

A grayscale photograph of several people, likely in a meeting or office setting, looking towards the left. The image is partially obscured by a blue geometric overlay on the right side.

Introduction au monde des crypto monnaies



SCUB^{scub.net}

Stéphane Traumat

Fondateur de **Oak Invest**, une holding qui regroupe plusieurs sociétés :

- **Scub**, une Entreprise de Service Numérique d'environ 100 personnes sur Angoulême, Bordeaux & Niort.

- **SPS**, une solution de gestion de la relation client et de distribution de produits à destination des assureurs et des courtiers.

Je suis aussi associé plus ou moins actif dans différentes structures :

- **Agence 42**, une agence de communication.
- **Thanks For Leads**, une application qui devrait sortir en 2025.
- **Eldo**, une société qui fournit des outils de communication aux métiers du bâtiment.
- **Isia**, une société qui fournit une IA privée pour exploiter les documents de l'entreprise.
- **50 Partners**, un fond d'investissement dédié aux startups cryptos.

- Enfin, je suis développeur / Contributeur sur des projets Open Source comme Mogami, Royllo, Cassandra trading bot ou blockchain2graph (<https://github.com/straumat>).



SCAN ME

Scub

- ESN basée à Angoulême et Bordeaux.
- A peu près 100 personnes.
- Divers métiers : projet, dev, test, infra, data & conseil.
- Editeur du logiciel SPS, solutions SaaS.
- Très technophiles, très open source.

On recrute ! (stage, alternance, emploi)

Contactez nous ! recrutement@scub.net





Intro

Les concepts de base

Assets

Les différents types
d'actifs

Defi

Les possibilités de la
finance décentralisée

DAO

Les possibilités des
organisations distribuées



Intro

Les concepts de base

Assets

Les différents types
d'actifs

Defi

Les possibilités de la
finance décentralisée

DAO

Les possibilités des
organisations distribuées



Blockchain 101

Deux mots sur la philosophie...

Le crypto-anarchisme est une idéologie qui prône l'utilisation de la cryptographie et des technologies décentralisées pour créer un ordre social et politique à l'abri de la surveillance et du contrôle des gouvernements.



Blockchain 101

La promesse du blockchain

La **blockchain** est une **technologie** qui permet de **gérer un registre infalsifiable sans organe central de contrôle.**

Elle permet de réaliser des transactions sans avoir à passer par des intermédiaires.

Blockchain 101

Une citation de Milton Friedman

“Une chose qui manque est un système de paiement sécurisé qui permettra de transférer des fonds d’une personne A à une personne B sans qu’ils se connaissent. De la même façon que je vous tends un billet de 20\$”

C’est exactement ça, Bitcoin est une sorte de porte monnaie avec un système de téléportation.



Les promesses du Bitcoin

- Première devise monétaire électronique décentralisée.
- Une politique monétaire connue et immuable.
- Transactions quasi instantanées de personnes à personnes.
- Pas de notions de pays, de conditions préalables ou de limites arbitraires.
- Votre “compte” ne peut être bloqué ou confisqué.
- Relatif Anonymat.

Notre scénario

L'entreprise **BitcoinDistrib** décide de créer des distributeurs de boissons qui acceptent le bitcoin.

Nous allons voir :

- Comment se créer un “compte” bitcoin.
- Comment acheter ses premiers bitcoins.
- Comment recevoir son premier paiement.



Avant de poursuivre, deux choses à
savoir...



Blockchain 101

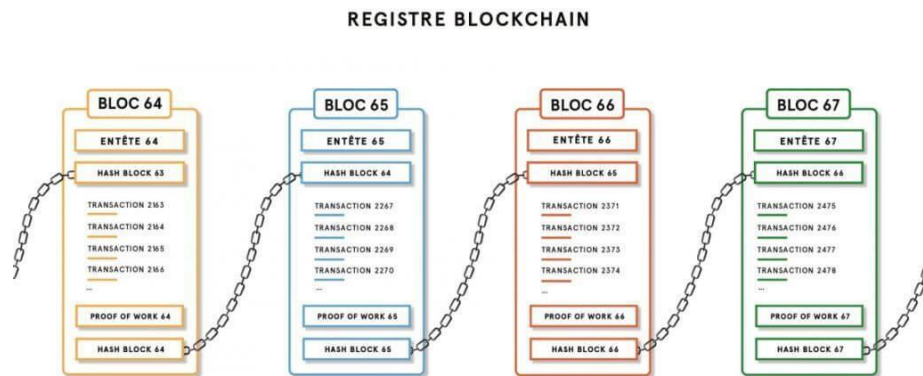
Première chose : Bitcoin fonctionne en P2P

Le réseau Bitcoin est un réseau de machines en peer to peer (P2P), ce qui signifie que toutes les machines qui y participent ne sont pas plus importantes les unes que les autres.

