alors que la crise des Subprimes aux Etats-Unis fait rage, un nouveau système s'apprête à apparaître..



# Introduction à la Blockchain

18 août 2008

Le 18 août 2008, le nom de domaine “bitcoin.org” fut réservé.

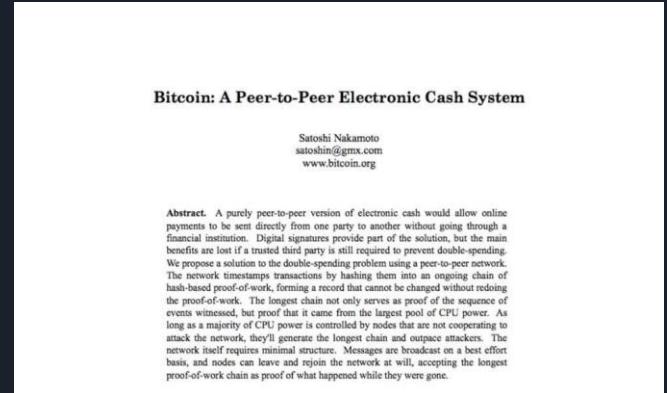


# Introduction à la Blockchain

Automne 2008

Le 31 octobre 2008, le Bitcoin et son concept de Blockchain sort de l'ombre via le ( ou ses ) créateur(s) Satoshi Nakamoto.

Le “White Paper” édité devient alors le document de référence expliquant le protocole Bitcoin.



*Le “white paper” de Bitcoin*  
<https://bitcoin.org/bitcoin.pdf>

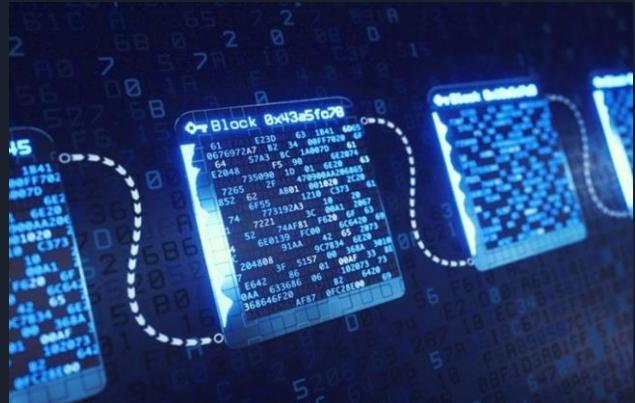
# Introduction à la Blockchain

Automne 2008

Le 9 novembre 2008, le terme de “blockchain” apparaît pour la première fois.

Le concept repose sur une base de données distribuée dont les informations sont envoyées par les utilisateurs.

Les liens internes de la base sont vérifiés et groupés sous forme de blocs formant ainsi une chaîne.



# Introduction à la Blockchain



3 Janvier 2009

Le 3 janvier 2009, les premiers Bitcoins naissent, le premier bloc de la blockchain naît.

Le premier échange a lieu le 12 janvier 2009 entre Satoshi Nakamoto et Hal Finney, un cryptographe qui aidera ce dernier à créer le protocole Bitcoin.



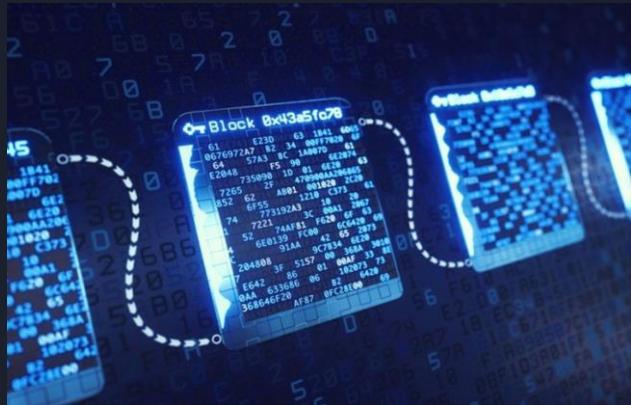
*Hal Finney*

# Introduction à la Blockchain

5 octobre 2009

Le 5 octobre 2009, le Bitcoin est estimé à 0,001 dollar.

Ce montant est déterminé par le coût de production en électricité que nécessite la création d'une unité par un ordinateur.



# Introduction à la Blockchain

12 décembre  
2010

Le 12 décembre 2010, Satoshi Nakamoto disparaît.

Il déclare passer le relais au développeur américain Gavin Andresen en lui confiant la clé d'alerte du protocole.

Cette dernière permet d'adresser instantanément un message à tous les ordinateurs qui constituent les nœuds du système.



# Introduction à la Blockchain

Février 2011

En Février 2011, le Bitcoin égale le dollar puis quelques jours plus tard, l'euro.



# Introduction à la Blockchain

Juin 2011

En Juin 2011, l'ONG WikiLeaks annonce accepter les paiements en Bitcoin afin de contourner les interdictions mises en place par Visa, Mastercard et PayPal de virement à destinations de cette dernière.



# Introduction à la Blockchain

Février 2014

En Février 2014, la plateforme MtGox, la première plateforme d'échange et d'achat/vente de Bitcoins fait faillite.

Mark Karpeles, considéré comme “le baron du Bitcoin” et créateur de MtGox est attaqué de toutes parts dans les tribunaux du monde entier.



# Introduction à la Blockchain

Juillet 2015

En Juillet 2015, Vitalik Buterin crée le protocole ETHEREUM

Ce dernier supporte les “smarts contracts”, des programmes informatiques irrévocables qui exécutent un ensemble d’instructions prédéfinies.



# Introduction à la Blockchain

Décembre 2017

En Décembre 2017, des contrats à terme sur Bitcoin sont lancés, de nouveaux produits financiers arrivent et font monter le cours du Bitcoin à 20.000 \$



# Introduction à la Blockchain

2018 - 2019

Entre 2018 et 2019, de nouvelles entreprises et institutionnels entrent sur le marché.

MicroStrategy, BlackRock..

Le Bitcoin repasse sous la barre des 6000 \$ suite à leur arrivée.



# Introduction à la Blockchain

Novembre 2020

En novembre 2020, Paypal ouvre un service d'achat et de vente de Bitcoin aux Etats-Unis.



# Introduction à la Blockchain

7 septembre 2021

En septembre 2021, le Salvador donne un cours légal au Bitcoin, il devient une monnaie légale au même titre que le dollar et donc un moyen de paiement.



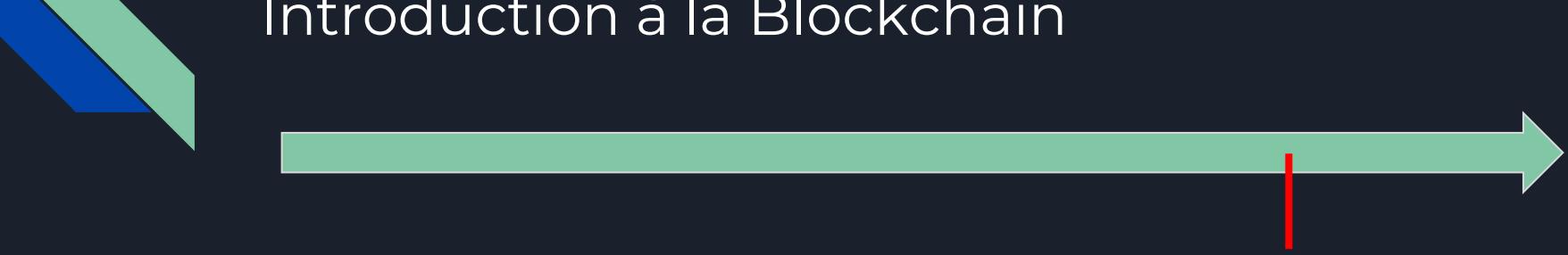
# Introduction à la Blockchain

Juillet 2022

En juillet 2022, le plus casse du siècle fait perdre 560 millions d'Euros à Axie Infinity sur la blockchain Ronin.



# Introduction à la Blockchain



Novembre 2022

Novembre 2022, FTX fait faillite avec à son bord Sam Bankman Fried, le plus jeune milliardaire au monde.

Pertes estimées : 10,5 milliards de dollars.



# Introduction à la Blockchain

Toutes ces infos sont la partie immergée de l'iceberg.

Aujourd'hui des centaines d'entreprises utilisent la technologie de la blockchain pour leur usage professionnel à différentes fins.

Traçabilité, sauvegarde, contrats...





Finally, what is a blockchain ?

