Présentation globale à la blockchain et aux cryptomonnaies

Sylvain Debras
ACII by Audensiel

AUDENSIEL

audensiel.com

Sommaire

- Qu’est ce qu’une blockchain ?
- Fonctionnement global d’une blockchain
- Les Smart Contracts
- Les cas d’usage
- Le trilemme de la blockchain
- Web2 vs Web3
- Le Bitcoin et son halving
- Les Altcoins
- Conclusion

Qu’est qu’une blockchain ?

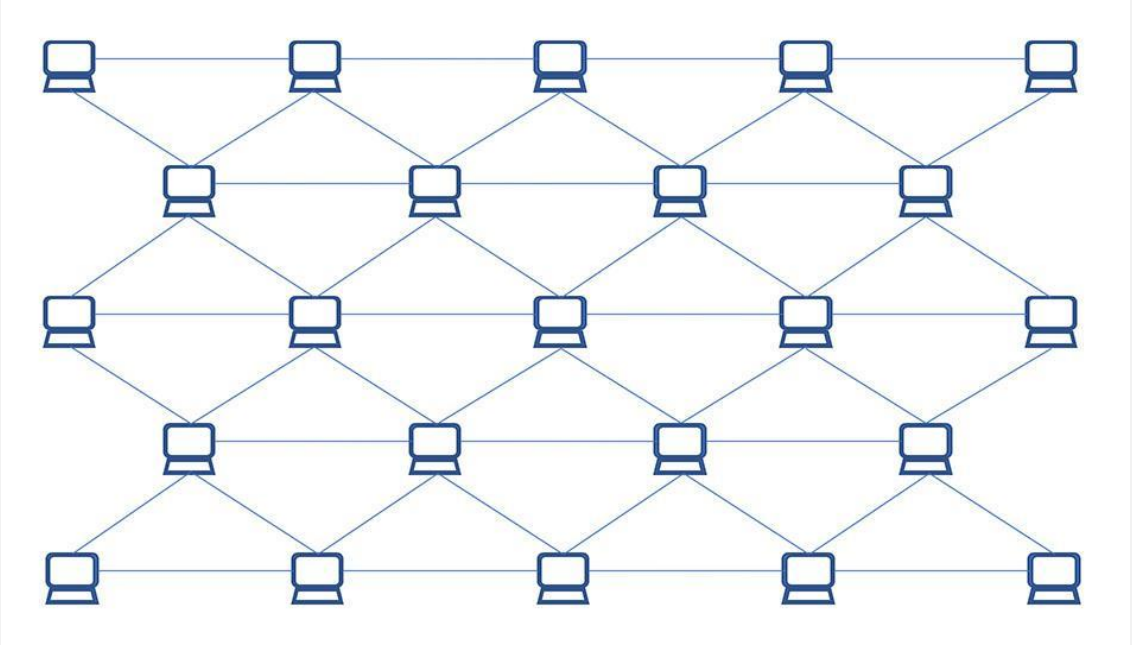
- Un nouveau concept numérique pour stocker des données sous forme de blocs chaînés les uns aux autres => Immuable
- Chaque transaction est regroupée avec d’autres dans un “bloc”
- Une fois que ce bloc est validé, il devient quasi impossible à modifier/supprimer sans le consensus du réseau
- Possibilité de garder une trace de tout
  - Droits de propriétés, soldes bancaires, ticket de métro etc …
- C’est une nouvelle façon de penser

Ok Comment ça marche ?

Fonctionnement global d’une blockchain

Registre distribué = Registre simultanément enregistré et synchronisé sur un réseau d’ordinateurs (P2P)

