RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Les cryptoactifs

Technologies de registre distribué et actifs numériques

Les Blockchains

Définition

Les blocks et le chainage (algorythme de hachage)

Différents types de blockchains – Preuves différentes de validations / minage

Les différents usages des blockchains

Les cryptomonnaies et les jetons

Les cryptomonnaies : les émanations natives de la blockchain

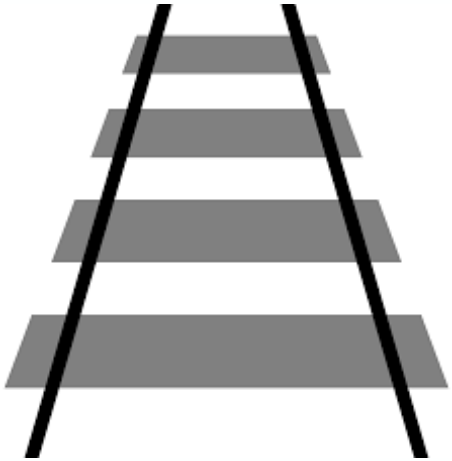
Les jetons / smart contracts : des projets et monnaies créés sur une blockchain préexistante.

Les différents usages : DeFi, smartcontracts,

1ère partie – Les blockchains

Une blockchain c'est :

Un réseau

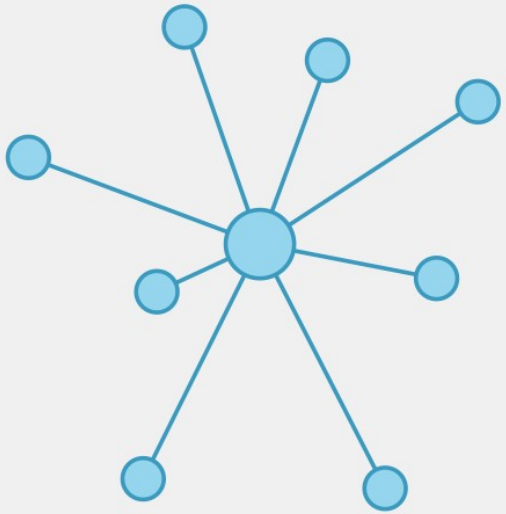


Un registre

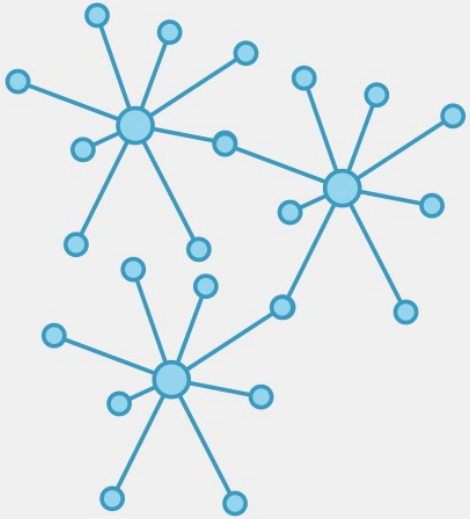
Une monnaie

Vers des registres comptables distribués

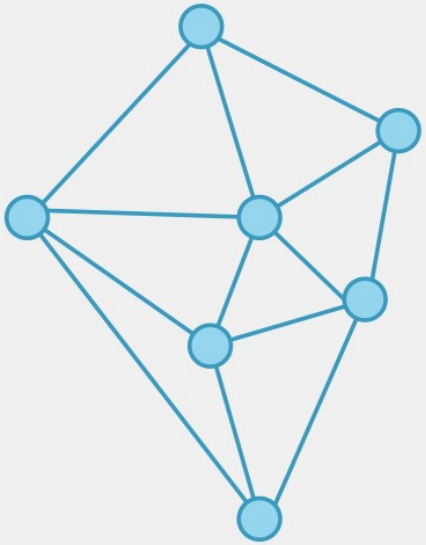
Centralisé



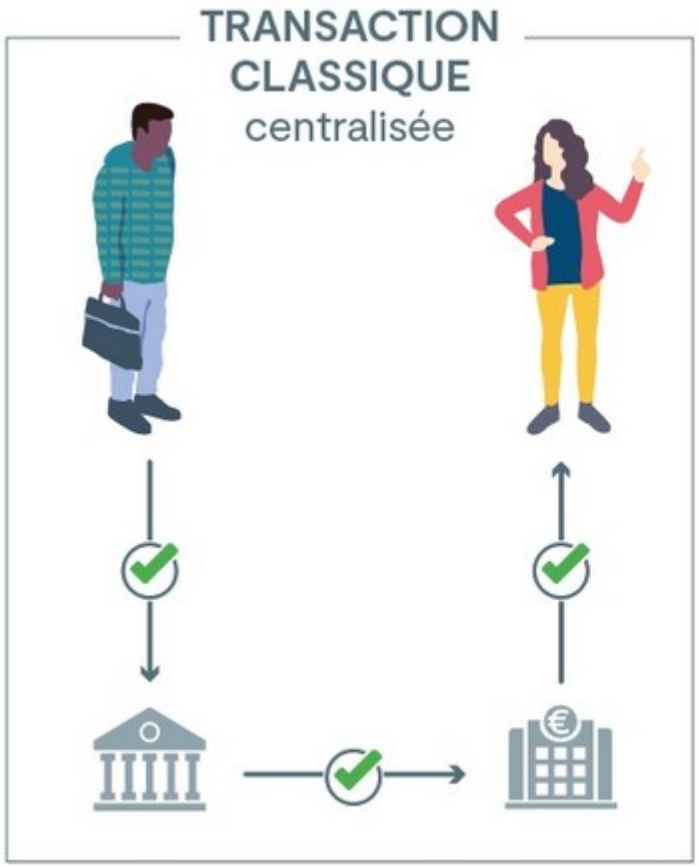
Décentralisé



Distribué



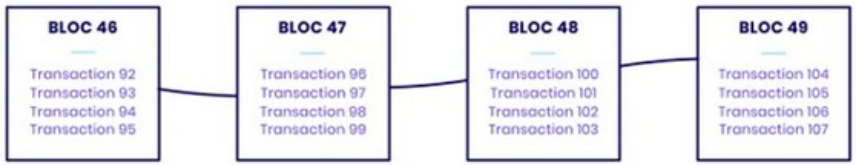
Avec de nouveaux schémas de transaction



©MEF

Comment fonctionnent les blocs d'une chaîne de blocs

Chaque bloc successif contient un ensemble de transactions qui se sont conclues dans le temps