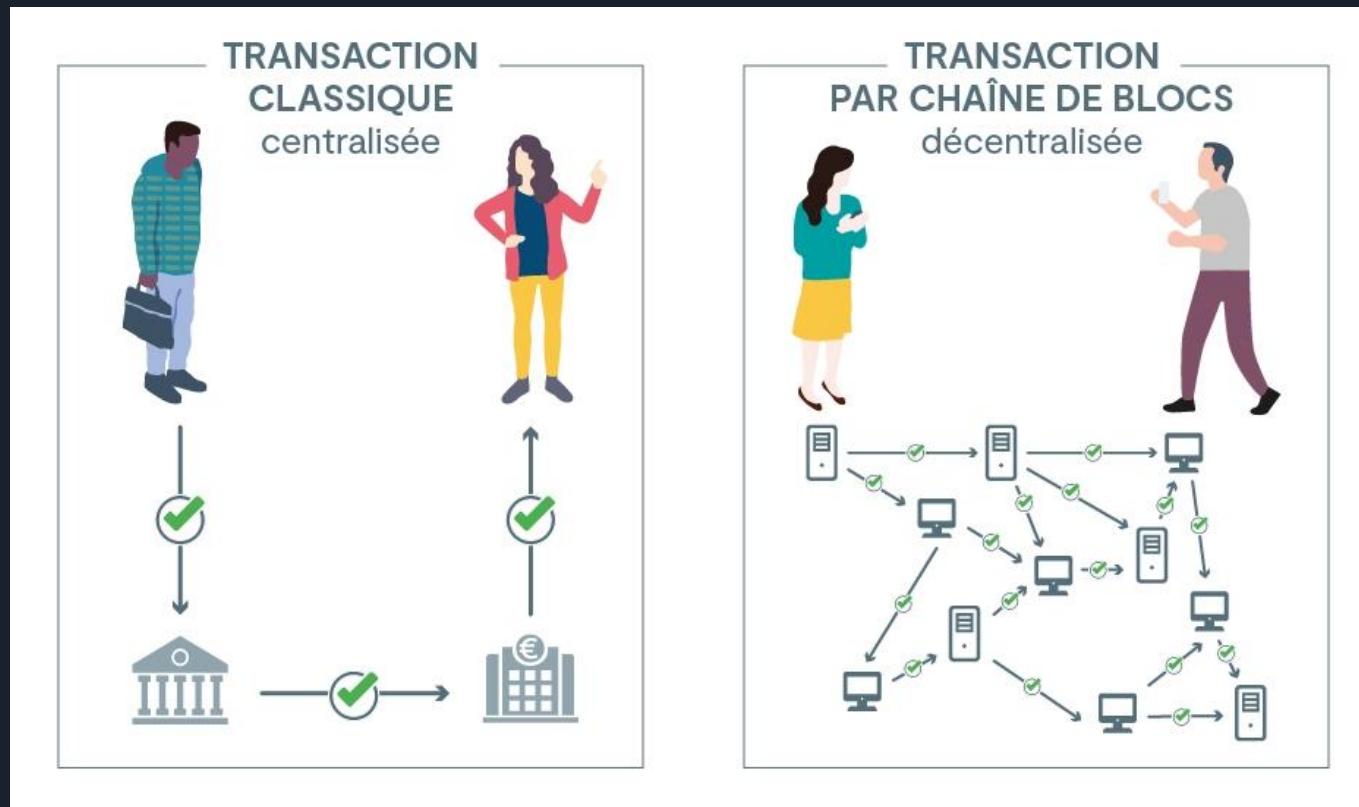


# Définition

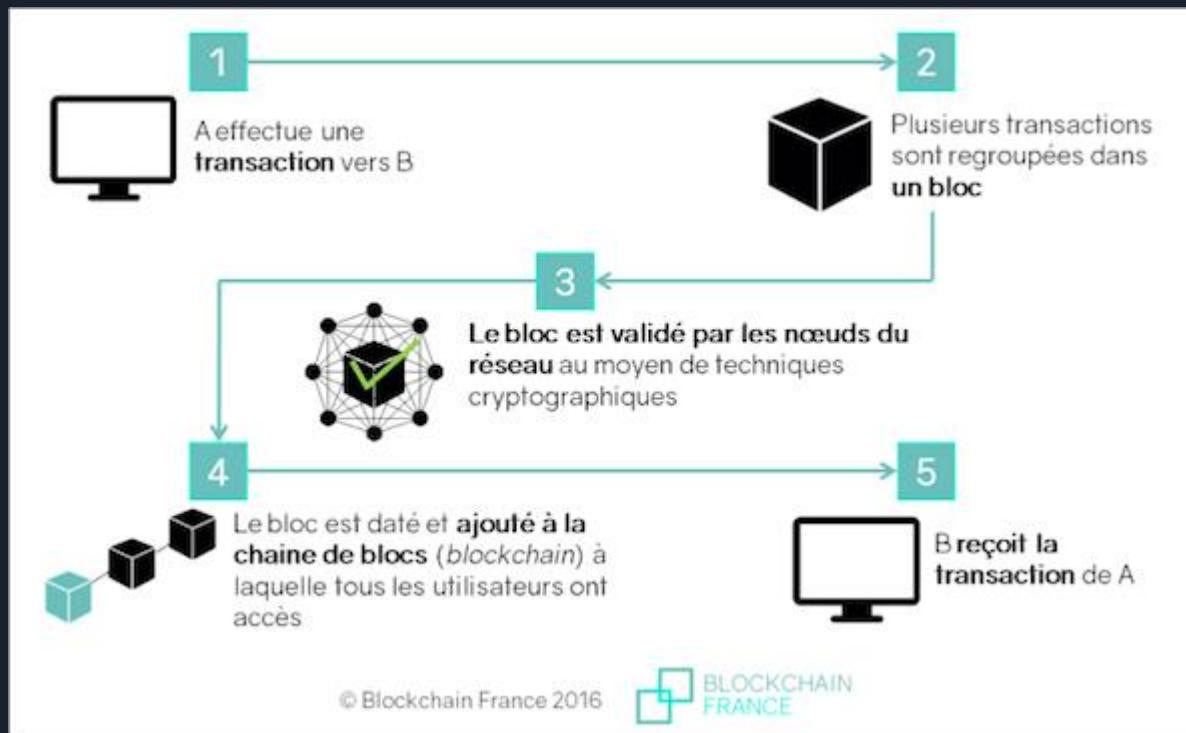
“Une chaîne de blocs (ou blockchain) est une technologie de stockage et de transmission d’informations prenant la forme d’une base de données. Elle fonctionne sans organe central de contrôle. Elle est partagée simultanément avec tous ses utilisateurs.”

*economie.gouv.fr*

# Définition



# Définition

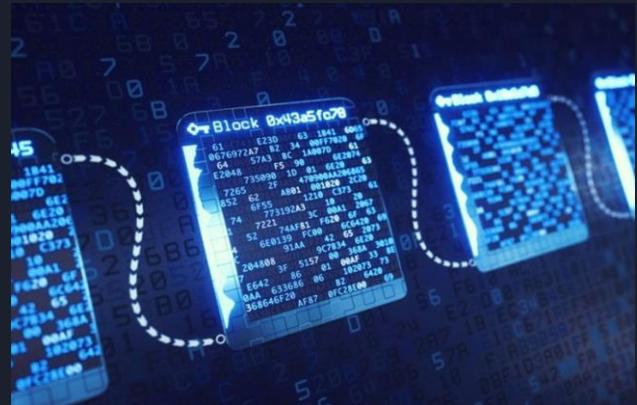


# Introduction à la Blockchain

On écrit une information numérique (une transaction, un contrat etc...) à l'intérieur d'un bloc.

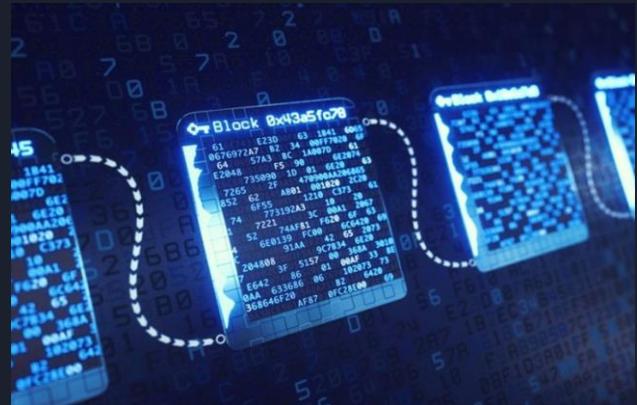
Référentiel : Protocole Bitcoin

Lorsque le bloc est "plein" (Taille variable selon les technologies, ici 1,6 Mo depuis la mise à jour TapRoot), il doit être validé par le réseau pour devenir "officiel".



# Introduction à la Blockchain

C'est ainsi que le principe de Blockchain est né, une suite de blocs validés par les utilisateurs et distribués sur toute machine souhaitant interagir avec la blockchain.



# Pour aller plus loin..



Chaîne Youtube Heu?Reka

Gilles Mitteau

[https://www.youtube.com/watch?v=h4XZpkrlb  
S](https://www.youtube.com/watch?v=h4XZpkrlbS)



Arté

<https://www.youtube.com/watch?v=OETcLj5jBy4>



# Introduction à la Blockchain

Qui peut utiliser la Blockchain ?

Ça dépend du type de blockchain !

Dans le cas de Bitcoin, Ethereum, Avalanche .. Tout le monde : Ce sont des Blockchains PUBLIQUES (cours 2)



# Introduction à la Blockchain

Qui peut utiliser la Blockchain ?

Dans le cas des entreprises, certaines ont déjà sauté le pas et utilisent soit des blockchains publiques, soit privées.



Pourquoi tout le monde n'utilise pas la même  
Blockchain comme Bitcoin par exemple ?



# Introduction à la Blockchain

“À titre d'exemple, le réseau Bitcoin traite très peu de transactions par seconde, contre plusieurs milliers pour un opérateur de carte bancaire. Jusqu'à présent, les mécanismes de la blockchain sont source de lenteur et ne sont pas prêts à une diffusion à large échelle. Il reste encore à trouver des solutions techniques pour trouver des mécanismes de validation moins lourds, mais par conséquent moins fiables.”

Source : Ecole Polytechnique Executive Education



# Les entreprises qui utilisent la blockchain

Il existe différents types d'entreprises qui utilisent la technologie blockchain :

Pour la traçabilité : LVMH, Walmart, Ford

Pour l'investissement : Meria, Coinbase, Binance

Les applications sont nombreuses :

Transport, Santé, Vote en ligne, Immobilier, Assurance, Divertissement...



26

**Alphabet****Honeywell****ORACLE****SAMSUNG****amazon****moderna****CATL****Coca-Cola****Nestle****RBC****abbvie****HYPERLEDGER FABRIC****ethereum**

18

**BANK OF AMERICA****Lowe's****SAMSUNG****Alphabet****amazon****Coca-Cola****ABBV****RBC****abbvie****Hyperledger Fabric****Quorum**

11

**accenture****J.P.Morgan****Goldman Sachs****UnitedHealth Group****Reliance****ingeguru****ABBV****RBC****abbvie**

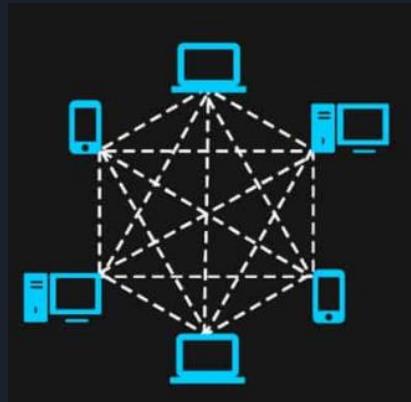
8

**accenture****TCS****BANK OF AMERICA****TOYOTA****Citi****Axon**

# Les blockchains publiques

Les blockchains publiques sont les premières à avoir été créées. (Notamment le protocole Bitcoin).

Ce sont celles qui ont permis de populariser la Technologie du Ledger Distribué (DLT)

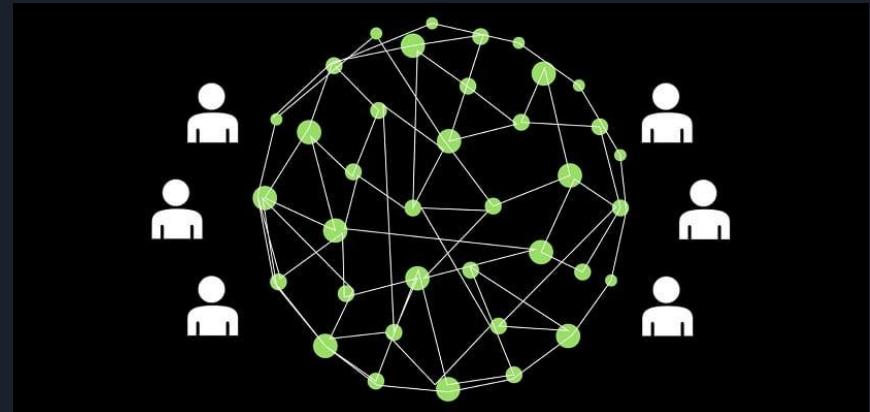


# Les blockchains publiques

Définition : DLT :

Distributed Ledger Technology

Système numérique d'enregistrement des transactions de biens dans lequel les transactions et leurs détails sont enregistrés à plusieurs endroits en même temps.