Blockchain 101

Deuxième chose : La blockchain est un livre de compte décentralisé & immuable

On peut simplifier le concept de blockchain à un livre de compte ouvert qui listerait l'ensemble des transactions ayant eu lieu depuis son origine et permettant ainsi à chacun de savoir qui à quoi.



Blockchain 101

Un exemple

Transaction Afficher les informations d'une transaction bitcoin

12af127dbc9f6abb4fc10883f0dde1d775101eebc3e504677aace310422f484c

12AVXnk44KQsZpgWJ4TRyrnR8rX6sbAhdE (1 BTC - Sortie)
1HBJCXhpGtG3B59sfm3bxcYz9Xuo3gZGKr (0.00030819 BTC - Sortie)



1Fe87sAgZAPnU3PbTKD667HZMypzjJ7JEN - (Dépensé)
18Ja7bjLu4t2zRGmiTd3b5xV34vbWpmsUf - (Dépensé)

1 BTC
0.00020819 BTC

1.00020819 BTC

Résumé

Taille	438 (octets)
Heure de réception	2014-12-27 22:22:44
Incluses dans des blocs	336213 (2014-12-27 22:29:16 + 7 minutes)
Confirmations	3284 Confirmations

Entrées et sorties

Apport total	1.00030819 BTC
Sortie totale	1.00020819 BTC
Taxes	0.0001 BTC
BTC estimée négociée	1 BTC



Reprenons

Étape 1 : Se créer un “compte”

La **clé privée** est un nombre choisi au hasard qui vous permet de signer des transactions sur les bitcoins qui vous appartiennent.

Exemple :

91149ee24f1ee9a6f42c3dd64c2287781c8c57a6e8e929c80976e586d5322a3d

La clé privée est un peu comme votre signature sur un chèque.

Blockchain 101

Étape 1 : Se créer un “compte”

La **clé publique** est calculée à partir de la clé privée et elle permet de générer des adresses bitcoin.

Exemple :

```
042c6b7e6da7633c8f226891cc7fa8e5ec84f8eacc792a46786efc869a408d29539a5e6f8de3f71c0014e8e  
a71691c7b41f45c083a074fef7ab5c321753ba2b3fe
```

La clé publique est un peu comme votre numéro de compte.

Étape 1 : Se créer un “compte”

Les **adresses bitcoin** sont des adresses générées qui correspondent à votre clé publique. C'est à ces adresses que l'on peut vous envoyer des bitcoins et vous pouvez en créer autant que vous voulez.

Exemple :

13mtgVARiB1HiRyCHnKti6rEwyje5TYKBW

Les adresses correspondent au champs “à l'ordre de” sur les chèques.

Étape 1 : Se créer un “compte”

La première étape est terminée, trois points importants :

- On a tout ce qu'il faut pour commencer à recevoir et envoyer des bitcoins.
- Tout ceci est géré de manière automatique par les logiciels du marché.
- Si vous perdez la clé privée, vous ne pourrez pas retrouver vos bitcoins.

Blockchain 101

Clé privée =
Clé



Clé publique =
emplacement de la
boîte aux lettres

Étape 2 : On achète des bitcoins

Il existe deux façons d'obtenir des bitcoins :