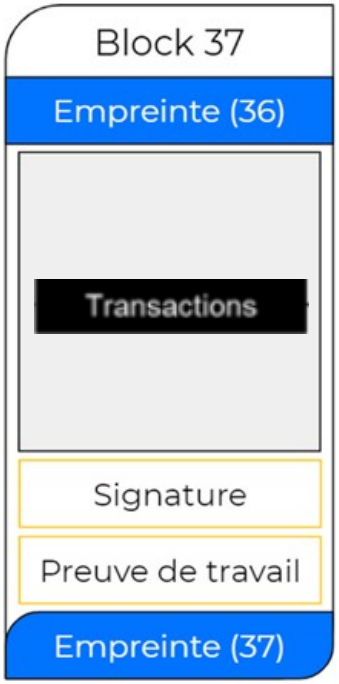
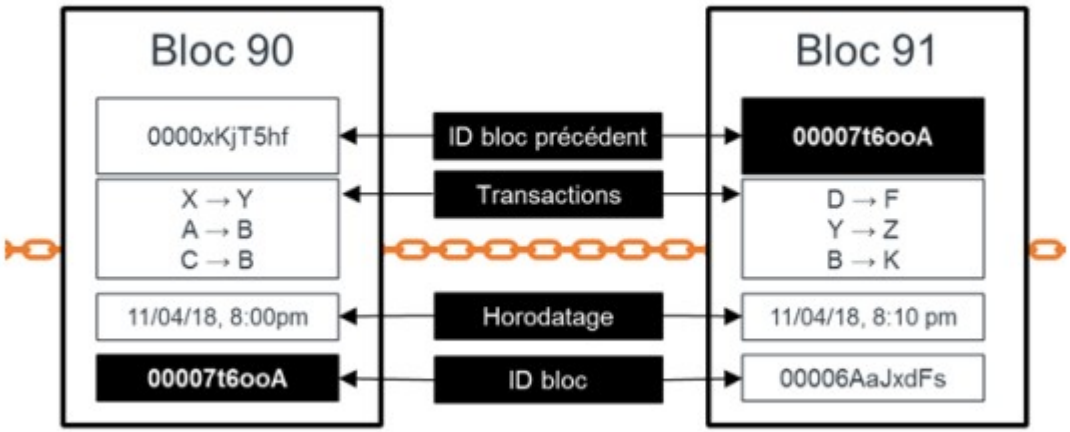


Fig.1 : Architecture simplifiée d'un block Bitcoin

Un bloc est aussi constitué de l'empreinte du bloc précédent, et de celle du suivant. Cette empreinte est aussi appelée « HASH ».

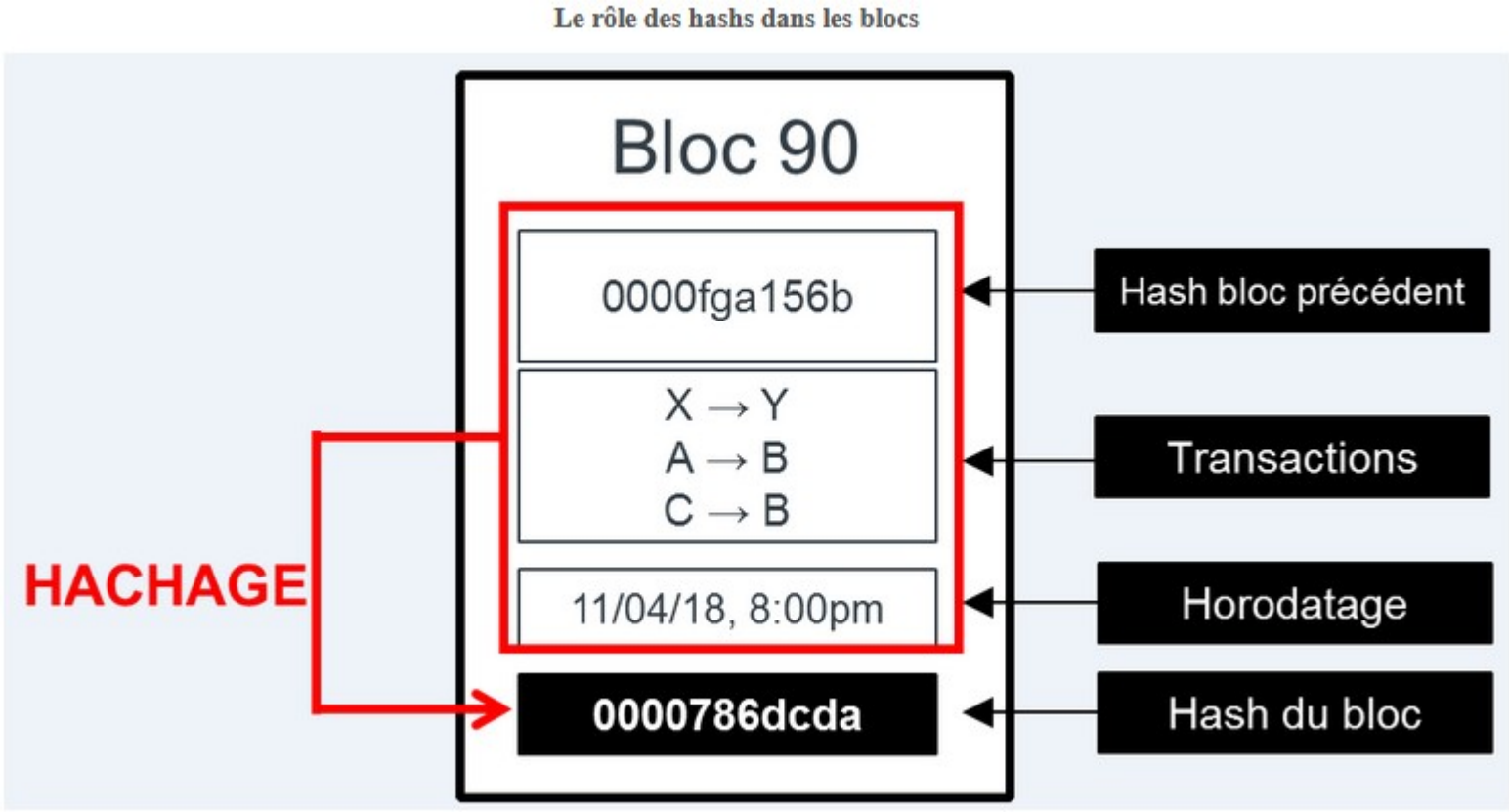
La fonction de hachage (Hash)

La structure d'une *blockchain* et le rôle des hashs

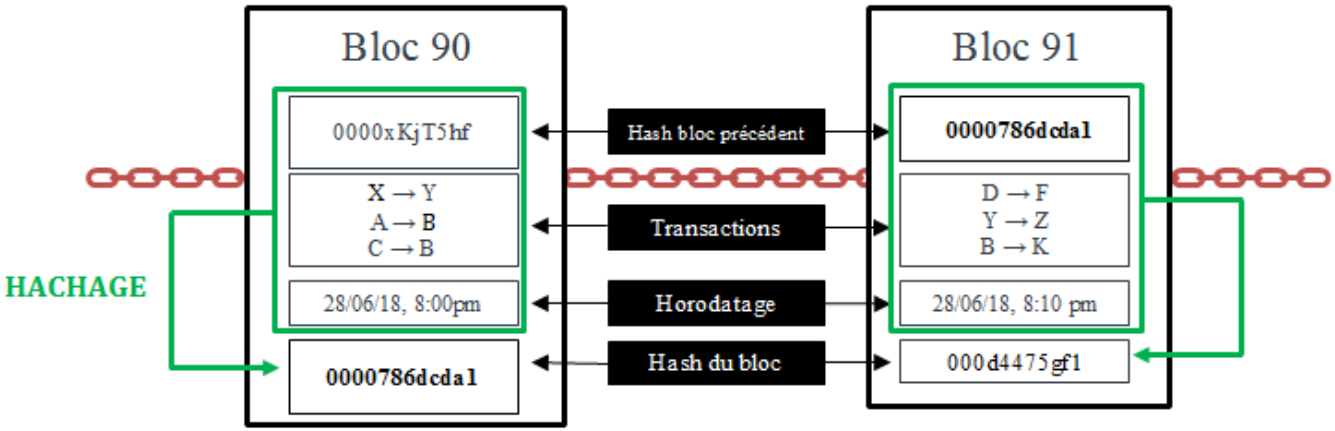


Source : Blockchain France

Dans le cas d'une chaîne de bloc, le hachage est effectué à partir du contenu du bloc, c'est-à-dire le hash du bloc précédent + un certain nombre de transactions + un horodatage = impossible de modifier le contenu d'un bloc