# Les blockchains publiques

Sa nature décentralisée exige une méthode pour vérifier l'authenticité des données.

On le fait notamment par un algorithme de consensus par lequel les participants de la Blockchain se mettent d'accord sur l'état actuel du Ledger.

# Les blockchains publiques

Il existe 2 méthodes de consensus courantes :

Le Proof of Work (Preuve de travail) (Bitcoin)

Le Proof of Stake ( Preuve d'enjeu) (Ethereum 2.0)



# Le Proof-Of-Work (PoW)

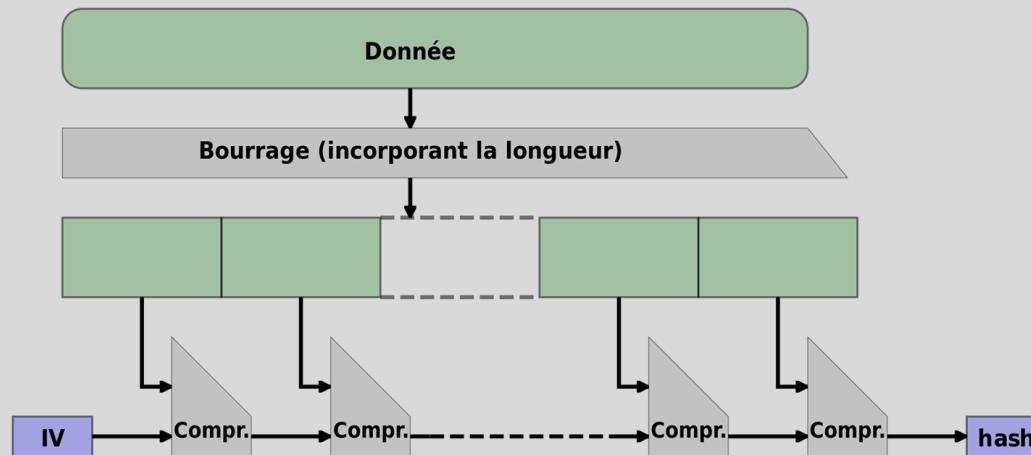
Le “Proof of Work” ou “preuve de travail” est le premier protocole consensus blockchain.

Il est d'abord utilisé pour contrer les spams sur les boîtes mails en utilisant l'algorithme SHA256.



# SHA 256

SHA : Secure Hash Algorithm : Ce sont des fonctions de hachage sur des mots de 32 bits pour la famille SHA 2.



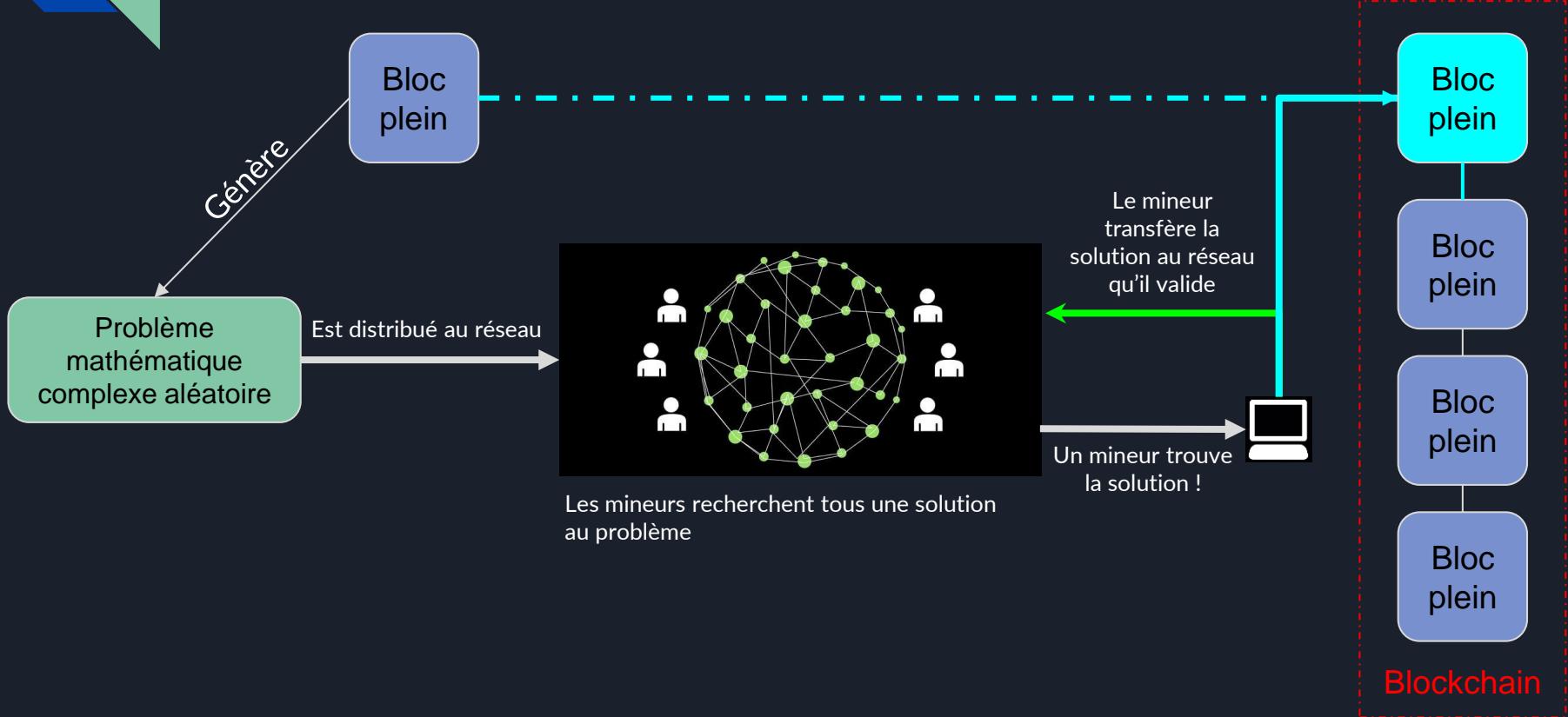


# Le Proof-Of-Work (PoW)

Le proof of Work consiste à résoudre un problème mathématique complexe en utilisant de la puissance de calcul.

Le premier ordinateur ou “mineur” à résoudre ce problème sera celui qui inscrit le prochain bloc sur la blockchain.

# Le Proof-Of-Work (PoW)





# Le Proof-Of-Work (PoW)

Une blockchain qui utilise le Proof Of Work fait appel à des “mineurs”.

Les mineurs sont des ordinateurs utilisant de la puissance de calcul pour vérifier les données entrant sur le registre pour valider l'authenticité des transactions et créer des nouveaux blocs.

Pour récompenser les mineurs qui dépensent de l'électricité et de la puissance de calcul, le protocole “offre” le token de la blockchain au mineur qui trouve la solution du problème.

L'objectif du Proof of Work pour le protocole Bitcoin est un mécanisme permettant d'éviter de dépenser 2 fois le contenu de son portefeuille.



# Le Proof-Of-Stake (PoS)

Le Proof of Stake ou “preuve d’enjeu” est une méthode par laquelle une blockchain vise à atteindre un consensus distribué.

Alors que le Proof-of-Work demande à l’utilisateur de résoudre des problèmes mathématiques, le Proof-of-Stake demande à l’utilisateur de prouver la possession d’une certaine quantité de crypto-monnaies correspondante à celle utilisée sur la blockchain.

Les utilisateurs sont rémunérés grâce aux frais de transaction (“transaction fee”) lors d’un échange ou d’une transaction sur la blockchain.

# PoW vs PoS

**Proof of Work      vs      Proof of Stake**

The infographic compares Proof of Work (PoW) and Proof of Stake (PoS) through six panels:

- Top Left (PoW):** A person mining with a pickaxe. Text: "proof of work is a requirement to define an expensive computer calculation, also called mining".
- Top Right (PoS):** A person standing next to a safe. Text: "Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake".
- Middle Left (PoW):** A person mining on a computer, with a lightbulb icon above their head. A pink bar chart shows 51% completion. Text: "A reward is given to the first miner who solves each blocks problem".
- Middle Right (PoS):** A person mining on a computer, with a diamond icon above their head. A pink bar chart shows 51% completion. Text: "The PoS system there is no block reward, so, the miners take the transaction fees".
- Bottom Left (PoW):** Three people mining together. Text: "Network miners compete to be the first to find a solution for the mathematical problem".
- Bottom Right (PoS):** A person standing next to a large pink money bag. Text: "Proof of Stake currencies can be several thousand times more cost effective".

## Bonus : Le “Proof-of-History” de Solana

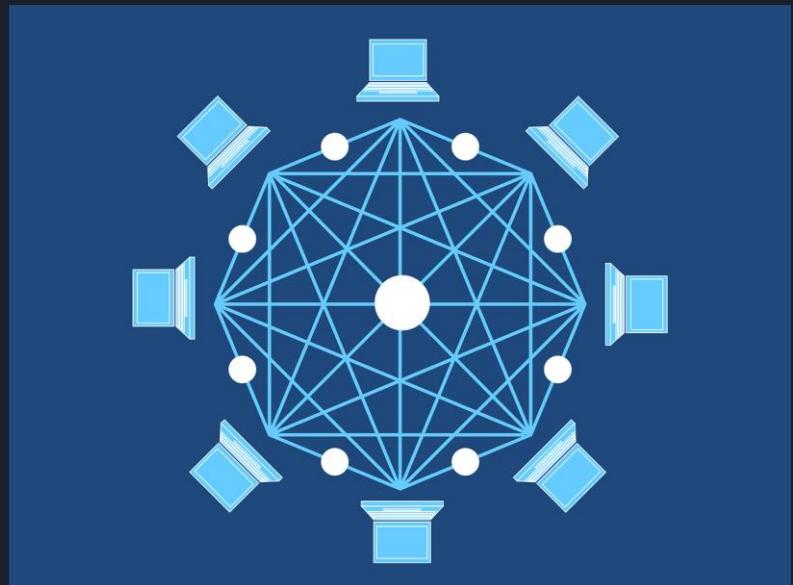


SOLANA

# Les blockchains publiques

Les blockchains publiques sont non restrictives et sans autorisation.

Toute personne disposant d'un accès à internet peut se connecter à une plateforme Blockchain pour devenir un nœud autorisé.



# Les blockchains publiques

Tout utilisateur se connectant à la blockchain peut avoir accès à l'entièreté des transactions, enregistrements passés et actuels des activités se passant sur la blockchain.

Aucun enregistrement ou transaction valide ne peut être modifié sur le réseau et n'importe qui peut vérifier les transactions, trouver des bugs ou proposer des modifications car le code source est généralement open source.