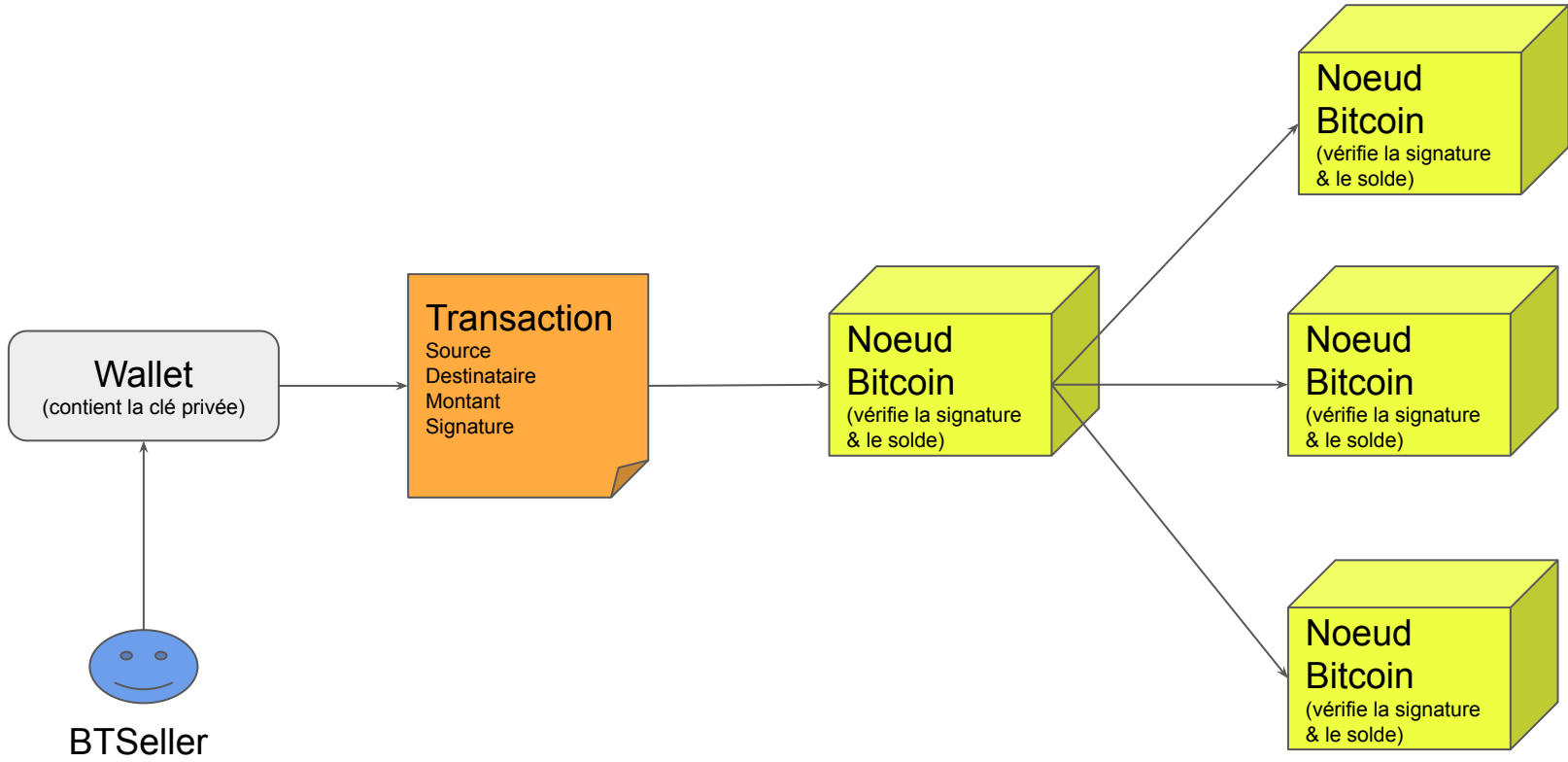
- En fabriquer.
- En obtenir auprès d'un tiers qui en possède.

Étape 2 : On achète des bitcoins

Pour en acheter, BitcoinDistrib va s'adresser à quelqu'un qui en possède et lui donner son adresse bitcoin : 13mtgVARiB1HiRyCHnKti6rEwyje5TYKBW

Il existe plein de vendeurs :

- Coinbase (plateforme en ligne).
- La maison du bitcoin (accueil physique).
- Des connaissances.
- Ou pour notre exemple, une plateforme fictive : BTSeller.