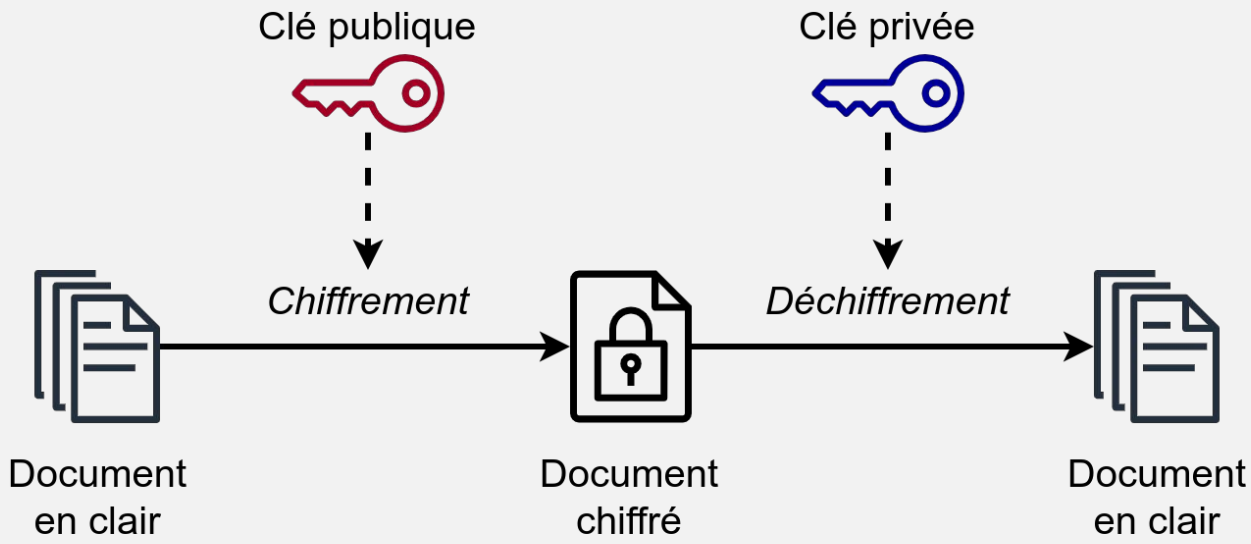
Blockchain = une base de données où chaque ligne ne peut jamais être modifiée, réplication sur des milliers de serveurs indépendants.



Fonctionnement global d'une blockchain

Cryptographie = Discipline de la cryptologie s'attachant à protéger des messages en s'aidant de clés. Assure la confidentialité, l'authenticité et l'intégrité de l'information

Il s'agit d'utiliser des outils mathématiques qui permettent la sécurité et l'immuabilité.



Fonctionnement global d’une blockchain

Blockchain = Registre distribué + cryptographie

Hash = C'est le résultat d'une fonction de hachage, qui est une opération cryptographique qui génère des identifiants uniques et non répétables à partir d'informations données, c’est une **empreinte digitale numérique.**

Noeud = Un ordinateur connecté à la blockchain pour stocker les données, valider les transactions, propager les transactions, assurer sécurité et décentralisation

Fonctionnement global d’une blockchain

Mineur = Un type spécifique de noeud qui se concentre sur la création de nouveaux blocs de transaction en résolvant des problèmes mathématiques complexes. Ils touchent des récompenses.

Tous les mineurs sont des noeuds mais tous les noeuds ne sont pas des mineurs. Les mineurs calculent les clés de hachage.

Chaque bloc contient donc une empreinte numérique unique et l’empreinte du bloc précédent.

Fonctionnement global d’une blockchain

Important

Si quelqu’un tentait de modifier les informations d’un bloc antérieur, le hash changerait invalidant tous les blocs suivant de la chaîne.

Il faudrait ainsi recalculer le hash de ce bloc et de tous les suivants afin d’obtenir le consensus de la majorité du réseau ce qui est pratiquement impossible.

La blockchain appliquée aux cryptomonnaies

Transaction = L'unité fondamentale d'une blockchain de cryptomonnaie est la transaction.

