

La blockchain et les cryptomonnaies



Qu'est-ce que la monnaie ?

- Unité de compte



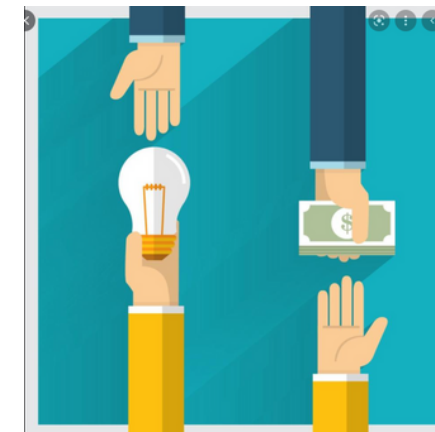
- Réserve de valeur



- Intermédiaire d'échanges



CONFIANCE



Premières banques

Le principe de d'emprunt et de prêt à intérêt existe depuis même plus longtemps que la monnaie elle-même

Le principe de protéger son argent à la banque existe depuis le 7^e siècle av. J.C.

Les banques aujourd'hui ont naturellement pour but de stocker notre argent et de nous permettre d'emprunter

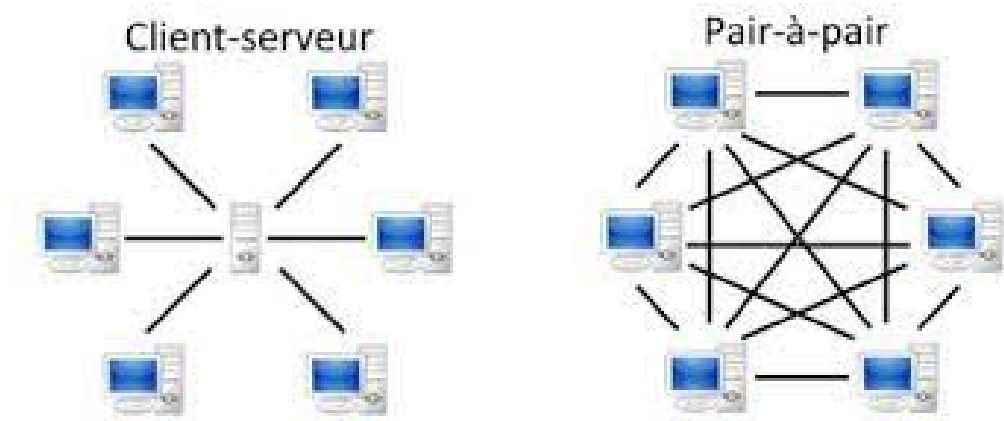
Mais cet objectif s'est rapidement perdu au profit de la cupidité des banquiers, qui manipulent notre argent

Cela à mené à la crise financière de 2008 et à la naissance du Bitcoin

Naissance du Bitcoin

Présenté en 2008 par une personne, ou groupe de personne, sous le pseudo Satoshi Nakamoto sur le site [bitcoin.org\(/bitcoin.pdf\)](https://bitcoin.org/bitcoin.pdf)

Protocole de paiement pair-à-pair, et donc décentralisé



Des protocoles pair à pair existaient déjà : BitTorrent, eMule, ...

Système de clé publique et clé privée pour signer les transactions.

Une blockchain pour la décentralisation.



Qu'est-ce qu'une blockchain ?

Registre distribué de transactions

Les transactions sont ajoutées à la file dans un bloc

Ce bloc est ensuite validé par le réseau

Si des transactions étaient "illégales" alors elles sont annulées

Permet de synchroniser toutes les machines du réseau

Pouvoir "backup" la blockchain à un certain bloc

Les Noeuds

Contient partiellement ou toutes les données de la blockchain

Éléments principaux du réseau

Enregistrent les nouveaux blocs

Fournissent aux mineurs (les faux) les données utilisateurs

Un noeud n'est pas forcément un mineur, mais un mineur (un vrai) est un noeud

Rôles possibles d'un Noeud :

Propagation

Décentralisation

Partage

Vérification

Ajout

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed Dec 1 20:56:03 2021 CET.