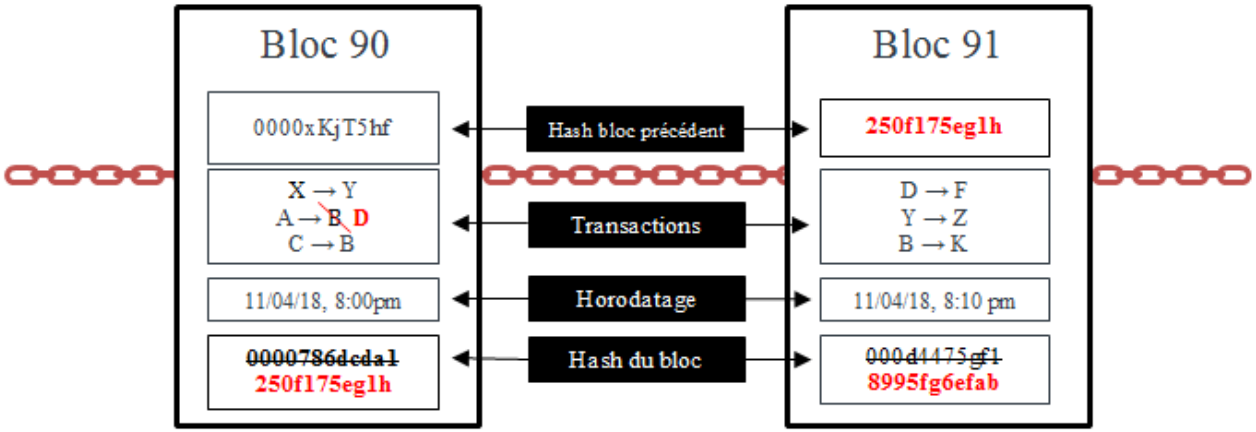
1. Les blocs sont liés par leurs hashs :



Le contenu d'un bloc est soumis à une fonction de hachage pour obtenir son hash (unique et imprédictible)

Ce hash est intégré au bloc suivant, il sera ensuite soumis à une fonction de hachage avec le contenu de ce nouveau bloc pour obtenir un nouveau hash

2. La modification éventuelle d'un bloc est répercutée sur les suivants :



Une **modification du bloc** (ici, le destinataire B remplacé par D) se traduit par un *hash* sensiblement différent

Le *hash* du bloc précédent étant modifié, **le *hash* du bloc suivant est différent** lui aussi, ainsi que le bloc suivant, etc...

Juste pour le plaisir (et la compréhension) : Exemple de cryptographie SHA-256 (Secure Hash Algorithm de 256 bits)

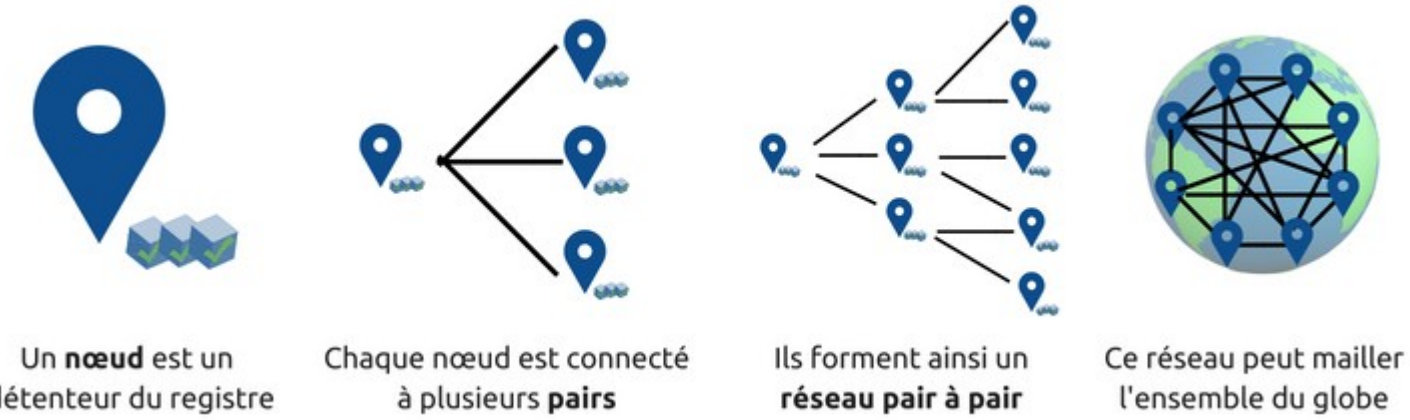
Binaire	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Hexadécimal	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

Le texte de la Constitution française comporte un préambule et un premier article hors titre, suivis de 16 titres (dont un, le Titre XI, possède un titre bis), réunissant en tout **108 articles**

En base Hexadécimale :

5c905f2f9ad289a5f6f2ecf695de23afd11c0cb5909dc5e55d429c28bf52ebc1

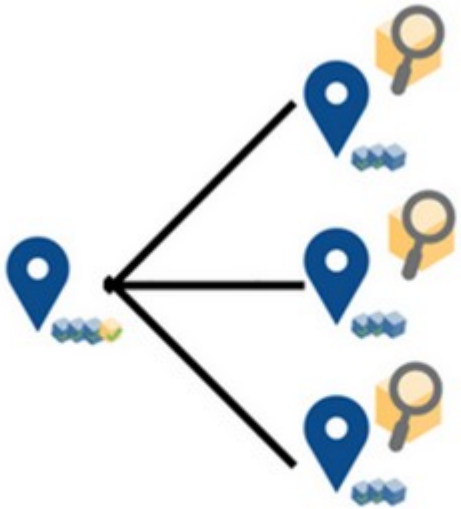
Composition structurelle du réseau



N’importe qui peut être nœud d’un réseau, il suffit de posséder un ordinateur

Diffusion d’un bloc dans le réseau

Quand un nœud crée **un bloc**, il l'ajoute à son registre et l'envoie à ses pairs

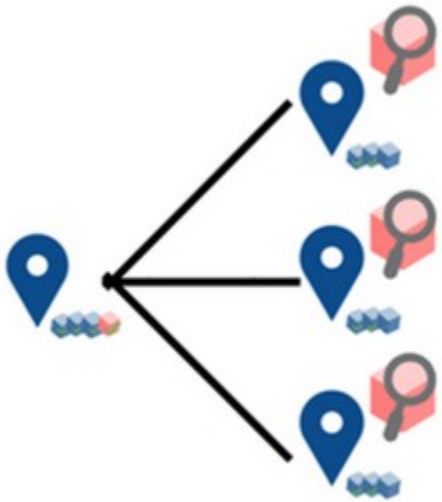


Ceux-ci vérifient alors sa **validité**

S'il est valide, ils l'**ajoutent** à leur registre et l'**envoient** à leurs pairs