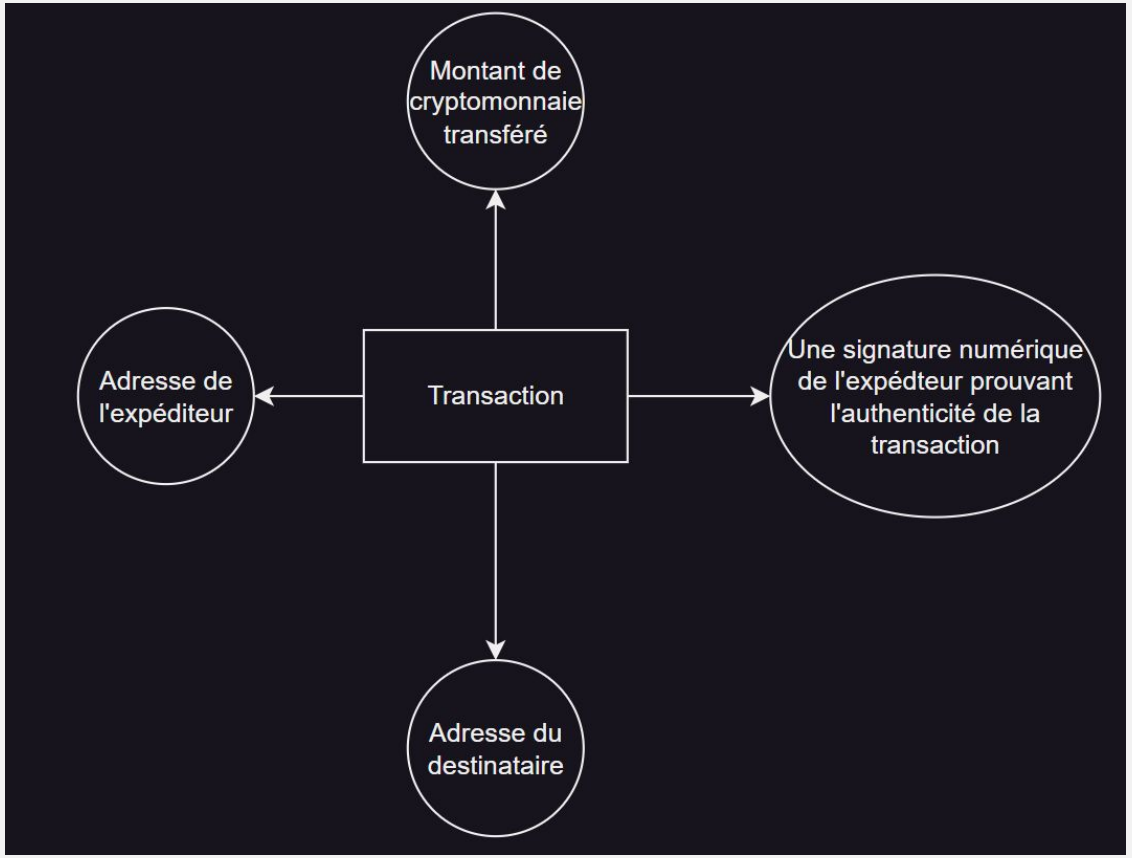
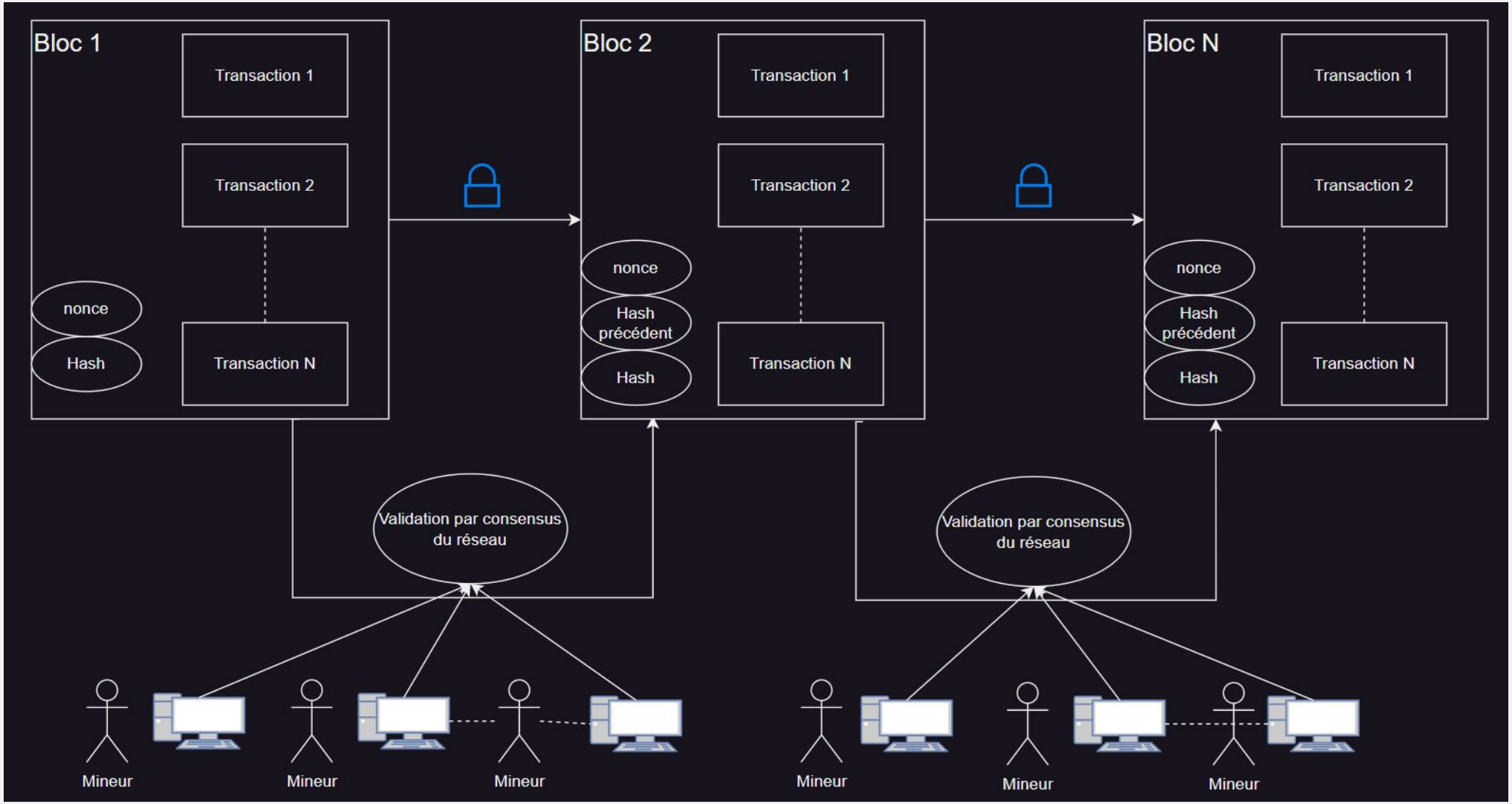