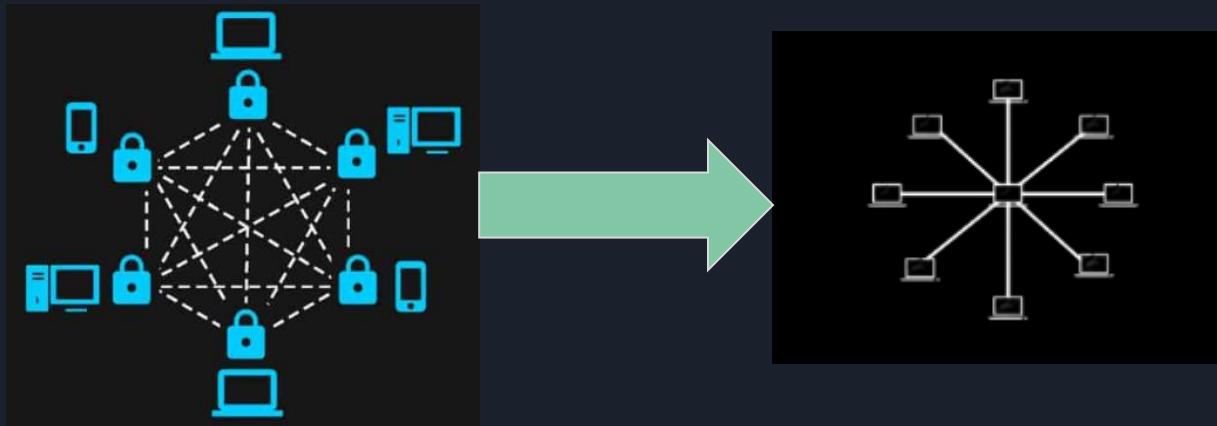
*<https://bitcoin.org/fr/telecharger>*

# Les blockchains privées

Les blockchains privées fonctionnent dans un environnement réseau et SI restrictif.

Le fonctionnement reste le même mais n'est exploité que sur de petites parties du réseau.

Elles sont également appelées “blockchains à autorisation” ou “blockchains d’entreprise”.





# Les blockchains privées : avantages

L'organisation qui les contrôle définit de nombreux paramètres comme par exemple :

Les niveaux de permission

Qui peut interagir (en lecture, en écriture..) avec la blockchain ?

Les autorisations et l'accessibilité

Qui peut voir les nœuds du réseau ?  
Quels nœuds peut-on montrer ?

La sécurité de manière globale

Empêcher des tiers d'accéder à certaines informations



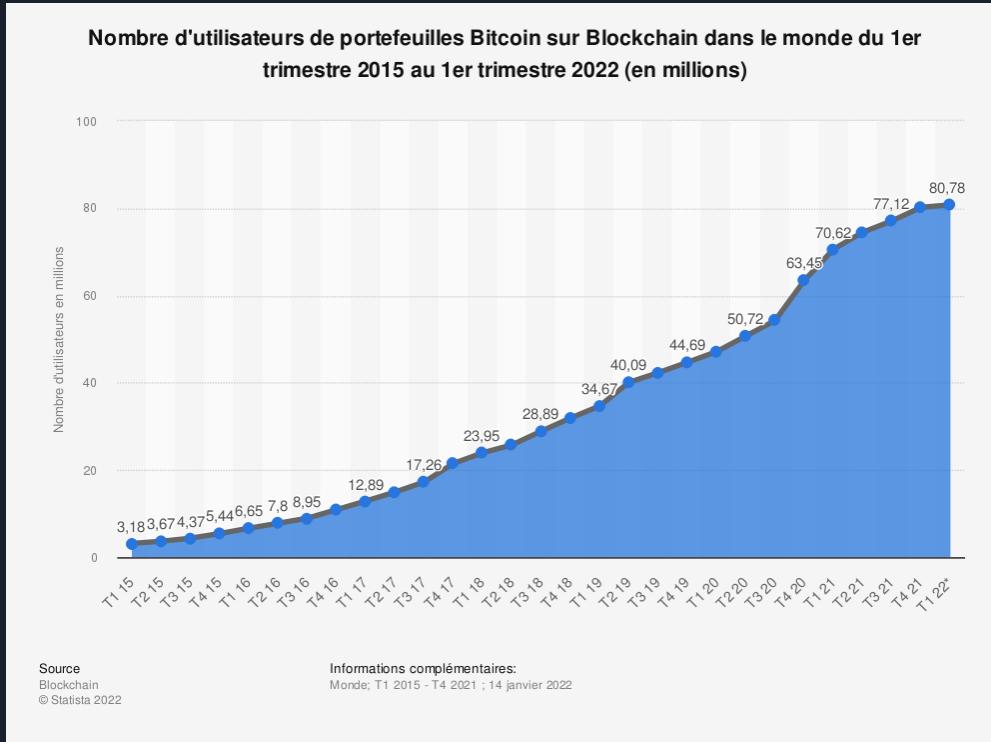
# Les blockchains privées : avantages

Parce qu'elles sont limitées en taille, les blockchains privées peuvent être très rapides et traiter des transactions beaucoup plus rapidement que les blockchains publiques.

Comme le nombre de clients est restreint, il y a globalement moins de transactions.

Blockchain privée	Quelques centaines (Entreprise du CAC40)
Blockchain publique	Protocole Bitcoin (T1 2022) 80,7 millions de portefeuilles

# Les blockchains privées : avantages





# Les blockchains privées : inconvénients

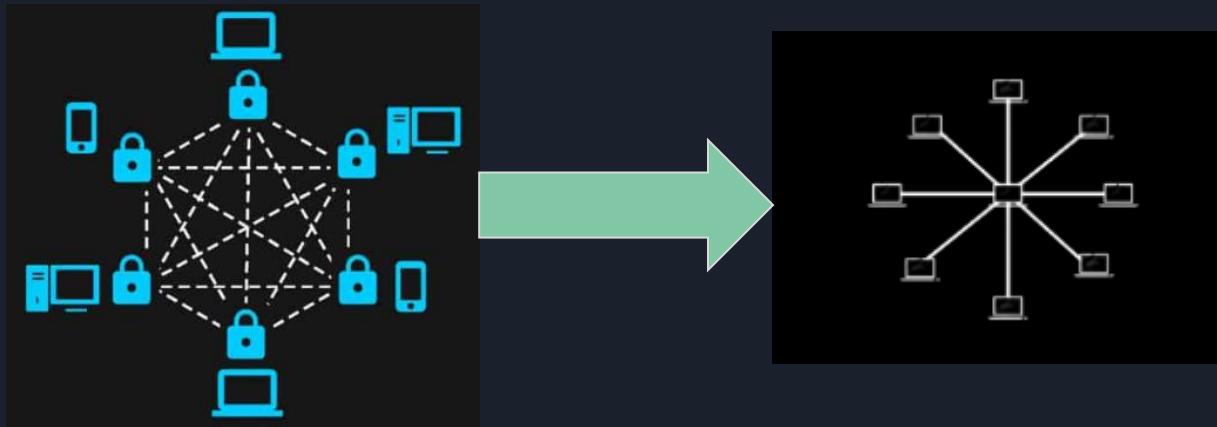
Les inconvénients des blockchains privées incluent l'affirmation controversée qu'elles ne sont pas de véritables blockchains.

La philosophie de base de la blockchain est la décentralisation. Il est également plus difficile d'obtenir une confiance totale dans les informations, puisque des nœuds centralisés déterminent ce qui est valide.

Le petit nombre de nœuds peut également signifier une sécurité moindre. Si quelques nœuds se rebellent, la méthode de consensus peut être compromise.

# Les blockchains privées : inconvénients

Le code source des blockchains privées est souvent propriétaire et fermé. Les utilisateurs ne peuvent pas le vérifier ou le confirmer de manière indépendante, ce qui peut conduire à une sécurité moindre. L'anonymat n'existe pas non plus sur une blockchain privée.



# Les blockchains privées

La rapidité des blockchains privées les rend idéales pour les cas où la blockchain doit être cryptographiquement sécurisée mais où l'entité qui la contrôle ne veut pas que le public ait accès aux informations.

Aujourd'hui les entreprises sont de plus en plus nombreuses à adopter cette technologie.

Le meilleur exemple français reste LVMH (Louis Vuitton Moët Hennessy) pour ses produits de luxe.



Un exemple : Walmart



# Un exemple : Walmart

Walmart est une entreprise transnationale américaine spécialisée dans la grande distribution.

Elle vend donc de la nourriture.

Dans un objectif de traçabilité, (par exemple de la viande) Walmart déploie actuellement via le framework Hyperledger Fabric, une blockchain privée afin de tracer la provenance de la nourriture.



<https://www.hyperledger.org/use/fabric>



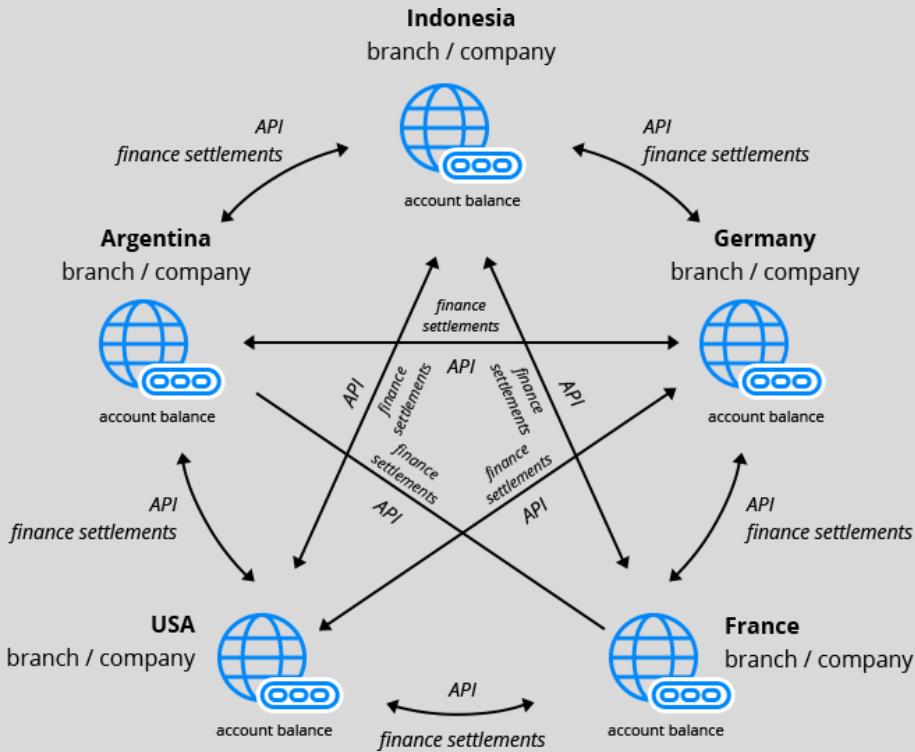
# Hyperledger Fabric

Hyperledger Fabric est un projet open source de la Linux Foundation. C'est un framework pour développer et déployer des blockchains d'entreprise, des Dapps (des Decentralized Apps).