Introduction d’un bloc invalide

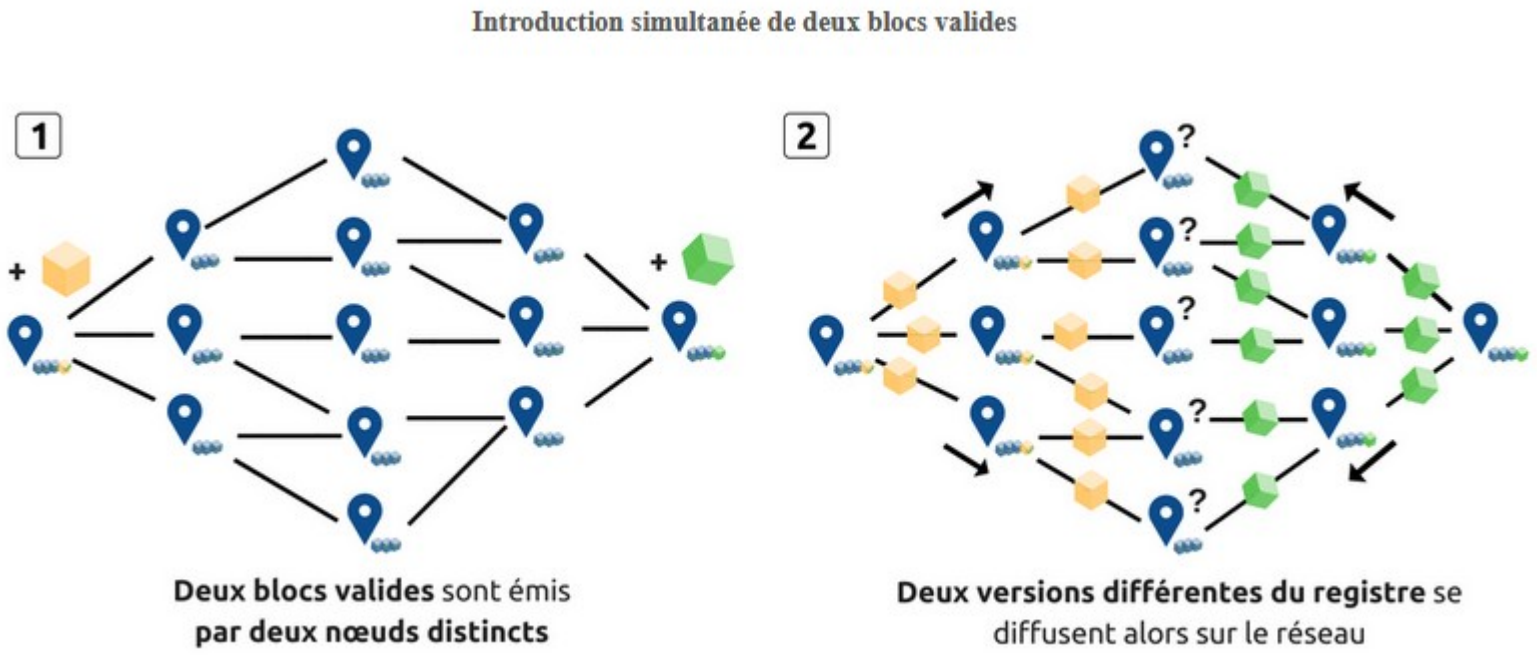
Si un nœud crée un
bloc invalide



Les nœuds identifient
la fraude

Ils ne l'ajoutent pas à leur
registre et ne le diffusent pas

METHODES DE CONSENSUS



Il est nécessaire que les nœuds s'accordent sur le prochain bloc à ajouter à la chaîne, c'est pourquoi les protocoles de blockchains prévoient une « méthode de consensus »

METHODES DE CONSENSUS

- empêcher ou rendre difficile la prise en main de la création des blocs par une seule entité ;

- permettre une temporisation dans la création des blocs, afin que l'ensemble des nœuds du réseau puissent mettre à jour leur registre.

⇒ La PREUVE DE TRAVAIL (Proof of work ou POW) : des épreuves cryptographiques dénommées « minage » (ex Bitcoin)

Dans le cas du bitcoin, le mode de validation est une compétition cryptographique appelée « preuve de travail ».

Celle-ci suppose la réussite d'un utilisateur appelé « mineur » à une épreuve cryptographique, dénommée « minage », qui se répète en moyenne toutes les dix minutes pour le bitcoin. Les mineurs remportent les nouveaux bitcoins créés lors de chaque validation de bloc.

La création de chaque bloc conduit à l'émission de nouveaux bitcoins, utilisés pour récompenser chaque mineur validant un bloc.

Le montant de cette récompense est divisé par deux tous les 210 000 blocs, c'est-à-dire tous les quatre ans. Il était ainsi de 50 bitcoins jusqu'en 2012, puis de 25 jusqu'en 2016, puis de 12,5 jusqu'en 2020. Il est aujourd'hui de 6,25 et passera à 3,12 en 2024. Cette réduction progressive du niveau d'émission de nouveaux bitcoins est appelée « halving ».

Elle a pour objectif de maintenir une certaine rareté de cette monnaie.

Le bloc validé par le mineur qui sort victorieux des épreuves cryptographiques est alors transmis de pair à pair à chaque nœud qui ajoute à sa propre blockchain le bloc ainsi validé.

METHODES DE CONSENSUS

METHODES DE CONSENSUS

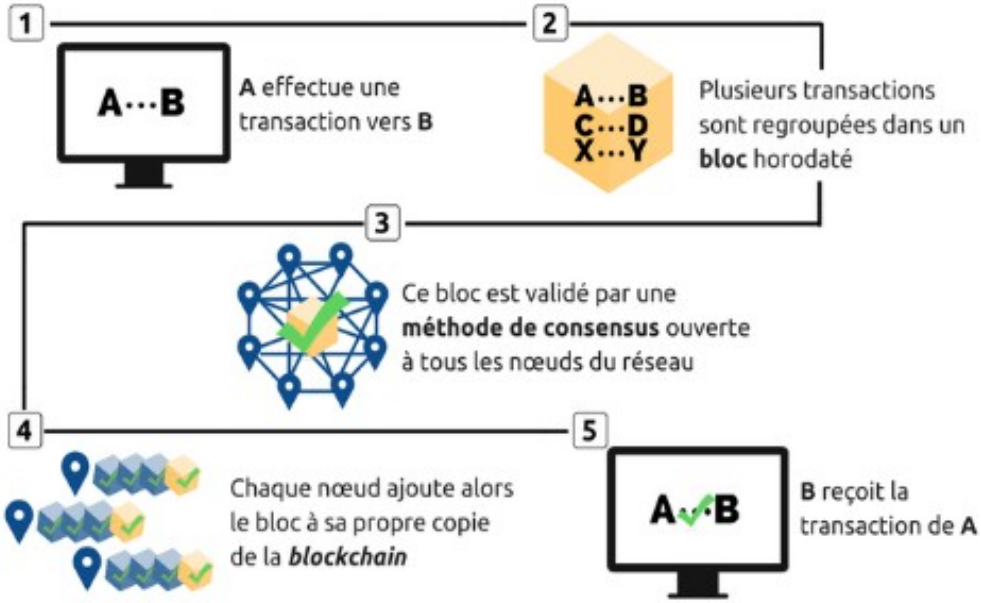
⇒ **La PREUVE D'ENJEU** (Proof of Stake ou POS) (ex Cardano) est composée en réalité de deux preuves :

- la preuve de participation, qui consiste à attribuer les blocs en fonction de la quantité de cryptomonnaies possédée par un nœud,
- la preuve d'enjeu, en tant que telle, qui exige de mettre en gage ces monnaies, qui seront détruites en cas de fraude.