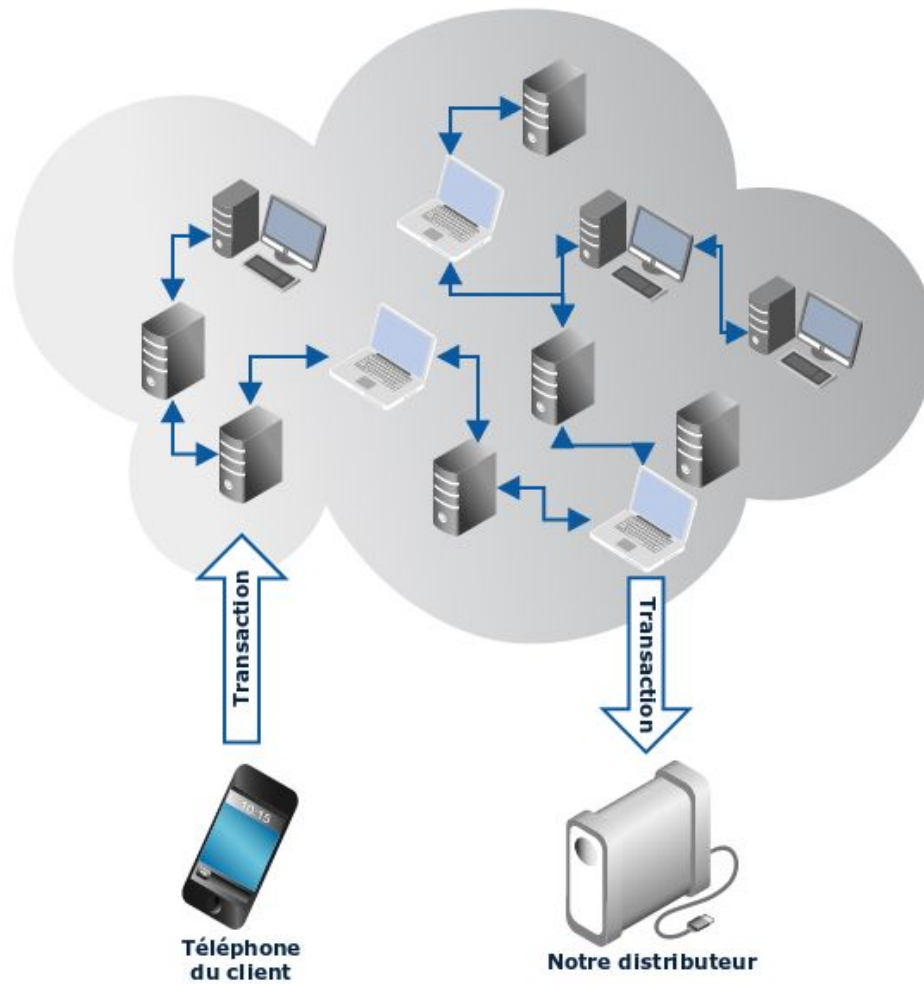


Étape 3 : on reçoit des bitcoins

Pour son distributeur de boisson d'Angoulême, il va créer une adresse bitcoin spécifique.

Il va ensuite encoder cette adresse, avec le montant à régler dans un QRCode qu'il va coller sur la machine.





Quatres points à noter

- Contrairement aux cartes bancaires, ni le vendeur, ni l'acheteur n'ont besoin de fournir des informations confidentielles.
- Les machines du vendeur et de l'acheteur n'ont pas besoin de communiquer directement.
- La transaction ne peut être "interceptée" car modifier la transaction détruirait la signature.
- Tout ce que nous avons vu peut être fait en quelques minutes.



Blockchain 101

Qu'est ce qu'un contrat

Un contrat est un **agrément** entre **plusieurs parties** sur le fait **de faire ou de ne pas faire quelque chose en échange de quelque chose d'autre**.

Chaque partie doit avoir **confiance** dans le fait que chacune des parties va remplir ses obligations.

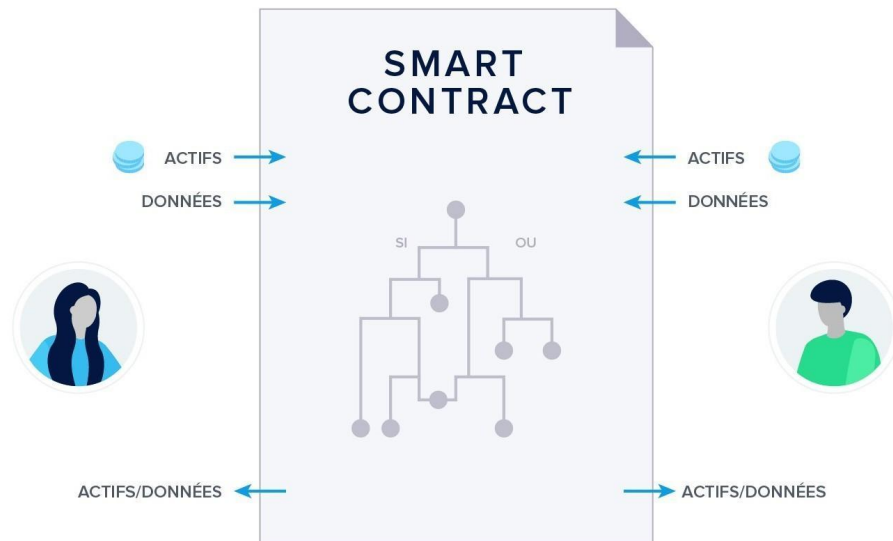
La blockchain permet ce genre d'agrément mais elle **enlève le besoin de confiance entre les parties**.

Blockchain 101

Des contrats autonomes et inarrêtables

Aujourd'hui, les contrats s'exécutent dans des programmes qui se trouvent sur des serveurs centralisés (banques, assurances, mutuelles...). Si un contrat est déployé sur un serveur centralisé, alors une panne, une faillite ou une attaque peuvent bloquer son exécution.

Un smart contract (ou contrat autonome) est un programme qui s'exécute sans qu'un tiers puisse l'empêcher ou le modifier.





Blockchain 101

Comment cela fonctionne-t-il ?