Schéma Blockchain



Les Smart Contracts : Définition

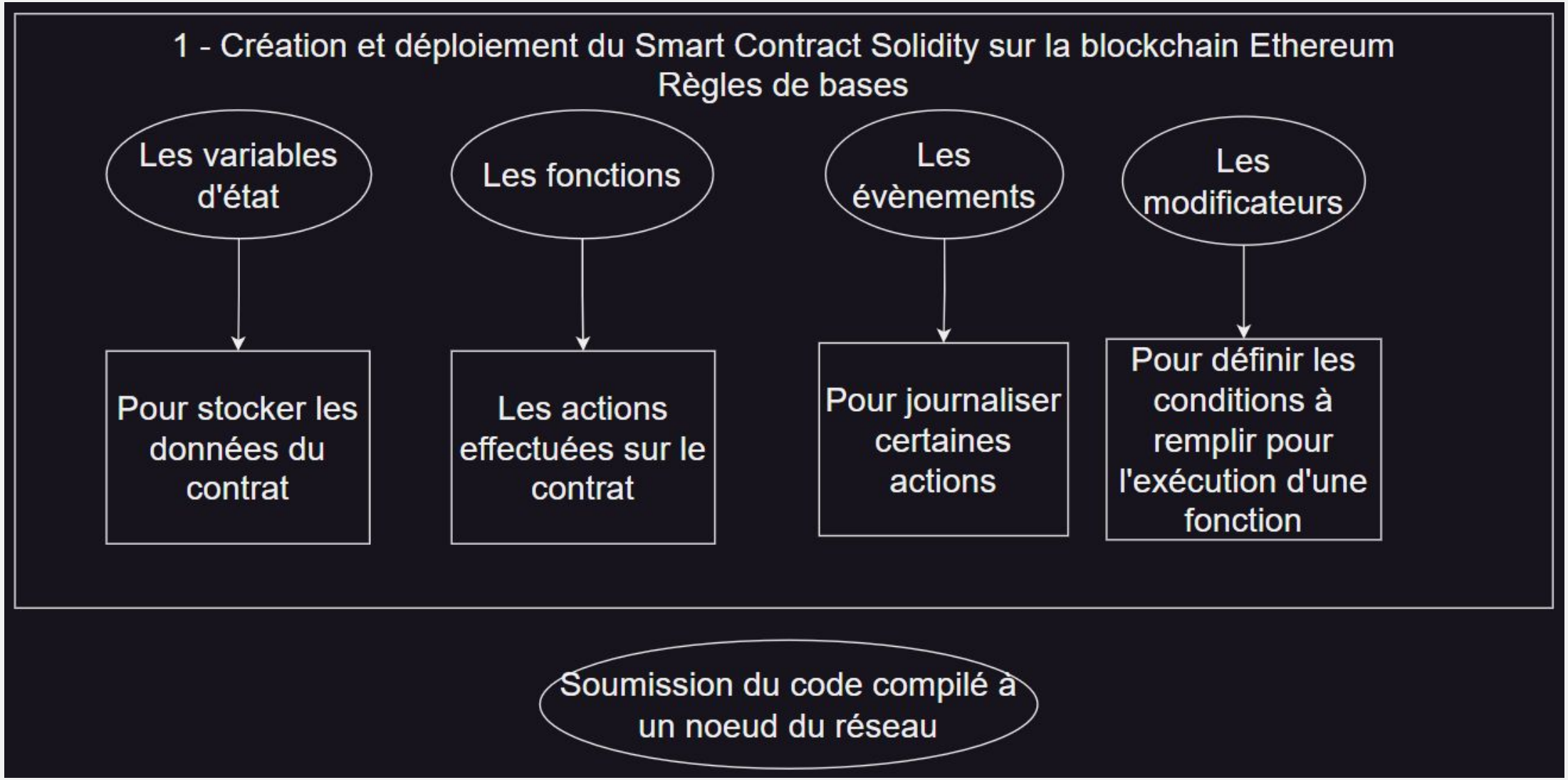
Un smart contract (ou contrat intelligent) est un programme informatique qui s'exécute automatiquement sur la blockchain lorsqu'un ensemble de conditions sont réunies.