⇒ Les dérivés :

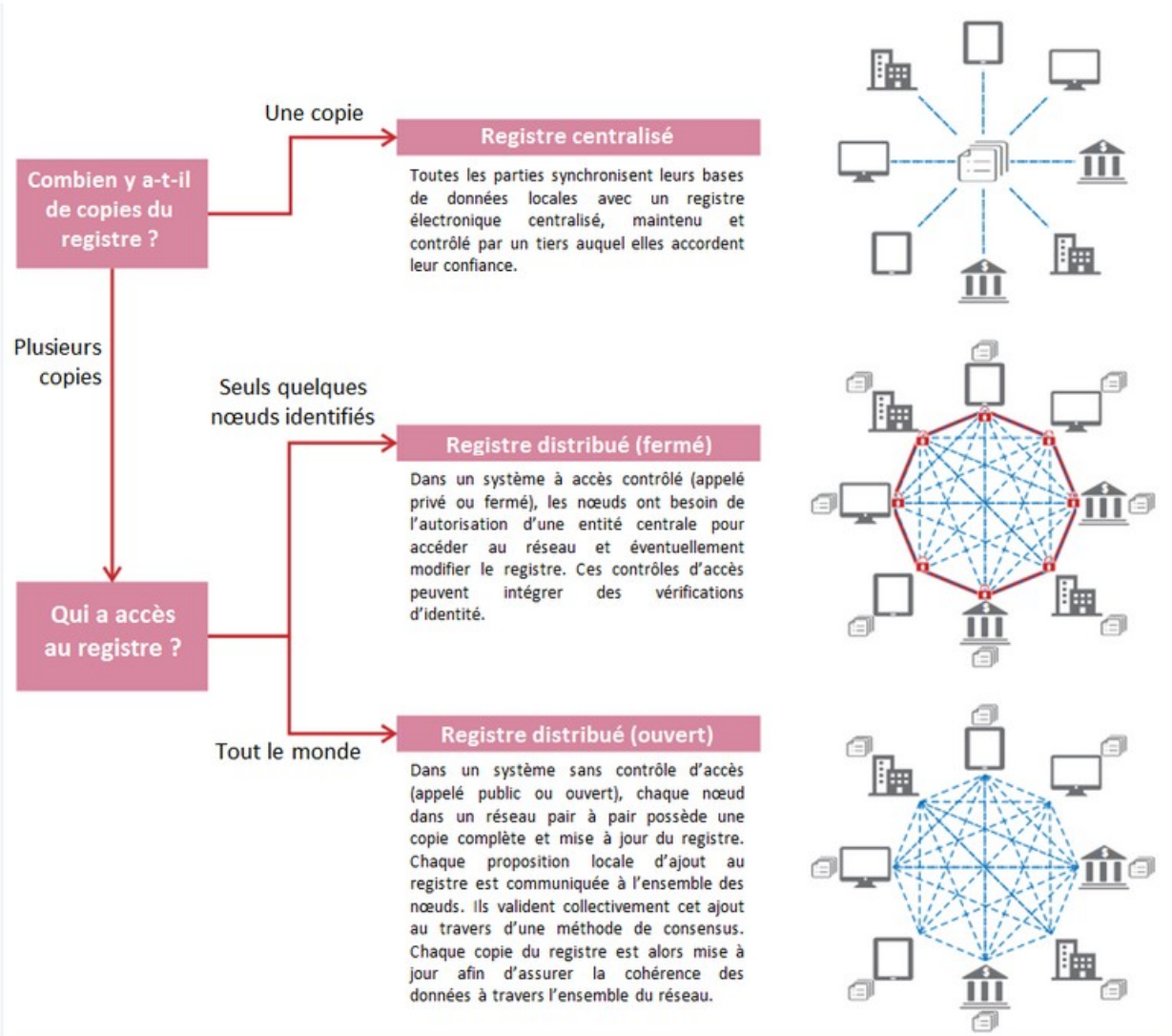
- Preuve de possession
- Preuve d'utilisation
- Preuve d'importance, etc..

EXEMPLE D'ENREGISTREMENT D'UNE TRANSACTION SUR UNE *BLOCKCHAIN*



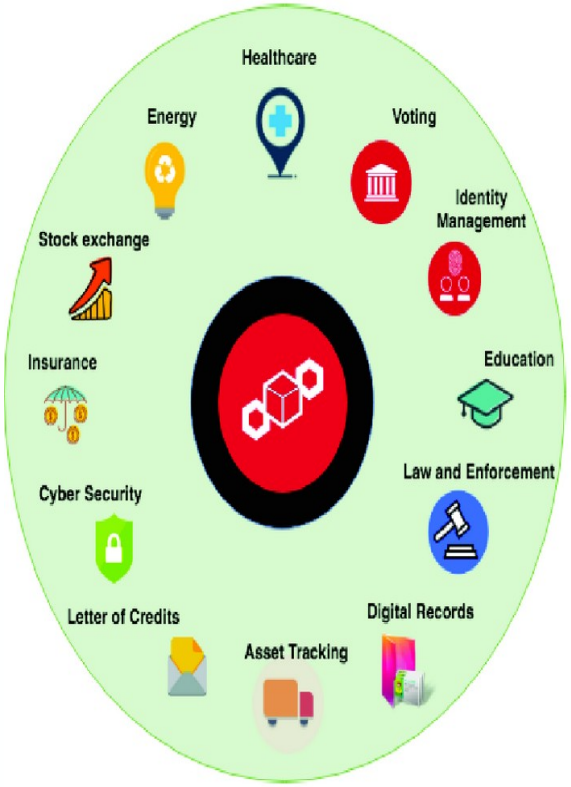
Source : Office parlementaire des choix scientifiques et technologiques

Différents types de registres selon leur caractère centralisé ou distribué et leur caractère ouvert ou fermé



Source : OPECST d'après le chapitre « Cryptocurrencies : looking beyond the hype » du rapport annuel 2018 de la Banque des règlements internationaux, et la note de la Banque mondiale « Distributed ledger technology and blockchain » par H.Natarajan, S.Krause and H.Gradstein, 2017