14814 NODES

24h

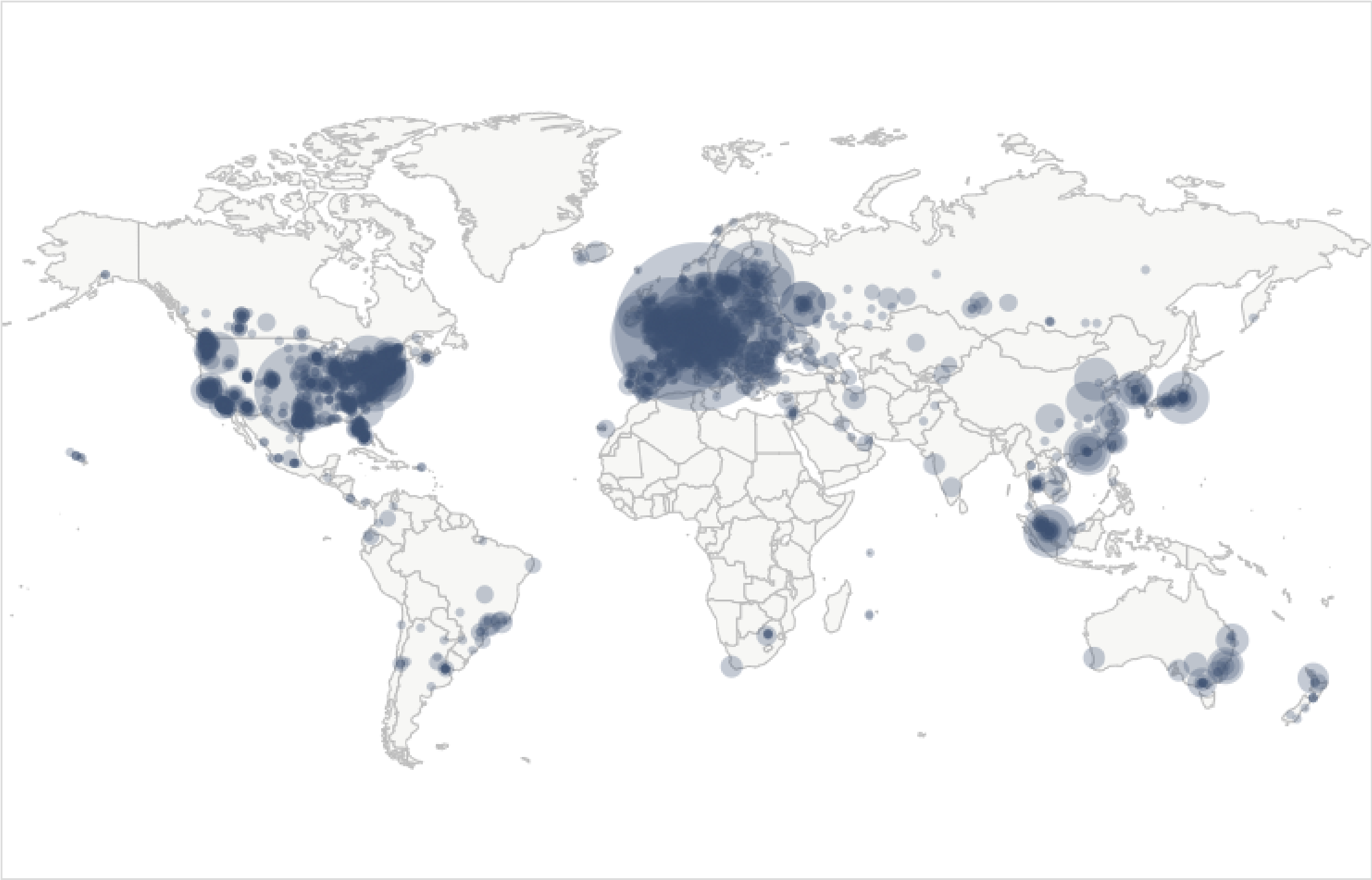
90d

1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	7588 (51.22%)
2	United States	1806 (12.19%)
3	Germany	1794 (12.11%)
4	France	557 (3.76%)
5	Netherlands	378 (2.55%)
6	Canada	294 (1.98%)
7	United Kingdom	222 (1.50%)
8	Finland	204 (1.38%)
9	Russian Federation	177 (1.19%)
10	China	135 (0.91%)