Ils reposent sur 5 principes :

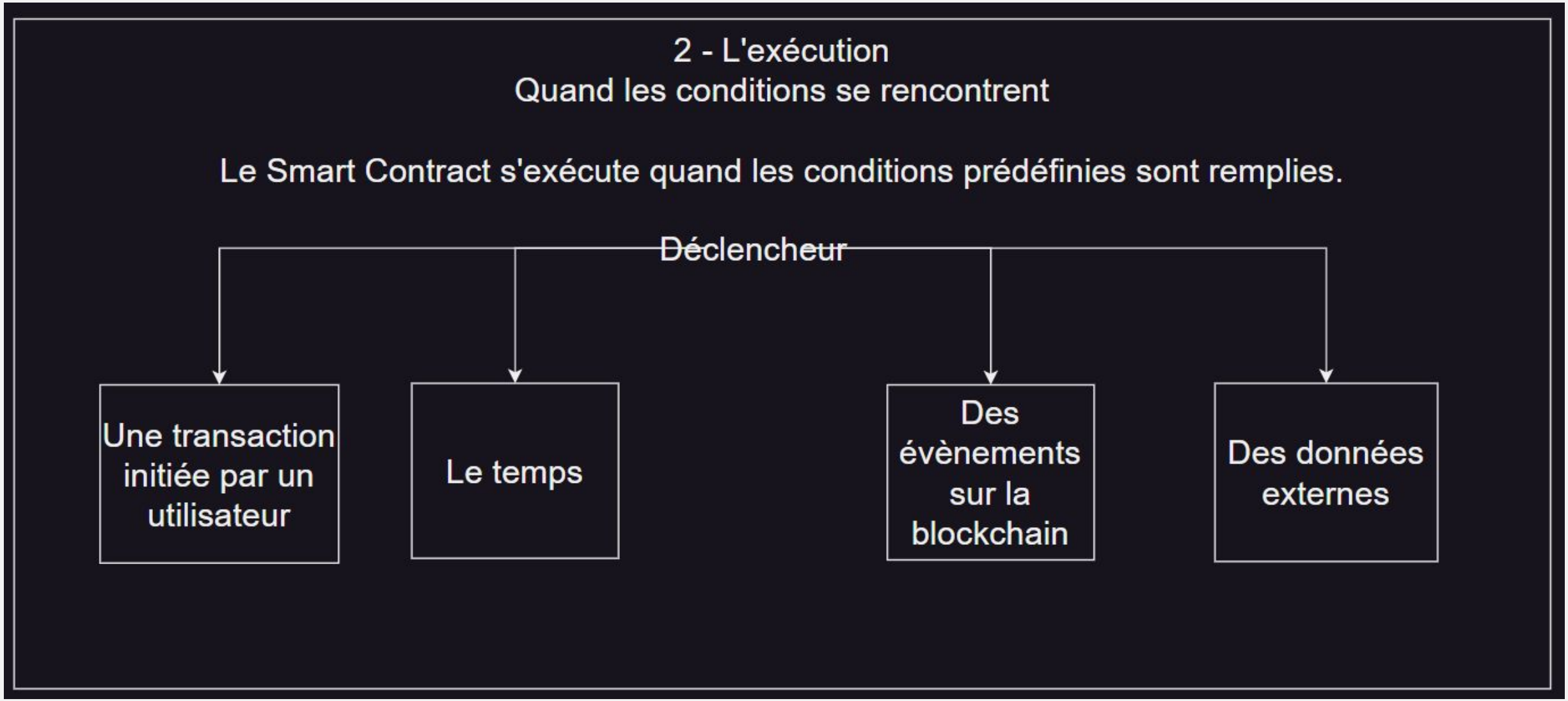
- Autonomie
- Transparence
- Immuabilité
- Sécurité
- Efficacité