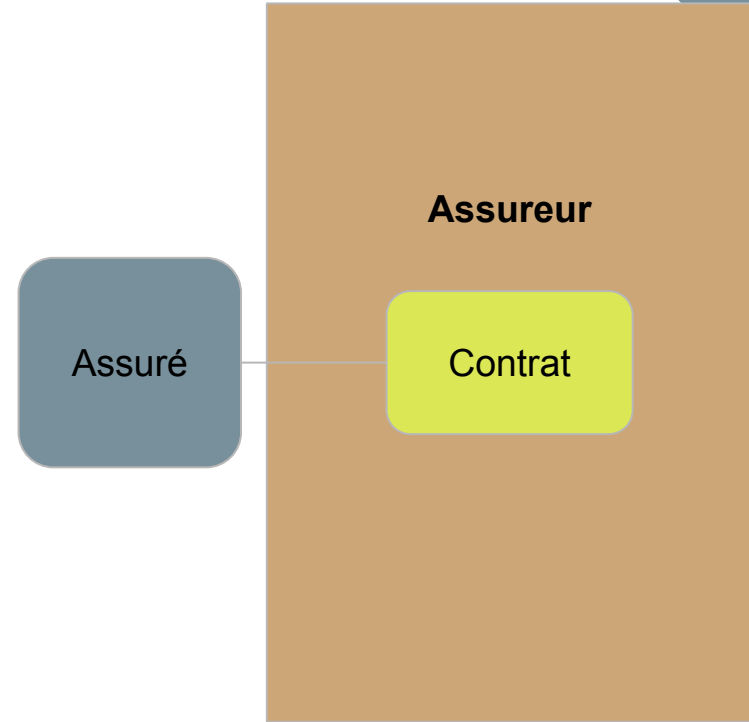
De la même façon que les bitcoins sont “stockés” la blockchain bitcoin, les programmes (contrats) que l’on va écrire vont être stockés sur la blockchain ethereum et ils vont être exécutés son réseau.

Vous pouvez imaginer ethereum comme une sorte d’ordinateur global qui exécutera votre contrat de manière impartiale.

Blockchain 101

Contrat météo

Aujourd'hui : Il va s'adresser à un assureur qui va prendre une commission pour assurer son risque.

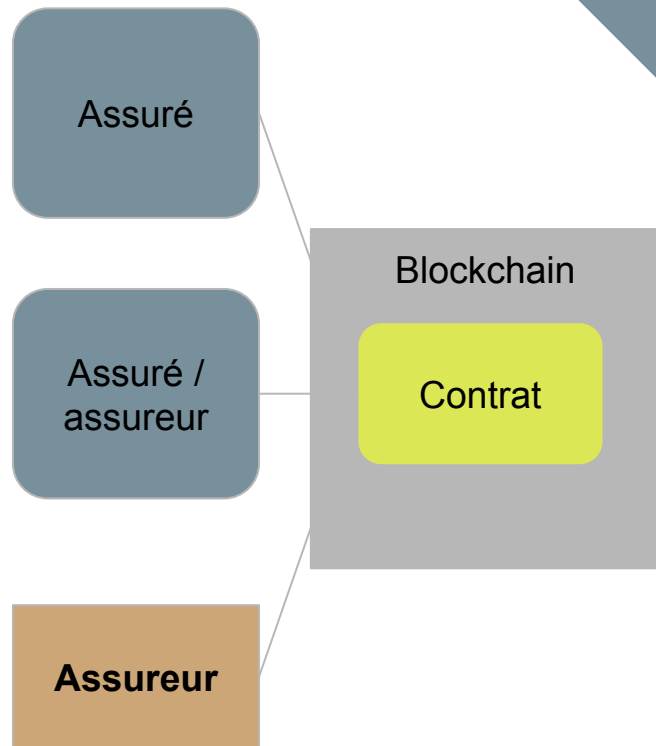


Blockchain 101

Contrat météo

Demain : il va se connecter à une place de marché où il va proposer les termes de son contrat :