More (85) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Les mineurs

Valident les transactions, ils font les calculs nécessaires à la validation d'un bloc

Dépensent de l'énergie pour valider les transactions

Un mineur est un nœud du réseau se contentant de valider les transactions

Un seul mineur est récompensé lorsqu'un bloc est validé (1 bloc/10 min ~)

Systèmes de "pools" de minage, fusion de la puissance de calcul et répartition de la récompense

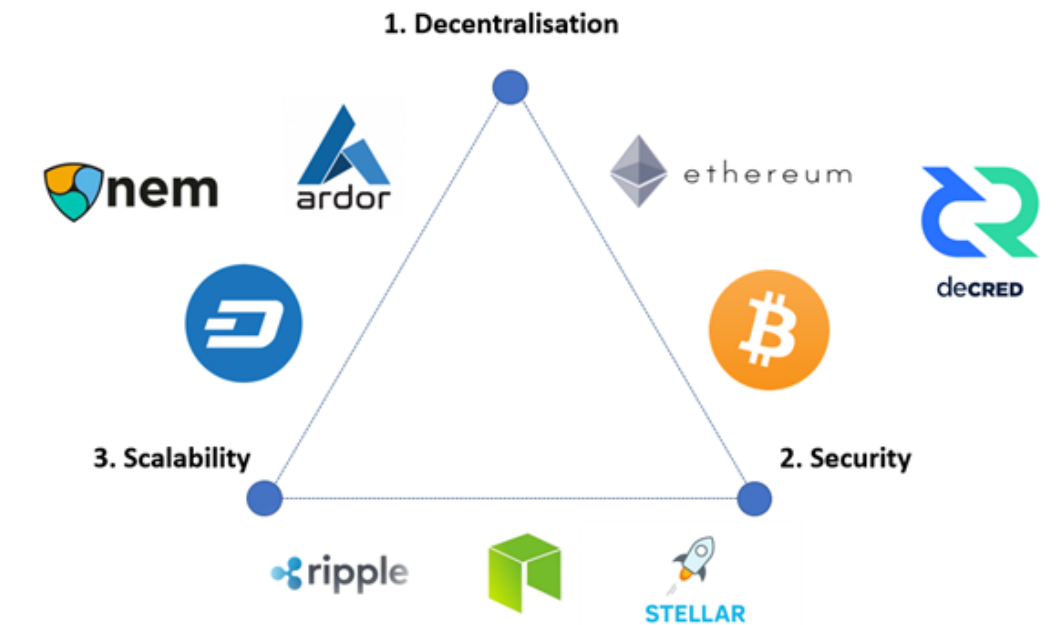
Inconvénients du réseau

Trilemme : Sécurité, Scalabilité, Décentralisation

Sécurité: Transactions infalsifiables

Scalabilité : Grosse capacité de traitement de transactions

Décentralisation : Maximum de machines sur le réseau



Bitcoin :

- 3-6 tx/s
- Frais 2-20\$
- 10,000+ Nodes

Ethereum :

- 15 tx/s
- Frais 10-200\$
- 10,000+ Nodes

Elrond EGLD :

- 3000 tx/s
- Frais : 0.01-0.1 \$
- 3200 Nodes

Visa :

- 3000 tx/s
- Frais : 0
- Centralisé

Solutions : Lightning Network, Segwit

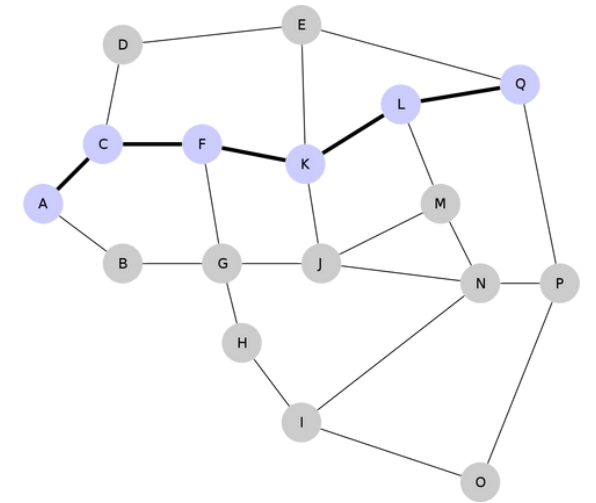
Le Lightning Network est un réseau de seconde couche (Layer 2)