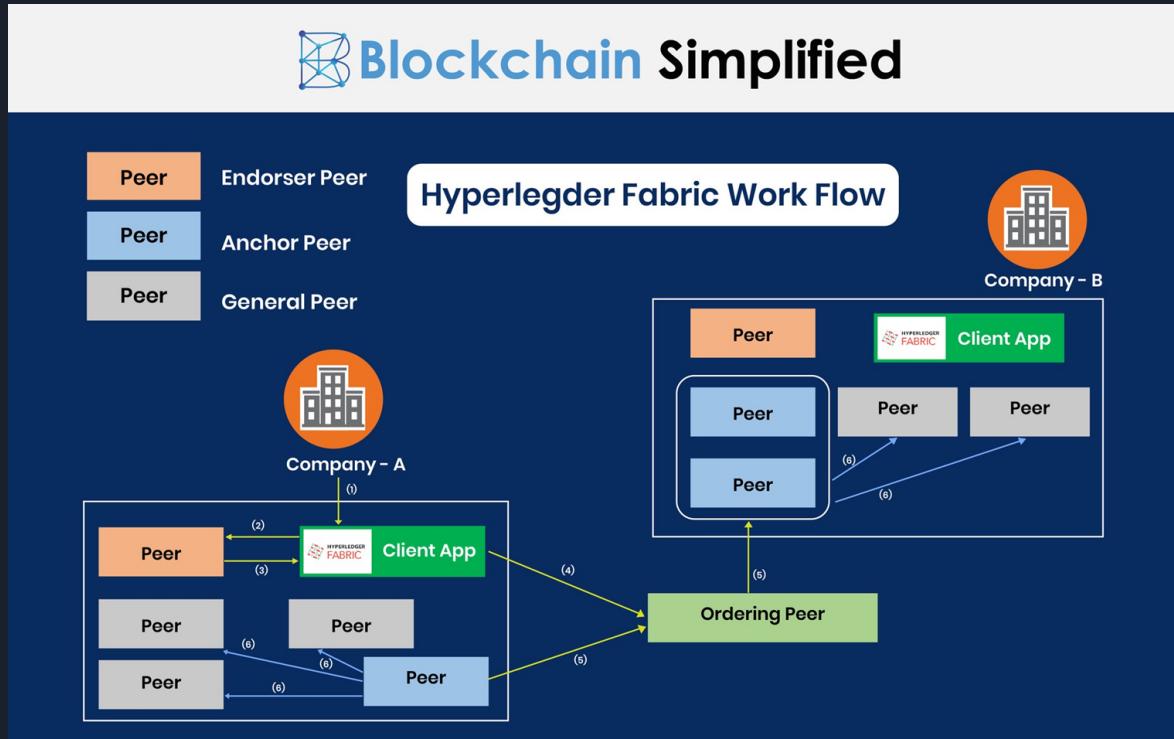
On y retrouve des composants plug-and-play, des architectures préconstruites pour faciliter le développement des ces Dapps

“Aujourd’hui 120 000 organisations et 15 000 ingénieurs travaillent sur cette technologie.”

# Comment fonctionne Hyperledger Fabric ?



# Hyperledger Fabric





# Les blockchains hybrides

Afin de combiner le monde de la Blockchain publique et privée, les entreprises peuvent allier ces 2 technologies afin de donner naissance aux blockchains hybrides.

Elle donne la possibilité aux entreprises et aux organisations de mettre en place un écosystème privé, pourvu d'autorisations, mais en conservant l'aspect publique en laissant une possibilité de vérification par des "smarts contracts".



# Les blockchains hybrides

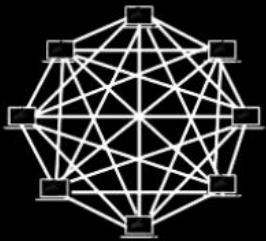
Même si une organisation privée peut posséder une blockchain hybride, elle ne peut pas modifier les transactions. De manière générale, les transactions et les enregistrements d'une blockchain hybride ne sont pas rendues publiques mais peuvent être vérifiées.

Même si une entité privée possède ce type de blockchain, elle ne peut pas modifier les transactions en son sein.

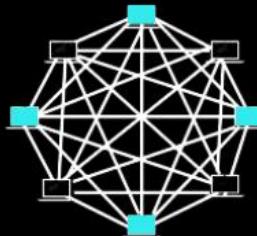
# Les blockchains de consortium

## • Archipels

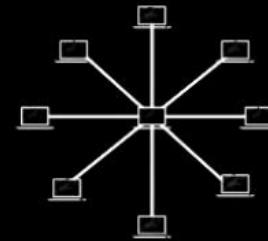
### Publique



### Consortium



### Privée



- Accessible à tout le monde, en lecture et en écriture
- Non soumise à une autorité centrale
- Tous les utilisateurs participants à la validation

- Certains acteurs peuvent valider les transactions
- Les transactions peuvent être publiques ou limité aux participants
- Système partiellement décentralisé

- Un seul acteur peut valider les transactions
- Le système est contrôlé
- Les utilisateurs sont identifiables



AURA



# AURA BLOCKCHAIN CONSORTIUM

## FOUNDING MEMBERS

---

LVMH    Mercedes-Benz    OTB    PRADA Group    RICHEMONT





# AURA Blockchain Consortium

Aura Blockchain Consortium est un rassemblement d'entreprises d'abord initié par LVMH, Prada Group, Richemont et Cartier en 2021, rejoint par la suite par OTB en octobre 2021 et Mercedes Benz en mai 2022.

L'objectif est de permettre d'authentifier les produits d'origine de ces marques en les couplant par des NFT dans des Smarts Contracts.



LUXURY AUTHENTICATION



SUPPLY CHAIN TRANSPARENCY



TRANSFER OF OWNERSHIP



PERSONAL RELATIONSHIP



CONVENIENCE & CIRCULAR ECONOMY



SUSTAINABLE BLOCKCHAIN

*<https://auraluxuryblockchain.com/>*

# Aura Standard

Aura Standard is a self-managed offering for brands that care about decentralization and want control over data. The Aura Blockchain Consortium's software is run directly by the brand and the brand participates in the blockchain governance.

[JOIN US](#)

## ARCHITECTURE / INFRA

- ✓ Self-managed infrastructure via Microsoft Azure ®™ subscription
- ✓ Customizable APIs & SDKs
- ✓ Self-managed data privacy

# Aura SaaS

Aura SaaS is an offering for brands that want to quickly leverage the Aura Blockchain Consortium's software without the hurdle of hosting the solution. Brands use blockchain as a service without running any node.

[JOIN US](#)

## ARCHITECTURE / INFRA

- ✓ SaaS offering, managed by Aura Blockchain Consortium
- ✓ Default APIs & SDKs
- ✓ Data privacy managed by Aura Blockchain Consortium



# Les layers en blockchain

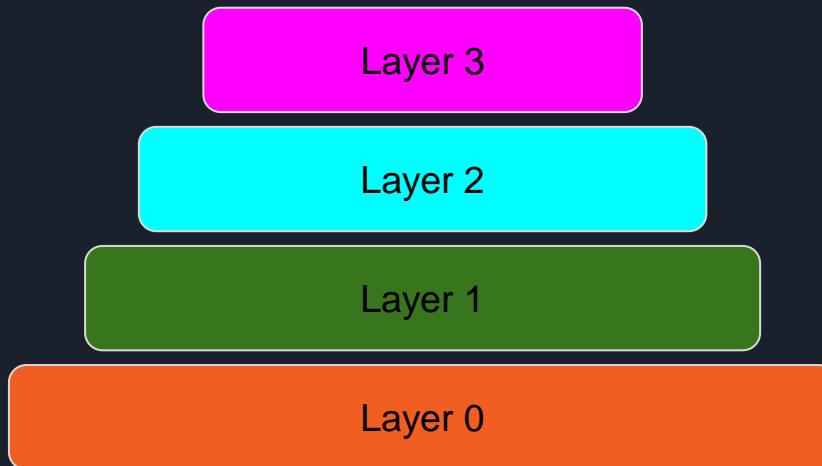
Le terme de “layer” en blockchain est utilisé pour décrire la “couche” sur laquelle se situe une blockchain.

Ces couches vont regrouper un ensemble de composants nécessaires pour le fonctionnement d'une blockchain.

Chaque couche de “niveau supérieur” vient compléter une couche de “niveau inférieur” en ajoutant des fonctionnalités ou des applications.

# Les layers en blockchain

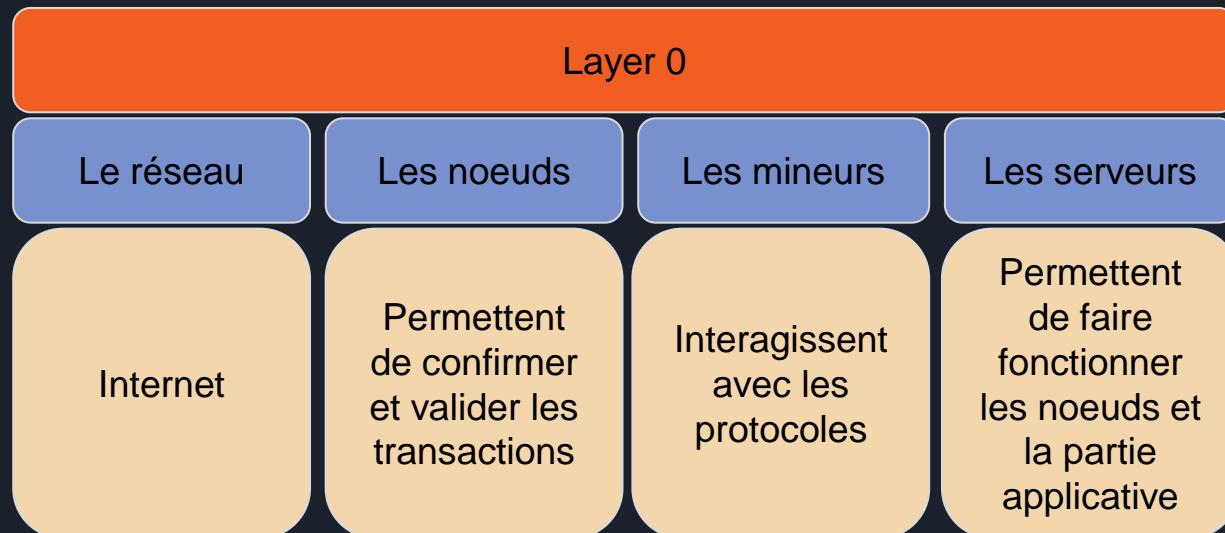
On peut matérialiser les layers (ou couche) par une pyramide :



# Le Layer 0 : Le socle commun

Le layer 0 est l'ensemble des composants communs permettant à toute blockchain de fonctionner.

Elle va regrouper les éléments suivants :





# Le Layer 0 : Le socle commun

Ces composants de base vont permettre le fonctionnement d'une blockchain de manière décentralisée et connectée. Chaque module est indispensable à la stabilité d'une blockchain.

Le layer 0 est le noyau d'une blockchain.



# Les protocoles de Layer 0

Les “protocoles de Layer 0” sont des ensembles de fonctionnalités qui vont s’intégrer au layer 0 sans avoir à créer un layer de niveau supérieur.