Solidity sur Ethereum
Rust sur Solana

Les Smart Contracts : Comment ça marche ?



Les Smart Contracts : Comment ça marche ?



Les Smart Contracts : Comment ça marche ?

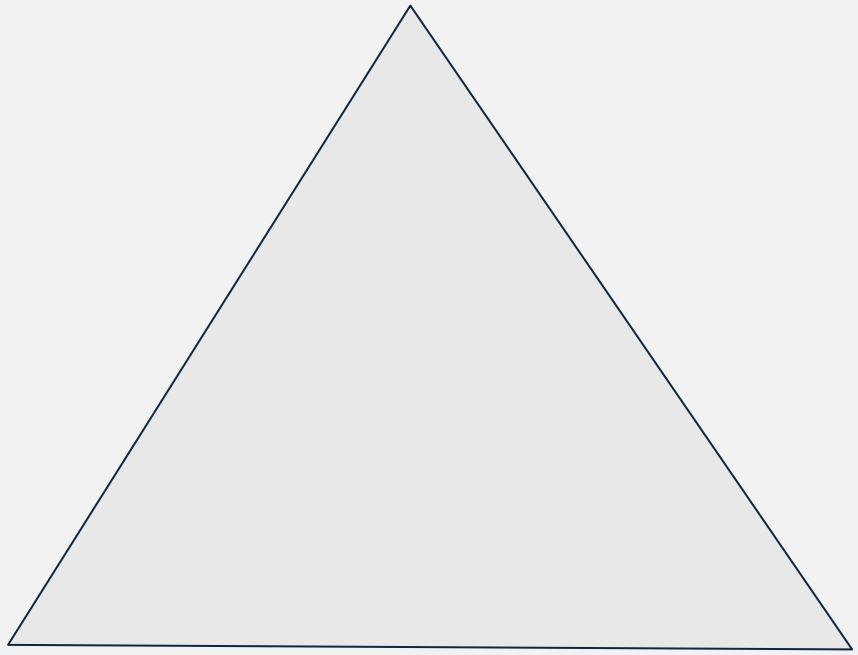
3 - Après l'exécution du code

- L'état du Smart Contract est mis à jour sur la blockchain
- Cette mise à jour est immuable et transparente

Les Smart Contracts : Cas d’usage à imaginer

- Finance
  - Prêt sans intermédiaires bancaires
- Immobilier
  - Achat/vente de propriété directement, sans notaire pour le transfert de fonds
- Logistique et chaîne d’approvisionnement
  - Un Smart Contract pourrait automatiquement déclencher le paiement au transporteur quand le colis arrive à destination, vérifié par des capteurs IoT
- Santé
  - Gérer les données des patients et l’approvisionnement des médicaments via des capteurs IoT
- Education
  - Les diplômes et certifications peuvent être sur la blockchain

Le trilemme de la blockchain



Il est difficile d'optimiser simultanément ces 3 aspects.

Bitcoin privilégie la sécurité et la décentralisation au détriment de la scalabilité.

Ethereum tente de combler les lacunes via le PoS ou sharding par exemple.