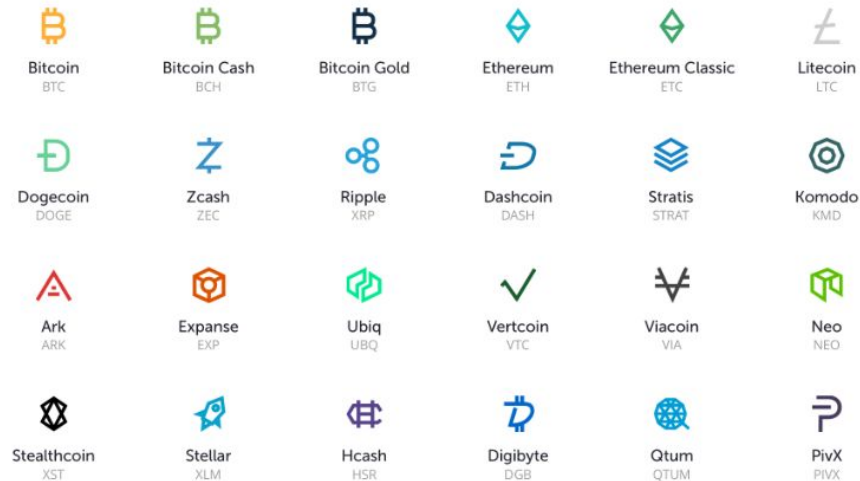
- Je propose de payer une prime de 10 €. S'il pleut moins de 50 centimètres cet été, je veux recevoir un montant de 100 €.
- Les acteurs de la place de marché pourront souscrire à son contrat en versant une fraction de 100 €.
- L'ensemble des montants va être "séquestré" dans le contrat.
- Fin juillet, le contrat va s'exécuter et verser l'argent en fonction du niveau de pluie.



Blockchain 101

Des tonnes de Blockchain !

Il existe énormément de blockchains avec chacune leurs spécificités.



Cela se présente comment ?

L'exemple MetaMask



Blockchain 101

Les Portefeuilles (wallets)

Un wallet est une application qui permet à un utilisateur de gérer ses fonds en gérant : stockage des clés privées, vérification des fonds sur la blockchain, création et signature de transaction.

Une des plus connues est MetaMask.



METAMASK

Features ▾

Support ▾

About ▾

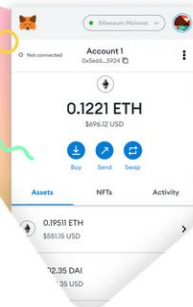
Build ▾

Download

A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 30 million users worldwide.

Download for 



Blockchain 101

MetaMask installé

Metamask est un simple plugin qui s'installe dans votre navigateur.

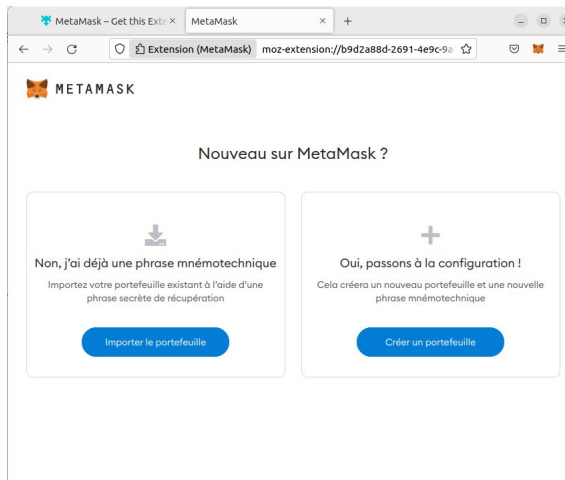


Blockchain 101

Initialisation de votre portefeuille

Dans le monde crypto, l'idée d'avoir un compte (email, mot de passe, adresse...) est vu comme quelque chose d'inacceptable.

A l'installation, soit vous pouvez importer un "portefeuille existant" ou en "créer un"

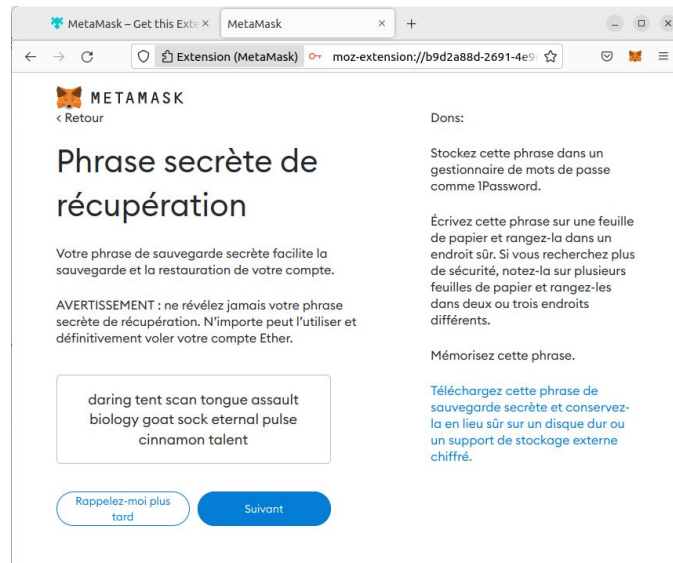


Blockchain 101

Portefeuille créé

Il s'agit d'un portefeuille déterministe : toutes les clés privées sont dérivées à partir d'une clé privée "maître" (appelée seed) et peuvent donc être retrouvées à partir de celle-ci .