LES DIVERSES APPLICATIONS POUR LES BLOCKCHAINS



BANQUE

ASSURANCE

LOGISTIQUE

AGROALIMENTAIRE

SANTE

ENERGIE

LUXE

IMMOBILIER

2ème partie – Les Actifs numériques

Les cryptomonnaies

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies · Exchanges · Watchlist — USD · Next 100 → · View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$70 892 320 402	$4 026,25	$8 920 566 862	17 607 537 BTC	0,05%	
2	Ethereum	$14 500 945 335	$137,62	$4 047 164 482	105 369 501 ETH	0,03%	
3	XRP	$12 915 694 924	$0,309982	$592 675 739	41 666 017 553 XRP *	-0,56%	
4	Litecoin	$3 670 345 971	$60,14	$2 100 620 197	61 025 011 LTC	-1,25%	
5	EOS	$3 309 395 828	$3,65	$1 360 086 902	906 245 118 EOS *	-0,60%	
6	Bitcoin Cash	$2 934 619 929	$165,89	$420 936 441	17 689 838 BCH	0,25%	
7	Binance Coin	$2 432 734 466	$17,23	$294 003 391	141 175 490 BNB *	13,67%	
8	Stellar	$2 051 269 047	$0,106696	$213 218 409	19 225 307 319 XLM *	-1,09%	
9	Tether	$2 037 274 702	$1,01	$7 425 032 648	2 020 708 392 USDT *	0,03%	
10	Cardano	$1 611 982 034	$0,062174	$127 923 898	25 927 070 538 ADA	3,83%	

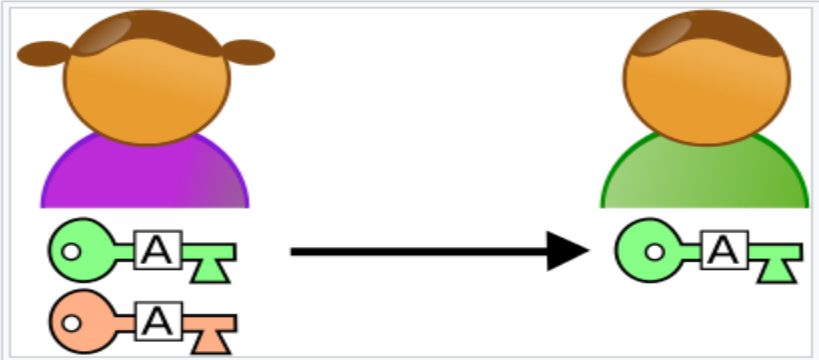
TOP 5 des Crypto Monnaies Prometteuses 2022

- **Dogecoin** – Le cours du Dogecoin a enregistré une très forte hausse depuis plusieurs mois
- **Safemoon** – Cette crypto est l'une de celles qui attirent le plus les investisseurs actuellement
- **Shiba Inu** – Une crypto monnaie récente et particulièrement prometteuse avec une hausse de 10 000%
- **Uniswap** – Cette crypto devise commence à voir son cours monter en 2021
- **Pancake Swap** – Une crypto monnaie prometteuse pour 2022 qui bat des records de transactions

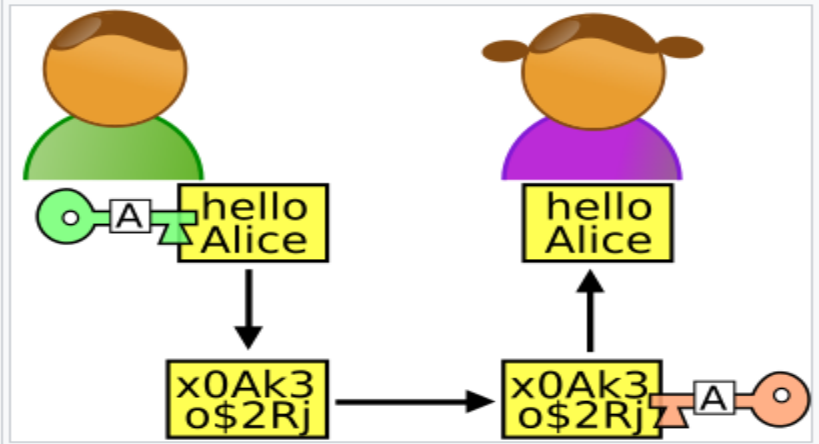
Cryptographie asymétrique

La clef publique d'Alice peut être vue par tous et utilisée par tous pour envoyer un message à Alice.

En revanche, elle seule sera en capacité de lire les messages envoyés grâce à sa clef privée.



1re étape : Alice génère deux clefs: Sa clef publique (verte) qu'elle envoie à Bob et sa clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.



2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

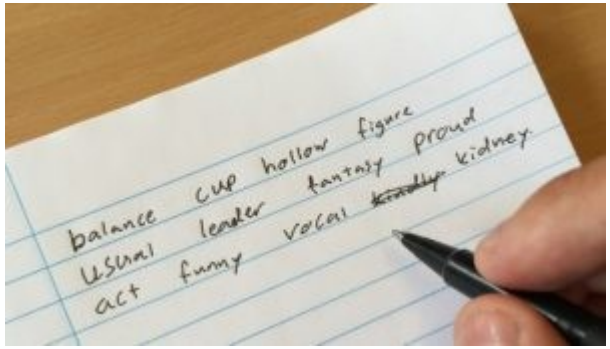
Clefs publiques / clefs privées et la graine...

clé publique

1M3RLrXve5wcT2ZcJu8WXoXjdh4WXcWQA9

clé privée

5K8BwE76VsatQiRa5wJpGng7758FAz4vLkMxAry8QnyZTdQJxPn



La graine (seed)

STOCKAGE DES ACTIFS

Il existe deux types de wallets :

- Les wallets dits de stockage à froid ou Cold wallets
- Les wallets dits de stockage à chaud ou Hot wallets

STOCKAGE DES ACTIFS

1 – Portefeuilles Physiques (Hardware wallets)

Les portefeuilles physiques sont des dispositifs qui conservent les cryptos des utilisateurs hors ligne et qui fournissent une sécurité supplémentaire contre les possibilités de piratage.

Avantages

- Très grande sécurité
- Les clés sont stockées hors ligne
- Un grand nombre de cryptomonnaies supportées
- Les transactions sont très rapides

Inconvénients

- Le prix est assez élevé
- Aucune assurance de dépôts
- Le stockage de vos jetons vous incombe

STOCKAGE DES ACTIFS

2 – Hot Wallets (portefeuille en ligne)

Encore appelés *hot wallets*, les **crypto wallet en ligne** nécessitent une connexion internet pour fonctionner. Ils sont disponibles sur PC ou sur les appareilles mobiles et vous permettent de vendre, acheter ou échanger votre monnaie sans difficulté.

Avantages

- Il vous permet d'avoir accès à vos données de n'importe où
- Son utilisation est gratuite
- Aucune installation nécessaire
- Facilité de navigation
- Disponibilité du service client

Inconvénients

- **Sécurité réduite**
- Clés privées gérées par des tiers
- Risques de piratage accru

LES SMART CONTRACTS - TOKEN

- Une **cryptomonnaie** est l'unité de compte d'un registre distribué.
  Elle a son propre protocole. Le symbole du bitcoin est BTC.
  Un bitcoin est divisible : 1 satoshi = 0,00000001 BTC

  Ethereum est la blockchain dominante pour créer des *applications décentralisées*, à travers le standard ERC20 (pour *« Ethereum Request for Comment*, un type de *smart contract*.