Le trilemme de la blockchain : solutions prometteuses

- Le sharding (partitionnement)
  - Diviser la blockchain en plusieurs “morceaux” qui peuvent traiter des transactions en parallèle
- Les “side-chains” (chaînes latérales)
  - Des blockchains séparés qui peuvent interagir avec une chaîne principale
- Les “Layers 2” (solutions de couche 2)
  - Des protocoles construits au dessus de la blockchain principale pour traiter les transactions “off-chain” et n’enregistrer que sur la principale
- De nouveaux mécanismes de consensus différents du PoW
  - Peuvent potentiellement offrir une meilleure scalabilité et sécurité

Web2 vs Web3

Caractéristique	Web2	Web3
Infrastructure	Serveurs centralisés	Blockchain et réseau P2P
Contrôle	Centralisation (entreprises GAFAM)	Décentralisation (utilisateurs et réseaux distribués)
Propriété des données	Données sont sur serveurs Google …	Données stockées sur la blockchain. Elles sont à nous
Modèle économique	Principalement centralisée	Emergence de la tokenisation et des crypto monnaies
Confiance	Confiance nécessaire envers les intermédiaires	Confiance via le code (Smart Contrats) et les mathématiques
Gouvernance	Décision prise par les entreprises	Potentiellement plus communautaire
Identité	Comptes gérées par les plateformes	Portefeuille cryptographique (auto-souveraineté)

Le Bitcoin

- Une crypto monnaie décentralisée => Une monnaie numérique
- Créée en 2008 par Satoshi Nakamoto
- Fonctionne grâce à la technologie Blockchain
- Transactions P2P entre utilisateurs sans intermédiaires

Avantages :

- Sécurité des transactions
- Transparence
- Coûts réduits par rapport aux banques
- Rapidité : Plus rapide que les banques classiques

Le Bitcoin

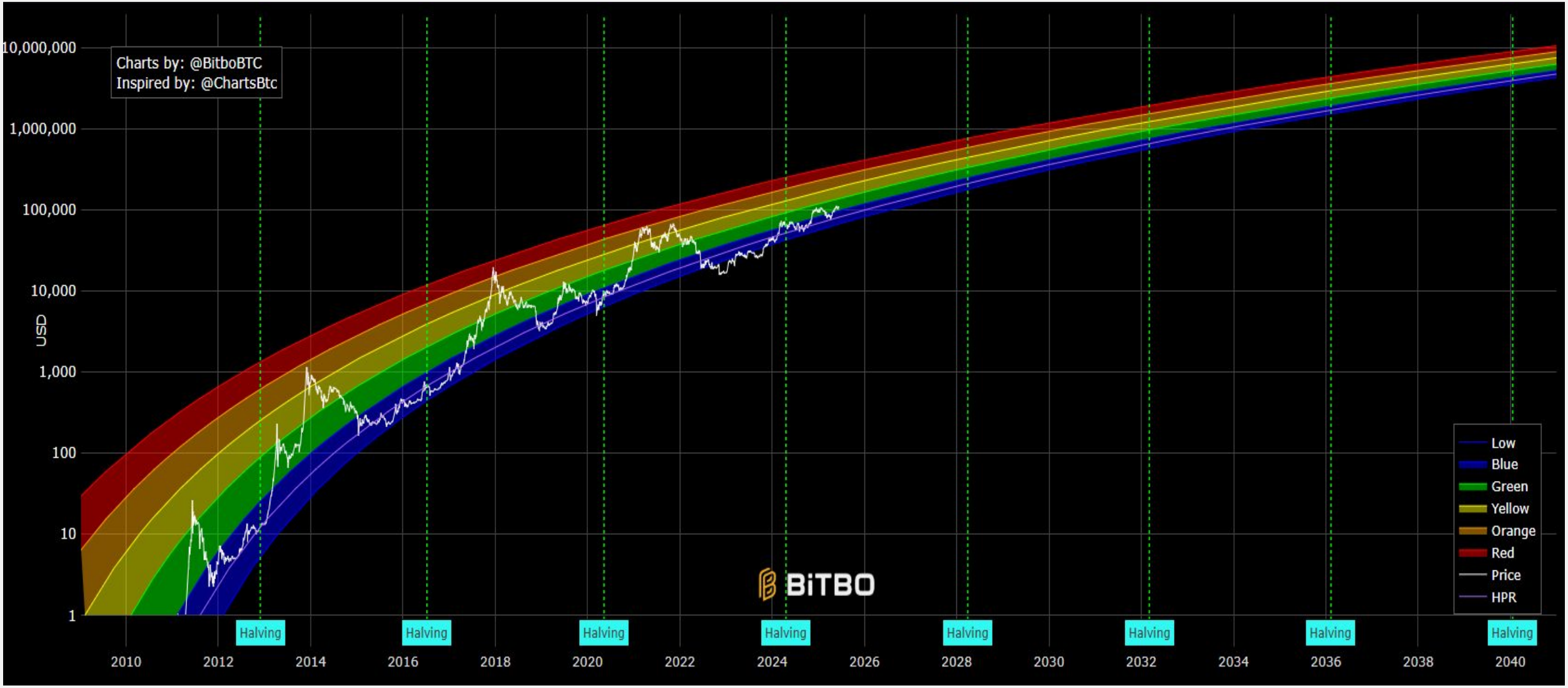
- Rareté : Le nombre de BTC est limité dans le temps => 21 millions.
- Volatilité : Le prix du BTC est connu pour sa forte volatilité
- Cas d’utilisation : C’est une réserve de valeur => L’or numérique