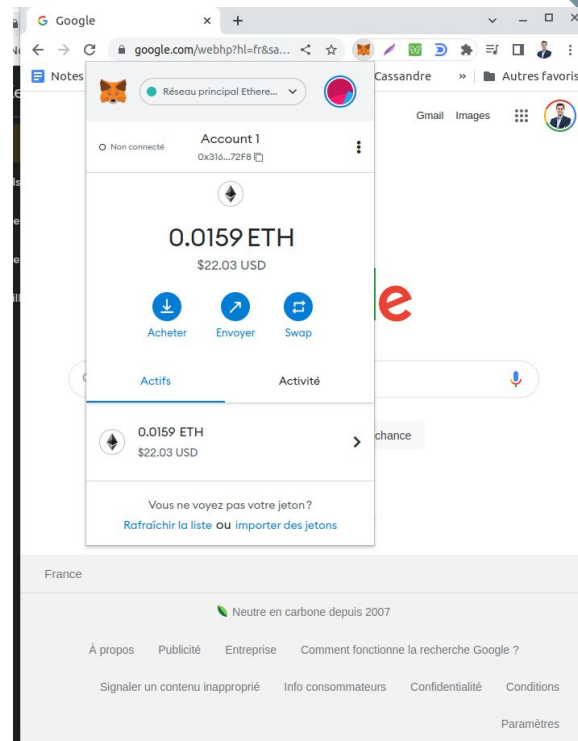
La façon de créer un seeds a été standardisée par la BIP-39, elle permet de créer un seed à partir d'une séquence de mots anglais (entre 12 et 24 mots).



Blockchain 101

Voir mes actifs

Maintenant que vos mots sont entrés dans le wallet, celui-ci va aller voir sur la blockchain tous les actifs verrouillés que vous pouvez déverrouiller avec vos clés privées.



Blockchain 101

Envoyer des Ethers

Très simple, on clique sur nouvelle transaction, vous entrez l'adresse, le montant puis on envoi !

Interface de l'application pour envoyer des Ethers (ETH).

En haut à gauche : Logo de la Fox (Ethereum) et un menu déroulant "Réseau principal Ethere...".

En haut à droite : Bouton "Envoyer".

Champ de destination : Une adresse Ethereum (0x912fD21d7a69678227fE6d08C64222Db41477bA0) est saisie, précédée d'une coche verte.

Message d'information : "Nouvelle adresse détectée ! Cliquez ici pour ajouter à votre carnet d'adresses."

Actif : ETH. Solde : 0.01590475 ETH.

Montant : 0,0005 ETH (\$0.69 USD). Un bouton "Max." est visible à gauche.

En bas : Deux boutons, "Annuler" (gris) et "Suivant" (bleu).

Blockchain 101

On peut faire du “swap”

On peut échanger nos tokens pour d'autres tokens...

 Réseau principal Ethere... 

Swap [Annuler](#)

Swap de

 ETH ▼

0.0005 ≈ \$0.69

0.0159 ETH disponibles pour un swap

↕

Swap vers

 USDT ▼

Vérification effectuée sur 8 sources. Confirmez toujours l'adresse du jeton sur [Etherscan](#). 

[Options avancées ▼](#)

Vérifier le swap

[Conditions de service](#)



Si vous ne possédez pas vos clés,
vous ne possédez rien du tout !



Intro

Les concepts de base

Assets

Les différents types
d'actifs

Defi

Les possibilités de la
finance décentralisée

DAO

Les possibilités des
organisations distribuées

Qu'est ce qu'un actif digital ?

Considérez le terme "actif numérique" comme un large ensemble qui englobe tout ce qui est produit et échangé sur une blockchain

Différence entre blockchain & actifs

La blockchain est un livre de compte qui permet de stocker l'information, notamment quelle adresse dispose de quoi.

Les actifs vivent "dans" la blockchain, ils y sont créés et stockés, et transférés.

Vous pouvez donc avoir une blockchain comme Ethereum avec sa propre monnaie, l'Éther et des nouveaux actifs créés et stockés sur cette blockchain.

Blockchain

≠

Actifs

Premier type : Les crypto actifs

Toute unité qui est utilisée comme stockage de valeur ou médium d'échange qui est stocké sur la blockchain.



à savoir :

Les tokens ERC20

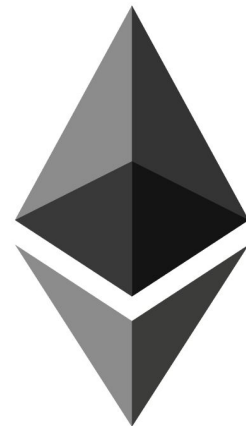
Ces tokens sont créés par un Smart Contract. Ces Smart Contract sont alors chargés de :

- Définir un nombre total du nouveau token
- Les transactions liées à ce token.
- la gestion des balances d'une adresse.