Ils ont pour but de résoudre des problèmes récurrents comme :

La scalabilité  
(vitesse des transactions sur la blockchain)

L’interopérabilité  
(communication entre les blockchains)

La sécurité

# Les protocoles de Layer 0

Au lieu de créer des couches supplémentaires pour résoudre ces problèmes, les développeurs ont décidé de prendre le problème à l'envers.

Ils vont développer au maximum les fonctionnalités d'un layer jusqu'à ce que le besoin de créer une nouvelle couche soit nécessaire.

## Scalabilité

Créer une blockchain plus facilement à l'aide d'un SDK

## Interopérabilité

Faciliter la communication entre les différentes blockchain qui utilisent la même base

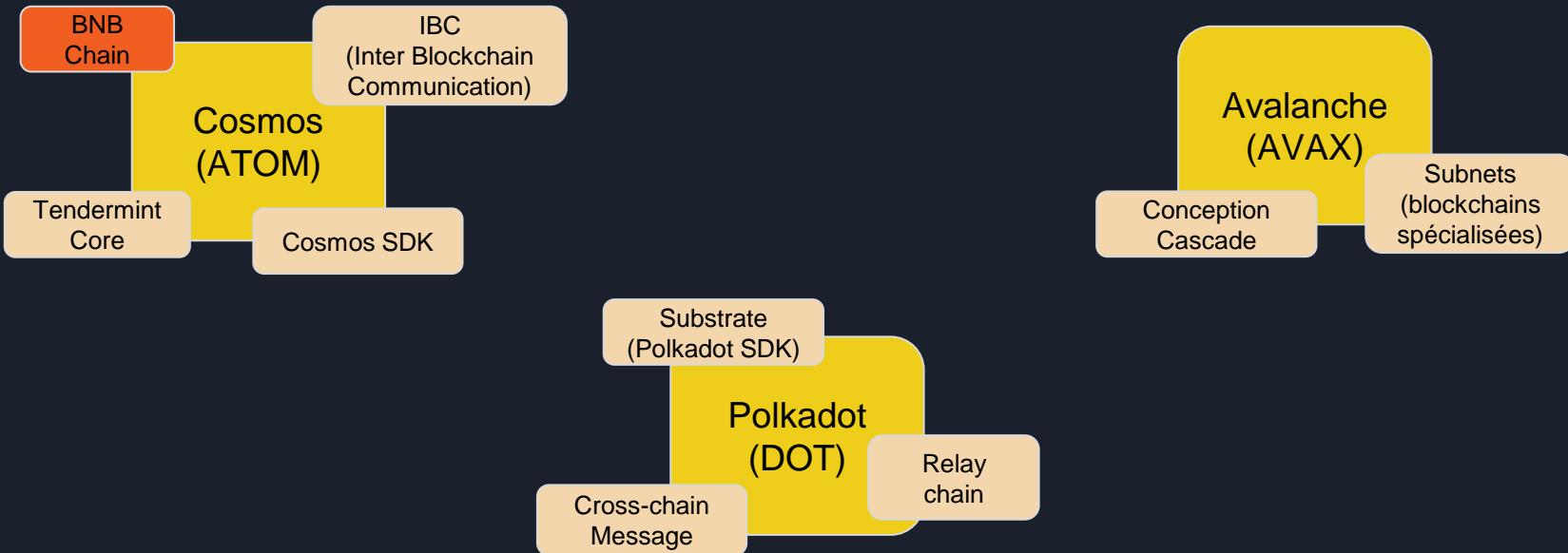
Utiliser le même système de consensus

## Sécurité

Utiliser le même système de stockage d'information

Améliorer la sécurité d'une infrastructure sans devoir forcément la gérer

# Les protocoles de Layer 0



# Cas d'étude : COSMOS



CØSMOS





# Les protocoles de Layer 0

On observe que chaque blockchain et son écosystème repose sur le layer 0 mais dispose de son propre protocole du même niveau.

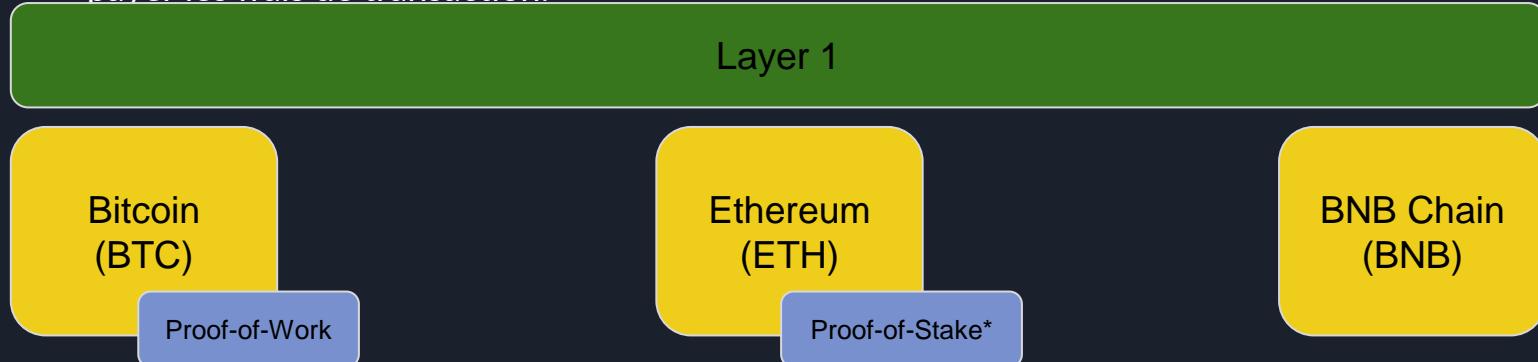
C'est un modèle de conception qui permet soit de simplifier la création de nouvelles blockchains, soit de réutiliser des modèles existants parmi ceux déjà créées.

On les appelle également "blockchain d'infrastructure"

# Les protocoles de Layer 1

Les protocoles de layer 1 sont des blockchains indépendantes. Elles ne dépendent d'aucune autre couche supérieure pour fonctionner.

Généralement les protocoles de layer 1 se servent du jeton mère de la blockchain pour payer les frais de transaction.





# Les protocoles de layer 2

Les layers 2 en blockchain sont dépendants de la première couche et de leur blockchain mère. Leur but est de venir ajouter des fonctionnalités et des optimisations.

Layer 1

Layer 2

Scalabilité

Anonymat/pseudonymat

Modularité



# Les protocoles de layer 2

Au lieu d'utiliser la blockchain mère, les protocoles de layer 2 vont réaliser certaines opérations spécifiques pour éviter de surcharger la blockchain mère ou s'ils n'ont pas l'autorisation de travailler dessus.

Layer 1 : Bitcoin

Layer 2 : Protocole Lightning Network

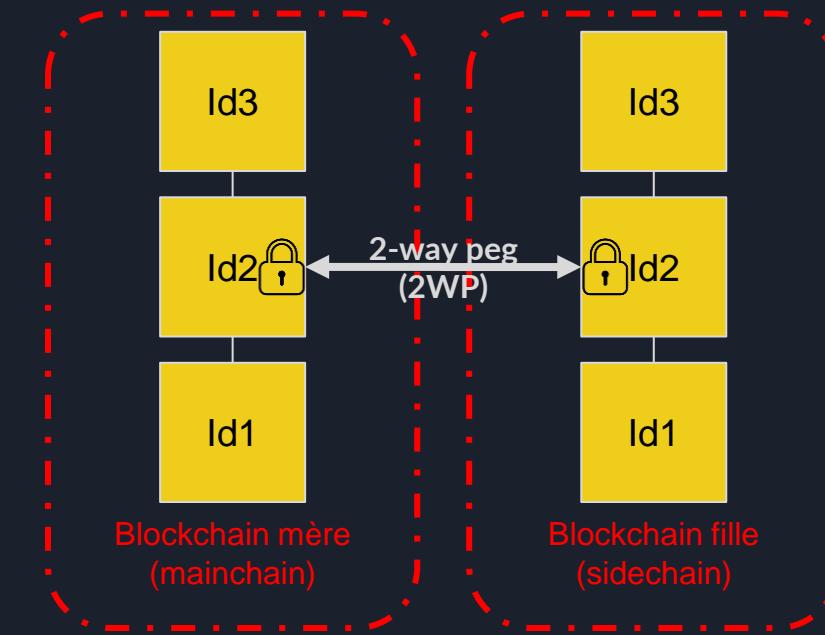
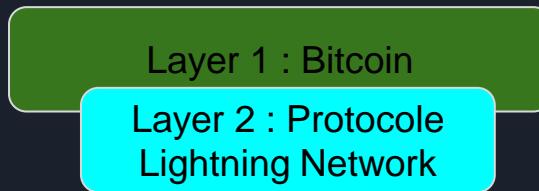
Transaction Off-chain

Scalabilité

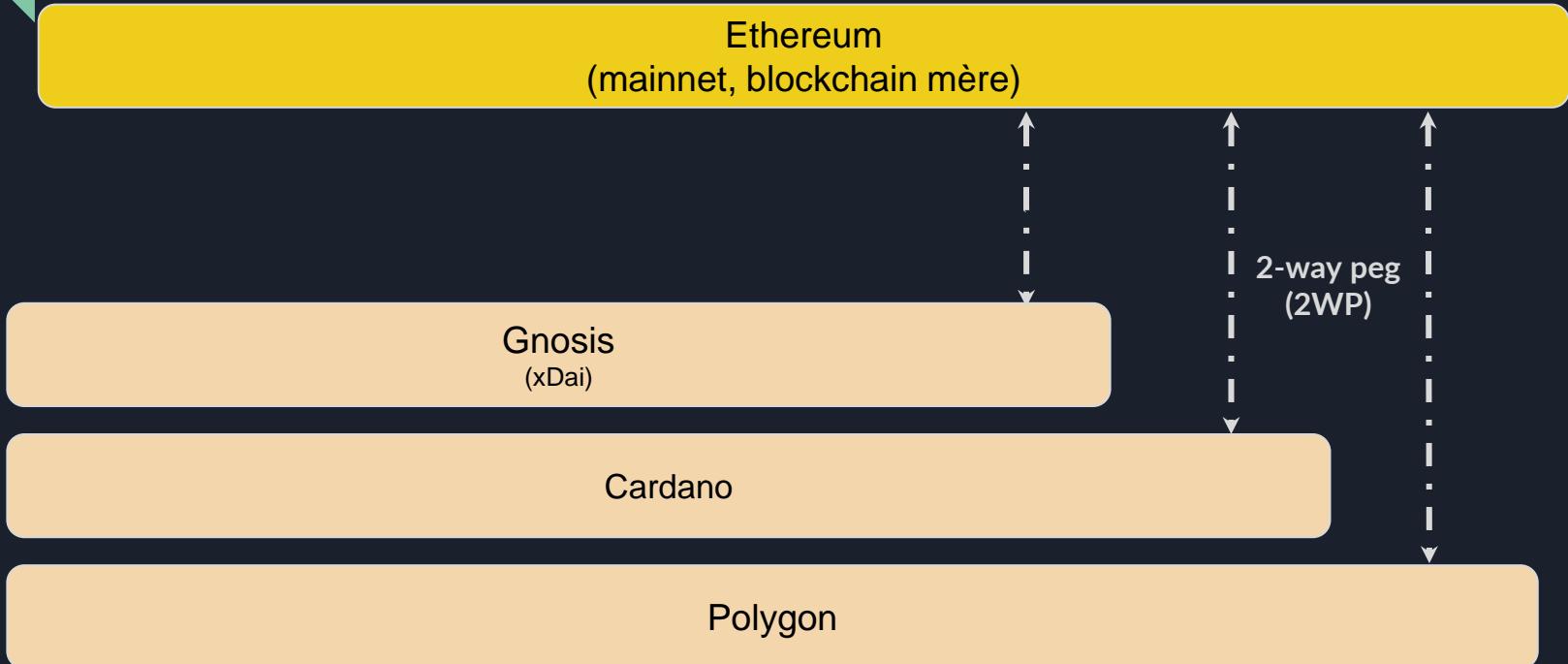
Vitesse de transaction

# Les sidechains

Les sidechains sont des blockchains construites en parallèle d'une autre blockchain mère alors que les protocoles de layer 2 sont construits sur la blockchain mère. Le concept date de 2014.