Le halving

- Un événement programmé qui réduit de moitié la récompense accordée aux mineurs de Bitcoin
- Cet événement se produit tous les 4 ans soit environ tous les 210 000 blocs

Année	Nombre de Bitcoin en récompense par blocs
2009	50 Bitcoins
novembre 2012	25 Bitcoins
juillet 2016	12.5 Bitcoins
mai 2020	6.25 Bitcoins
avril 2024	3.125 Bitcoins
aux alentours de 2028	1.5625 Bitcoins

Le Bitcoin Rainbow Chart



Les altcoins

- Abréviation pour “alternative coins” désigne toutes les autres crypto monnaies autres que le Bitcoin
- Marché vaste : Plusieurs milliers d’altcoins existent aujourd’hui
- Le but : Proposer des améliorations ou des alternatives au Bitcoin
- Grande diversité technologie
- Grande volatilité
- Innovation énorme !

Caractéristiques

- De nombreuses techniques
  - Mécanisme de consensus
    - Proof-of-Work (PoW) => Le mécanisme du Bitcoin
      - *Tous les participants du réseau se mettent d'accord sur la validité d'une transaction et l'ajout de nouveaux blocs à la chaîne*
    - Proof-of-Stake (PoS) => Une alternative récente
      - *Les participants (validateurs) sont choisis pour créer le prochain bloc en fonction de la quantité de crypto immobilisée*
  - Algorithmes de hachage
    - Différents SHA-256 utilisé par Bitcoin
- Utilité d'un token : Sa valeur est liée à son utilité
- En constante évolution : Il reste pleins de possibilité

Catégories d’altcoins

- Alternatives à Bitcoin (Ethereum, Solana, Cardano)
- Stockage et partage de fichiers décentralisés : FileCoin
- Réseaux sociaux
- Finance décentralisée (DeFi) : Uniswap, Aave
- None Fungible Token (NFT) : Flow, Mana
- Stables coins : USDT, USDC
- Memecoins : DogeCoin, PEPE
- IA/ Big Data : GRT, TAO, FET

Risques et opportunités des altcoins

- Opportunités
  - Potentiel de croissance élevé
  - Innovation
  - Diversification

- Risques
  - Volatilité élevée
  - Risque dans le projet
  - Complexité
  - Réglementation incertaine

Cryptomonnaies et Finance Réelle : Des Ponts en Construction

- **Stablecoins : Le maillon indispensable**
  - Cryptomonnaies conçues pour maintenir une valeur stable avec un actif du monde réel
  - C’est le pont entre les fiat et les cryptos
- **Adoption institutionnelle et produits financiers**
  - Investissements traditionnels dans la crypto (ETFs, produits dérivés)
  - Intégration par les entreprises (Tesla, MicroStrategy)
  - En développement dans les banques et institutions financières
- **Finance décentralisée (DeFi) vs finance centralisée (TradFi)**
  - La Defi propose des services financiers sans passer par les banques
  - La finance traditionnelle est obligée d’innover ou de s’y connecter
- **Paiements**
  - Projets de CBDC (Central Bank Crypto Currencies) contrôlés par les banques (Euro numérique)
- **Défis et régulation : Nécessité de régulation**
  - MiCA (Markets in Crypto-Assets) en Europe
  - Des discussions en cours aux Etats-Unis

Conclusion

- Sujet très vaste et passionnant
- Le Web3, c’est probablement notre travail de demain
- Prochaine présentation :
  - Développer une blockchain en Java
  - Rentrer un peu plus dans le détail de la Blockchain d’un point de vue technique
  - Montrer à quoi ressemble un SmartContract et le déployer sur le réseau testnet d’Ethereum

Merci pour votre attention

N'hésitez pas à revenir vers moi si vous avez des questions ou des idées, je suis ouvert à la discussion.
En cas de problèmes ou questions :

s.debras@audensiel.fr

AUDENSIEL

audensiel.com