Le LN permet des transactions quasi-instantanées et quasi-sans frais

Le LN est actuellement utilisé au Salvador, premier pays à avoir considéré le Bitcoin comme monnaie légale

SegWit est un SoftFork du réseau Bitcoin, une mise à jour

SegWit permet de retirer certains paramètres de transactions permettant aux transactions de peser moins lourd et donc d'en caser plus dans un bloc



Ethereum et les smart contracts

Co-Fondée par Vitalik Buterin en 2015



Ethereum c'est comme Bitcoin sauf qu'il y a ce qu'on appelle des smart-contracts

On peut donc qualifier cette blockchain de "Blockchain d'infrastructure"

La crypto-monnaie "Ether" est le carburant de la blockchain

Blockchain développée et soutenue par la Ethereum Foundation une OBNL

Un smart contract, c'est quoi ?

C'est un contrat sur la blockchain, un contrat qui s'exécute seul, et donc "intelligent"

Une adresse au même titre que celle que vous possédez grâce à votre clé privée

Une adresse contrôlée par un code et seulement ce code

Du code au même titre que du code en C ou en Java, mais qui tourne sur une blockchain

Manipulation de valeur de manière décentralisée

Création de Tokens indépendant sur les blockchains

Un smart contract est immuable, on ne peut pas le modifier, ni le supprimer

Finance Décentralisée

Pouvoir être acteur de la Finance sans passer par des fonds d'investissements, des banques, ou des brokers

Concept d'application décentralisée (dApp). Donc une application où le backend est géré seulement par un smart contract

Grandes plateformes auto-suffisantes d'échange, de staking et de prêt de liquidités

- AAVE, Compound, 1Inch
- PancakeSwap, BakerySwap
- Pangolin Exchange, Lydia Exchange
- Maiar Exchange

Les NFTs

Un NFT est un token non fongible (Nun Fongible Token), c'est un type spécial de Token et donc de smart contract auquel on a rattaché un fichier.

Cela permet de donner une identité numérique à un fichier, et donc de créer un "objet" sur une blockchain

La non fongibilité d'un token indique son immuabilité, son incorruptibilité

On peut donc s'assurer qu'un NFT est bien le bon NFT, et donc lui adosser une valeur

Aujourd'hui les NFTs sont surtout connus pour leur principe d'"Art numérique", où un artiste va créer une œuvre et la publier sous forme d'NFT.

Mais en réalité un NFT peut proposer énormément plus.

Cas d'utilisation d'un smart contract

Un smart contract va automatiser toute tâche qui relève de la manipulation de valeur

Exemple : Salaires des employés d'une entreprise, une assurance, une banque d'emprunt

Mais il peut aussi servir d'API pour des objets connectés par exemple

Allumer une lampe connectée, déverrouiller une chambre d'hôtel, se servir de la bière à une tireuse automatisée

Et on peut aller encore bien plus loin, une chaîne de super marché automatisé, des systèmes de votes en ligne sûrs,...etc.

Les autres blockchains

Il existe des centaines d'autres blockchains, proposant toutes quelque chose d'unique ou innovant

Transactions :

- Bitcoin
- Litecoin
- Dogecoin
- Monero
- ...

Infrastructure:










- Ethereum
- Solana
- Binance Smart Chain
- Elrond
- ...

Décentralisation de fichiers :


- Filecoin
- BitTorrent
- ...

Gaming :

- Decentraland
- The Sandbox
- WaxP
- ...