# Les sidechains

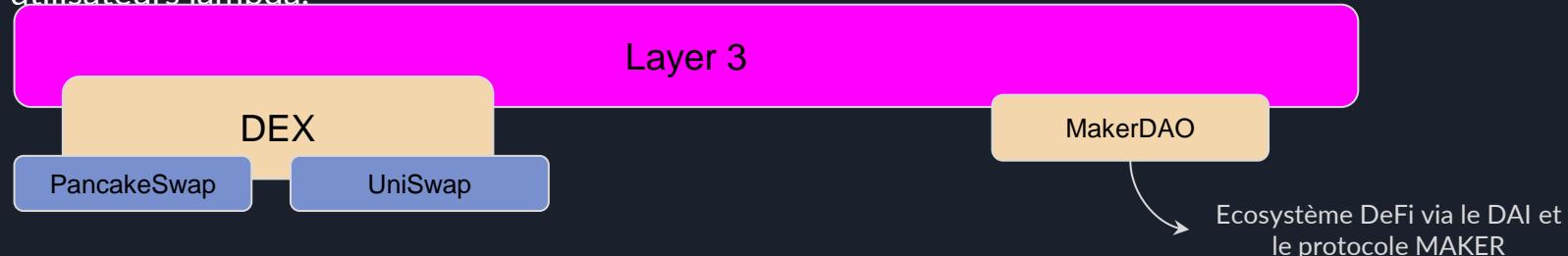


# Les protocoles de layer 3

Les protocoles de layer 3 sont les protocoles de plus haut niveau. On y retrouve la couche applicative.

C'est l'IHM avec laquelle nous interagissons au quotidien. On y retrouve les ***Dapp (ou D-App, applications décentralisées)***

L'objectif est de faciliter l'utilisation et l'interaction entre les blockchains pour les utilisateurs lambda.





# Les protocoles de layer 3

Aujourd’hui, de plus en plus de développeurs blockchain créent et déploient de nouvelles alternatives et technologies notamment via les layer 3.

Ces dernières se veulent plus accessibles et faciles d’utilisation notamment dans leur communication avec les couches inférieures.

La layer 1 et la layer 2 étant liées de par leur conception, les protocoles d’interopérabilité évite de rajouter une couche de complexité lors du développement d’une Dapp par exemple.

L’un des rôles de la layer 3 est donc de faciliter la communication et l’interopérabilité entre 2 blockchains en faisant abstraction de leurs différences de fonctionnement.



# Conclusion

On peut donc comprendre que les couches de plus bas niveau sont les plus importantes et servent de socle au fonctionnement d'une blockchain. Si une couche de niveau inférieur ne fonctionne pas, les couches supérieures ne peuvent pas fonctionner.

Néanmoins, une couche de blockchain peut fonctionner même si un layer de niveau supérieur est dysfonctionnel.

L'objectif de ces couches est donc d'avoir une base commune performante et évolutive pour répondre à l'adoption croissante de ces dernières années.



# Conclusion

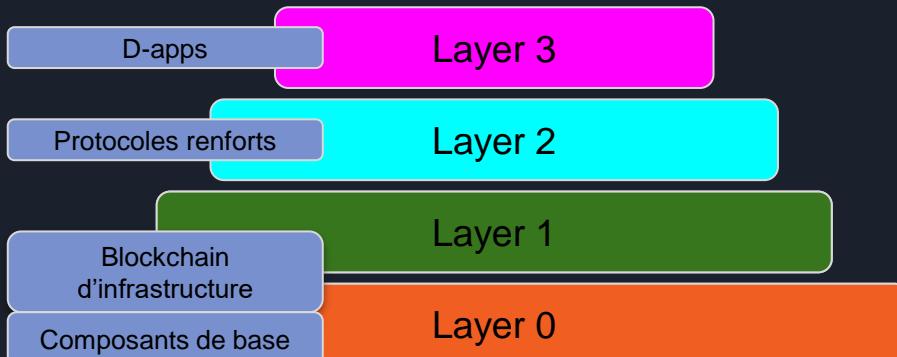
Ce type de solution permet aussi à de nouvelles équipes de proposer des alternatives d'optimisation tout en reposant sur une infrastructure déjà existante et fonctionnelle ou qui ne disposerait pas des droits nécessaires pour modifier un niveau inférieur.

Une façon d'améliorer l'évolutivité du réseau en combinant les différents composants et fonctionnalités.

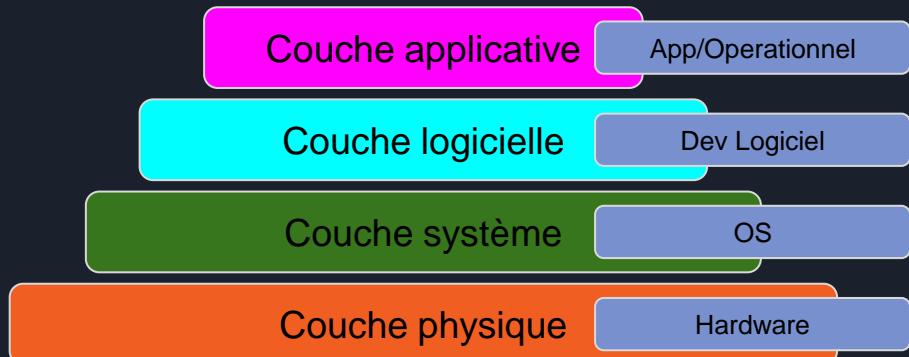
# Conclusion

Un layer est donc une couche qui rassemble des fonctionnalités et des composants inhérents au fonctionnement d'une blockchain. Les couches de plus bas niveau sont les plus importantes pour le développement des couches de haut niveau.

Les layers en Blockchain



L'architecture d'un SI





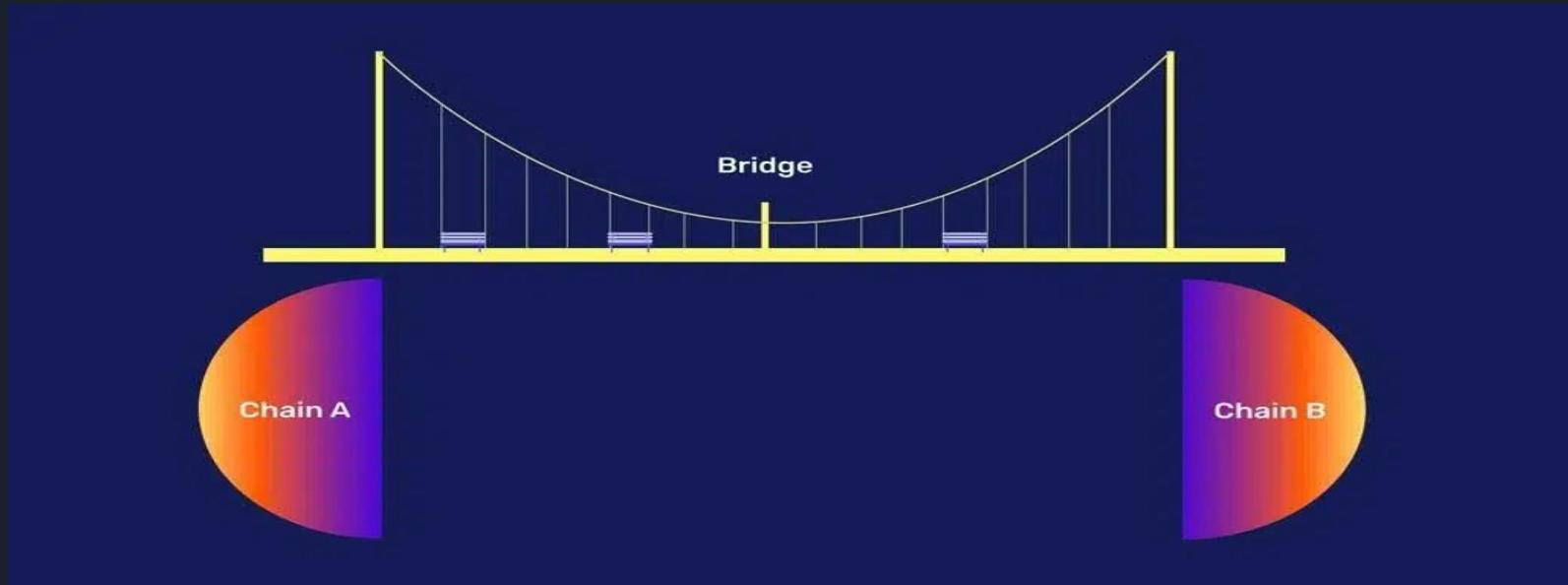
# L'interopérabilité

Dans le monde de la blockchain, l'interopérabilité permet d'apporter un langage commun aux différents acteurs de l'écosystème.

Elle permet des interactions entre les blockchains. C'est-à-dire qu'elles peuvent également échanger et se partager des données et de la valeur comme des crypto-monnaies ou des NFT.