- Un **token** est un jeton numérique personnalisé qui utilise le registre d'une cryptomonnaie. Elle représente un droit d'usage, un droit d'auteur, un droit d'utilisation d'un service, une identité, un droit de vote, une certification.. Elle permet aussi de lever des fonds via des *Initial Coin Offering*.

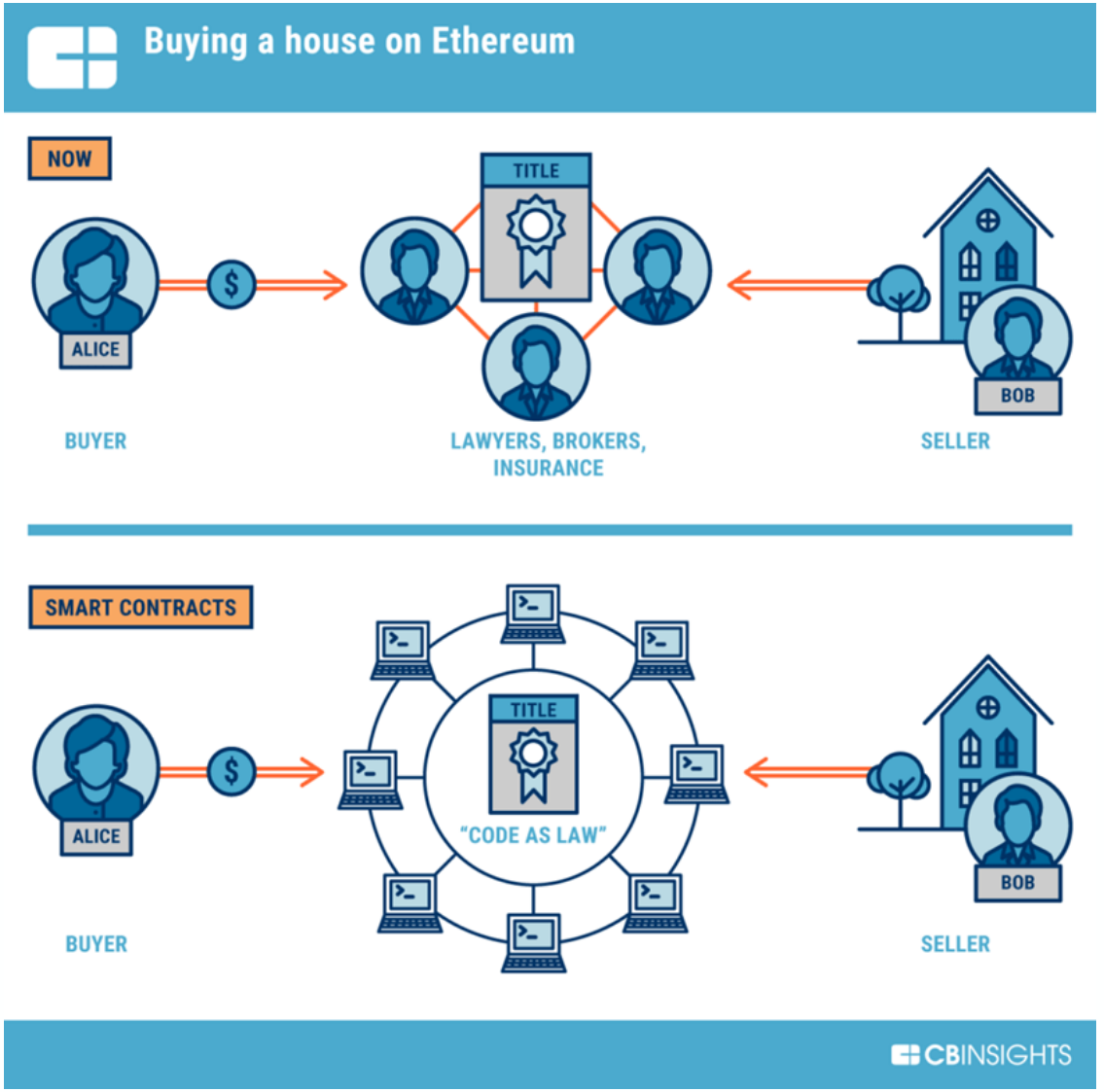
- Un ***smart contract*** est un logiciel qui automatise une transaction si une condition est réalisée : 30 jours sont passés (paiement), un train est en retard (indemnité), un loyer n'a pas été perçu (pénalité), etc...

Les smarts contracts

Les contrats intelligents, sont des programmes informatiques, déployés sur une blockchain, qui exécutent un ensemble d'instructions lorsqu'une ou plusieurs conditions sont réalisées.

Avantages : sécuriser l'accord (immutabilité), automatiser le paiement, éliminer les intermédiaires

Inconvénients : risque de faille, l'immutabilité de la blockchain ne permet pas de corriger des erreurs



LES NFT

Les Jetons non fongibles (NFT)

Les jetons non fongibles (NFT) aussi appelés *nifties* présentent des caractéristiques communes à celles d'un jeton classique :

- nativement numérique
- peuvent s'échanger sur la blockchain
- conservés dans un portefeuilles d'actif numérique

Mais chaque unité d'une masse donnée de NFT ne peut être divisée et ne peut être distinguées des autres en raison des caractéristiques propres

1  = 1  mais  ≠ 

Les NFT s'appliquent dans le domaine de l'art, des objets de collection, des jeux vidéos, etc...

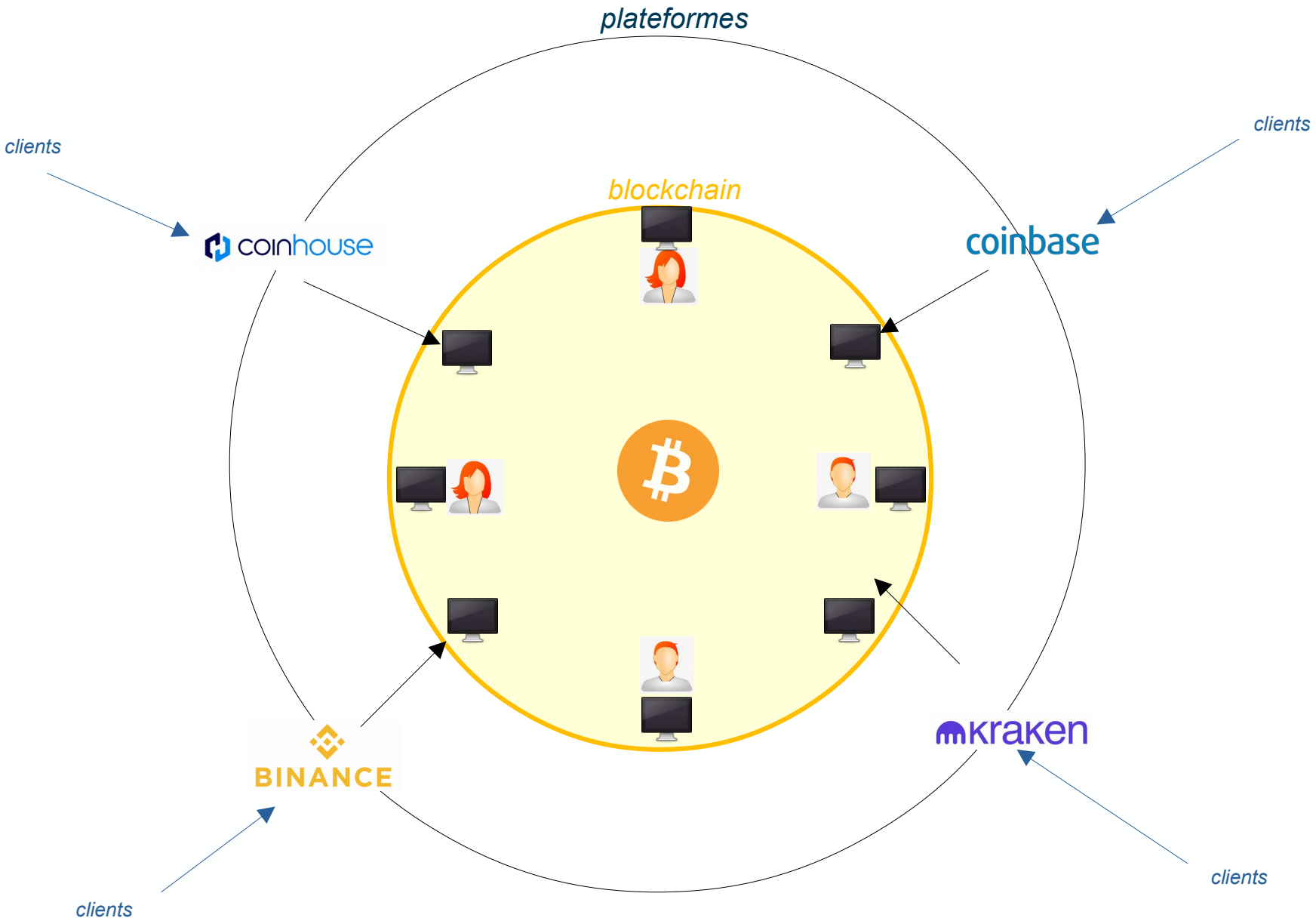
Comment acquérir des actifs numériques :