#	Nom	Prix	24h %	7d %	Cap. Marché	Volume (24 h)	Offre en Circulation
1	 Bitcoin BTC Acheter	€50,020.36	-1.47%	-4.45%	€946,555,929,268	€31,852,332,522 635,624 BTC	 18,888,843 BTC
2	 Ethereum ETH Acheter	€4,037.63	-4.02%	+3.71%	€479,857,610,551	€23,031,095,259 5,691,079 ETH	118,574,805 ETH
3	 Binance Coin BNB Acheter	€549.34	-4.07%	+2.09%	€91,862,973,722	€2,341,141,569 4,250,952 BNB	166,801,148 BNB
4	 Tether USDT Acheter	€0.8834	-0.72%	+1.56%	€65,425,052,577	€69,974,601,729 79,234,773,247 USDT	74,083,154,139 USDT
5	 Solana SOL	€202.10	-2.50%	+8.35%	€61,590,462,373	€3,391,608,815 16,823,335 SOL	305,506,040 SOL
6	 Cardano ADA	€1.40	-1.16%	+6.34%	€46,620,476,228	€1,476,868,316 1,055,314,807 ADA	 33,313,246,915 ADA
7	 XRP XRP	€0.8629	+3.55%	+7.42%	€40,790,092,547	€2,141,296,855 2,478,633,585 XRP	 47,216,103,219 XRP
8	 USD Coin USDC	€0.884	+0.58%	+1.45%	€34,478,317,200	€4,499,720,802 5,091,511,368 USDC	39,012,808,059 USDC
9	 Polkadot DOT	€31.70	+5.02%	+9.66%	€31,376,706,658	€1,042,952,853 32,828,857 DOT	987,579,315 DOT
10	 Dogecoin DOGE	€0.1905	-0.01%	+2.72%	€25,132,487,673	€1,432,639,192 7,544,919,281 DOGE	132,358,930,217 DOGE







Used by millions. Trusted with billions.

PancakeSwap has the most users of any decentralized platform, ever.
And those users are now entrusting the platform with over \$14 billion in funds.


Will you join them?



**2.8 million
users**
in the last 30 days



**31 million
trades**
made in the last 30 days



**\$14 billion
staked**
Total Value Locked

BitTorrent X

Le plus grand réseau distribué au monde, alimenté par BTT.

PLUS DE

200 millions
de portefeuilles

2 milliards
d'utilisateurs

100 millions
de MAU

Téléchargement du client **FREE**

Obtenez BTT

We expect that BitTorrent, the world's biggest decentralized protocol, will one day revolutionize the entire online gaming industry.

- Blizzard Entertainment

Protocole BitTorrent utilisé par :

NETFLIX facebook Google twitter LIONSGATE 

Ethereum Virtual Machine et autres

Technologie qui permet aux smart contracts Solidity de s'exécuter sur la blockchain

Arwen VM de Elrond : C, C++, C#, Rust, Go, TypeScript...

Solana : Rust et c'est tout.

Avalanche : X-Chain, C-Chain et P-Chain

Intérêt de ces blockchains : Interopérabilité, et facilité de migration des smart contracts
Ethereum

Le langage Solidity

Langage de programmation orienté objet dédié à l'écriture de smart contracts

Variables d'instances, constructeur, fonctions, procédure...

Environnement qui se distingue de celui d'un langage traditionnel

Rien de très compliqué mais un immense champ des possibles

Contrats accessibles depuis n'importe où dans le monde

```
1 // SPDX-License-Identifier: UNLICENSED
2 pragma solidity >=0.7.0 <0.9.0;
3
4 contract Demonstration {
5
6     address public owner;
7     mapping(address => uint) public totalDepot;
8     mapping(address => uint) public totalRetire;
9
10    constructor(address Owner) {
11        owner = msg.sender;
12    }
13
14    function printTest() public pure returns(string memory) {
15        return "test";
16    }
17
18    function deposit() public payable {
19        totalDepot[msg.sender] += msg.value;
20    }
21
22    function withdraw(uint montant) public {
23        require(montant <= totalDepot[msg.sender]-totalRetire[msg.sender], "Tu ne peux pas retirer plus que ce que tu as depose");
24        payable(msg.sender).transfer(montant);
25        totalRetire[msg.sender] += montant;
26    }
27 }
```

**Voilà c'est fini let's go posez
des questions**