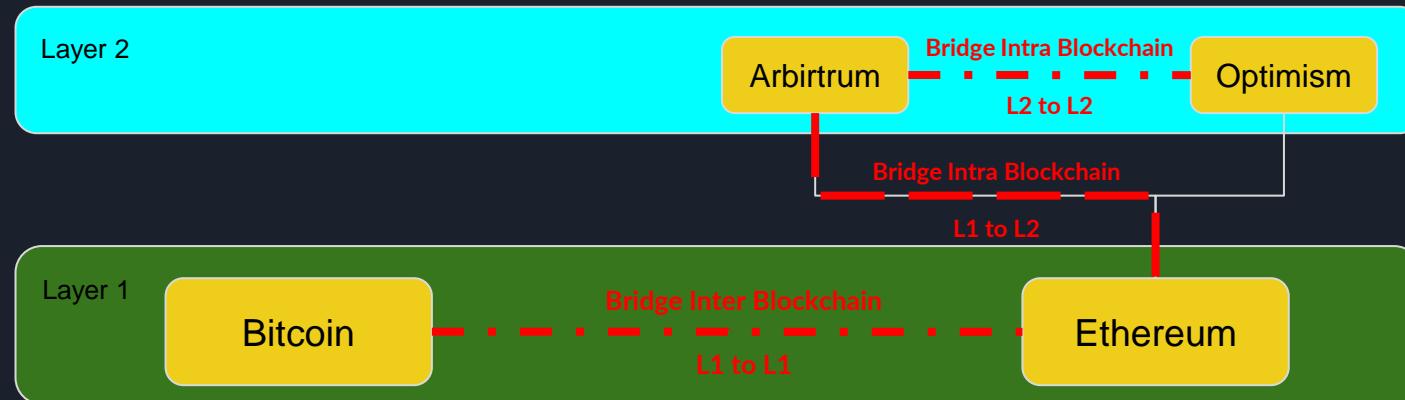
Elle peut également augmenter les performances des blockchains principales. Chacune de ces nouvelles couches vient apporter une ou plusieurs améliorations aux couches précédentes.

# Les “bridges” : la connexion entre les blockchains



# L'interopérabilité

L'interopérabilité est d'abord possible grâce aux bridges. Autrement dit, des ponts permettent de relier les différentes blockchains et layers entre elles.



Tous ces bridges peuvent opérer soit en sens unique, soit à double sens.



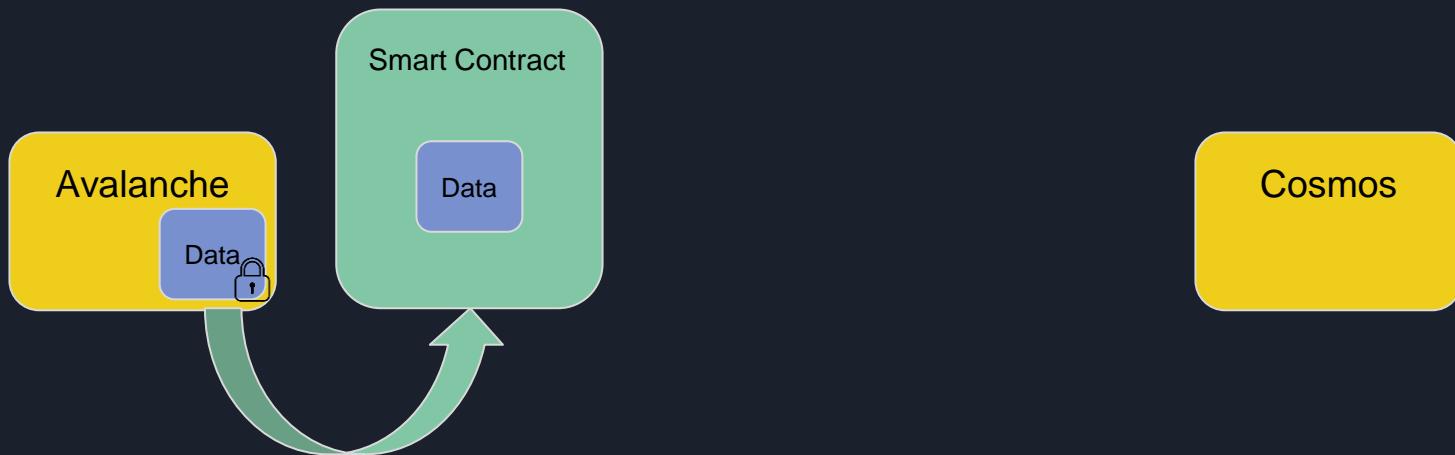
# L'interopérabilité

Généralement, les tokens ou les données à transmettre venant de la blockchain émettrice sont bloqués dans un **smart contrat** afin de ne plus être utilisables. En échange, une copie exacte de ce smart contrat est créée sur la blockchain cible choisie.

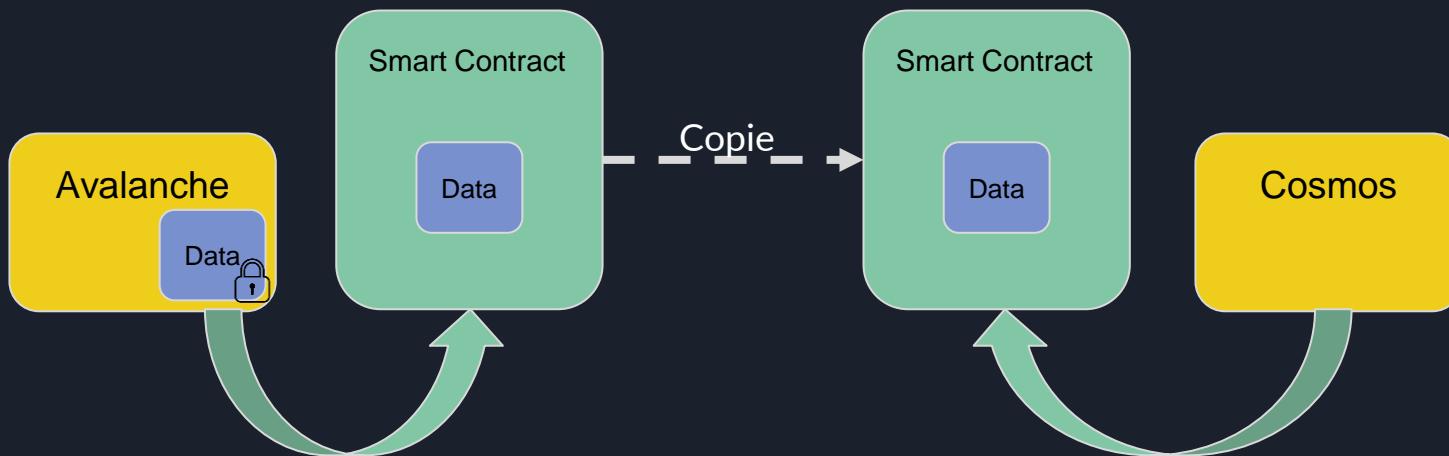
Avalanche

Cosmos

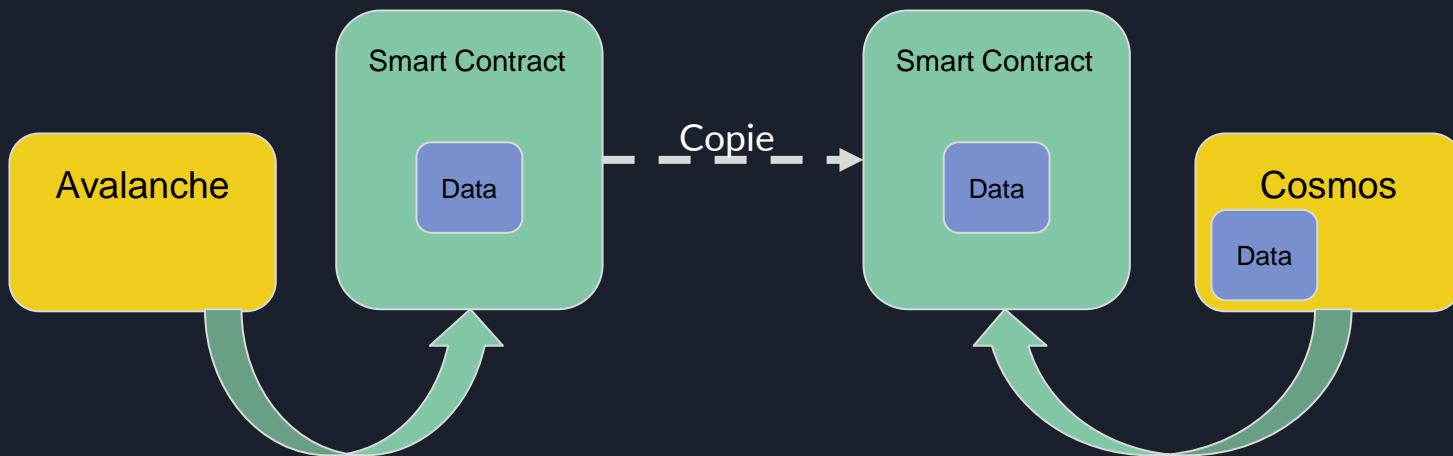
# L'interopérabilité



# L'interopérabilité



# L'interopérabilité



# L'interopérabilité

Avalanche

Cosmos

Data

# L'interopérabilité

Les layers 3 font partie des bridges créées. Ils permettent une interopérabilité entre plusieurs blockchains.

L'entreprise Starkware à travers sa solution Starknet actuellement en développement promettant de pouvoir relier tous les layers d'une même blockchain sans contrainte.

Le fonctionnement de ces bridges varie selon leurs caractéristiques et le problème qu'ils visent à résoudre. Les ponts peuvent être centralisés ou décentralisés, changeant également leur fonctionnement.



<https://starkware.co/>

# L'interopérabilité : les avantages

L'interopérabilité apporte des avantages à toutes les parties qui utilisent la blockchain.

## Les développeurs

Collaboration cross-chain pour les protocoles

Collaboration multi projets

Mise en commun de règles de sécurité et de protocoles

Diminution de la surcharge réseau

## Les utilisateurs

Facilitation des transactions

Diminution des frais de transaction

Découverte d'autres Blockchains

# L'interopérabilité : les risques

Le risque principal provient des bridges inter blockchains.

En 2022 le réseau Ronin a subi un hack de 173 600 ETH

soit 635 millions de dollars.





# L'interopérabilité

Dans l'écosystème COSMOS, une nouvelle solution a été développée permettant une interopérabilité entre plusieurs blockchains.

Il s'agit de l'IBC : L'inter-Blockchain Communication

Contrairement aux bridges, il n'existera pas de blocage de transaction sur la blockchain de départ pour pouvoir se servir des données sur la blockchain d'arrivée. Seul un smart contract va permettre d'envoyer via un langage commun inter-blockchain l'information sur la blockchain d'arrivée.

En évitant l'utilisation d'un bridge, on évite les risques de hack.



# L'interopérabilité

La sécurité est donc au cœur des protocoles de chaque blockchain. l'objectif étant de ne pas créer d'effet Black Swan (succession d'événements tragiques) sur tout un écosystème.

L'interopérabilité des blockchains semble être un excellent moyen de pérenniser l'écosystème en profitant du meilleur de chacun des nouveaux éléments ajoutés.

Elle fonctionne comme un gigantesque mille-feuille où les couches s'additionnent pour former un ensemble commun.

Néanmoins, plus il y a de couches, plus la base peut se fragiliser, plus les risques pour la sécurité des données, des transactions et donc des fonds des utilisateurs.

Merci de votre attention