- Sur des places de marchés (*exchanges*) : centralisées (CEX) ou décentralisées (DEX)
- Par la vente de particulier à particulier (exemple : *localbitcoin*)
- Par le minage
- Par le vol
- Par la vente de biens ou de services
- Via un distributeur de cryptomonnaies

Les prestataires de service sur actifs numériques (PSAN)

- Agrément obligatoire ou optionnel selon l'activité suite à la loi PACTE
- **Agrément obligatoire** pour les activités de conservation d'actif numérique et achats/ventes d'actifs numériques contre une monnaie ayant cours légal ou contre un actif numérique, et exploitation d'une plateforme de négoce d'actifs numériques.
- Leur équivalent mondial est le **Virtual Asset Service Provider (VASP)**

Ne pas confondre plateforme et Blockchain



La finance décentralisée (DeFi)

Ensemble de services financiers réalisés sur la blockchain, dont la fourniture comme l'utilisation est ouverte à tous, sans passer par des intermédiaires classiques.

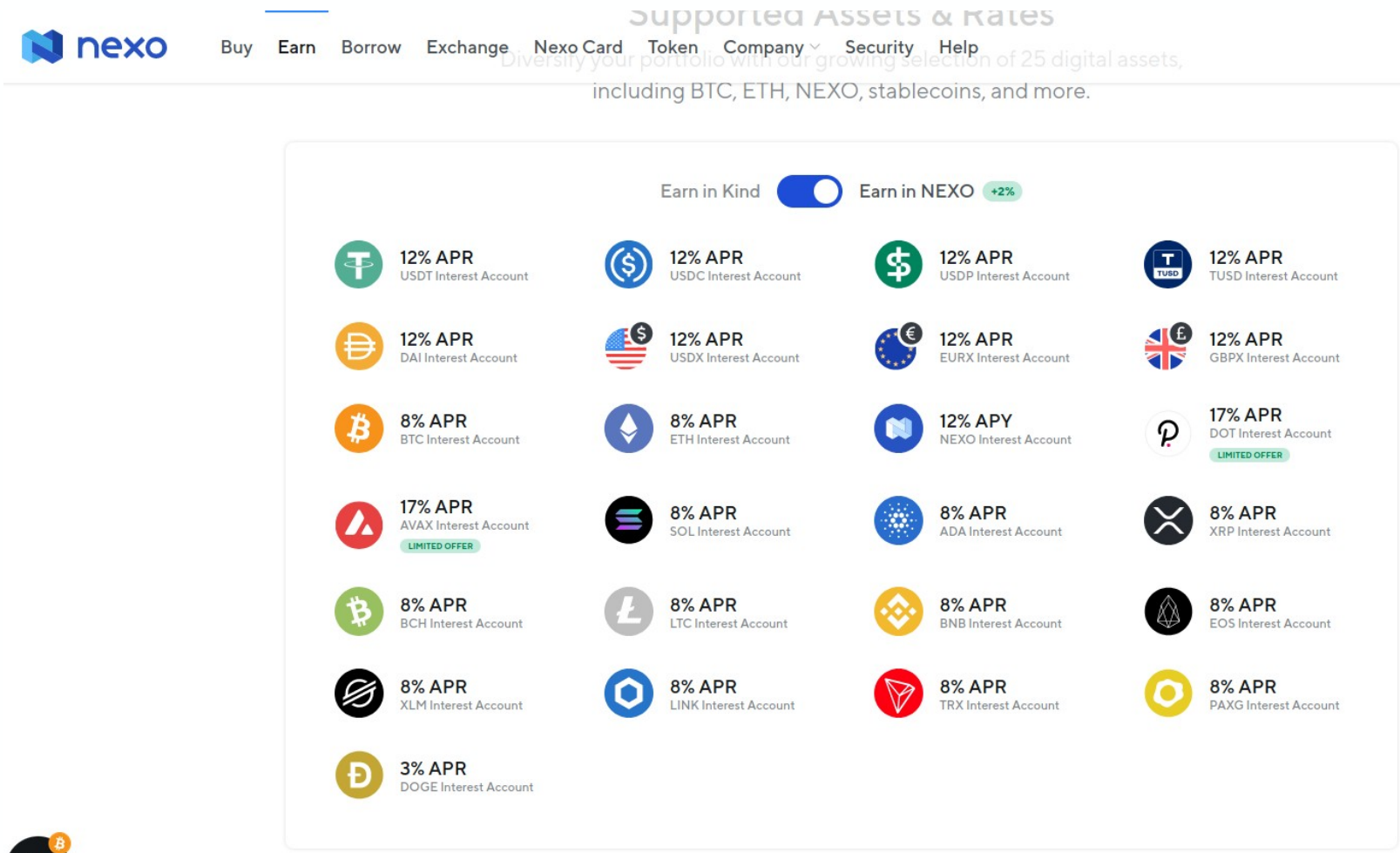
Exemples : prêt ou emprunt, pari sur la valeur d'un actif synthétique

Les rendements sont supérieurs à ceux obtenus dans la finance traditionnelle

Exemples :

- prêt d'actifs numériques (apport en tant que collatéral) pour obtenir des stablecoins
- prêt de stablecoins pour obtenir des rendements intéressants
- participation à des pools de liquidité sur des échanges décentralisées

Un exemple de rendement (DeFi)




Merci pour
votre attention