Pour obtenir des tokens, il faut payer le contrat en ethers.

Par exemple, Pour 2 Ethers, je peux obtenir 15 tokens...

ERC20



Deuxième type : Les stable coins

Une crypto-monnaie qui a été conçue pour avoir un prix lié à des monnaies ou actifs classiques.



Troisième type :

Les NFT

Un jeton qui représente la propriété d'un élément numérique unique (Une œuvre d'art, une pièce d'identité, une clé d'appartement...).

Un NFT certifie que le détenteur possède l'actif numérique sous-jacent et peut le vendre, l'échanger ou le racheter.

ERC-721



Quatrième type : Jetons utilitaires

Les jetons utilitaires sont conçus pour être utilisés dans un but précis.

Ils offrent aux titulaires un certain nombre d'avantages, souvent l'accès à des produits et services.

Par exemple, Filcoin vous permet de payer le stockage de fichiers.





Intro

Les concepts de base

Assets

Les différents types
d'actifs

Defi

Les possibilités de la
finance décentralisée

DAO

Les possibilités des
organisations distribuées

Qu'est ce que la DeFi ?

Decentralized Finance : c'est un système financier qui fonctionne sans tiers de confiance (transaction, contrats, prêt, épargne, crédit, hypothèque, trading, actions...).

Cela se présente comment ?

L'exemple AAVE



AAVE

Le principal prêteur du monde de la DeFi.

Aave est le leader des prêts décentralisés.

Aave a une valeur totale verrouillée (TVL) de 5,6 milliards de dollars et est sur la bonne voie pour générer 147,6 millions de dollars de revenus annualisés.



Une première version

“Banking is necessary; banks are not” Bill Gates

En 2017, Stani Kulechov, alors étudiant, découvre Ethereum et il se rend compte qu’on peut créer des contrats qui s’exécutent sans intermédiaire.

Il crée rapidement ETHlend qui essaye de faire matcher prêteur et emprunteur.

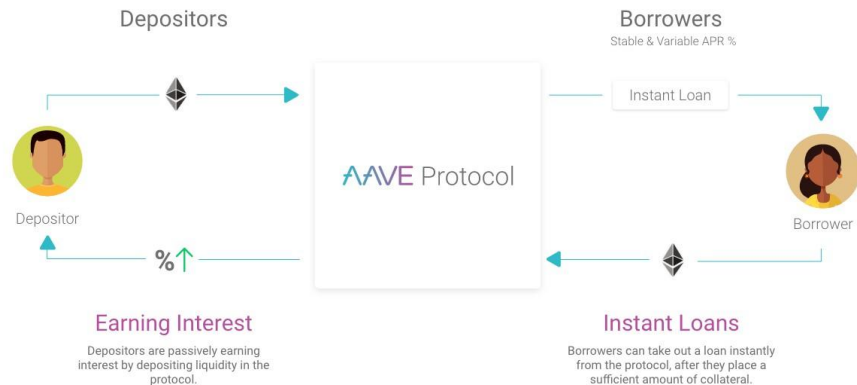
```
1  pragma solidity 0.4.24;
2
3  /*
4   The LoansLedger stores the data of all the loans in the platform.
5   Each loan agreement has a deposit smart contract associated, where the collateral, funds and
6   repayments are stored in the different states of the loan agreement.
7  */
8
9  /**
10   * @title Interface of the LoansLedger
11   */
12  interface ILoansLedger {
13      /**
14       * @dev Get the addresses of all the deposits
15       * @return A list of deposits addresses
16       */
17      function getLoanRequests() external view
18          returns (address[]);
19
20      /**
21       * @dev Get the addresses of all the deposits filtered by borrower address
22       * @param borrower - borrower address
23       * @return A list of deposits addresses
24       */
25      function getLoanRequestsByBorrower(address borrower) external view
26          returns (address[]);
27  }
```

Mise en place de pool

C'est très difficile de faire marcher son système mais il arrive à lever des fonds...

Puis change la philosophie pour passer à un système de pool.

Les pools de liquidités sont un mécanisme par lequel les utilisateurs peuvent regrouper leurs actifs dans les smart contracts afin de fournir des liquidités d'actifs aux traders pour échanger entre les devises.



Fonctionnement

Côté prêteur

Imaginons que vous ayez 100 Éthers... vous espérez que le prix va monter mais vous aimeriez bien avoir des intérêts...

Vous pouvez les déposer chez AAVE, qui va les mettre à disposition des emprunteurs!

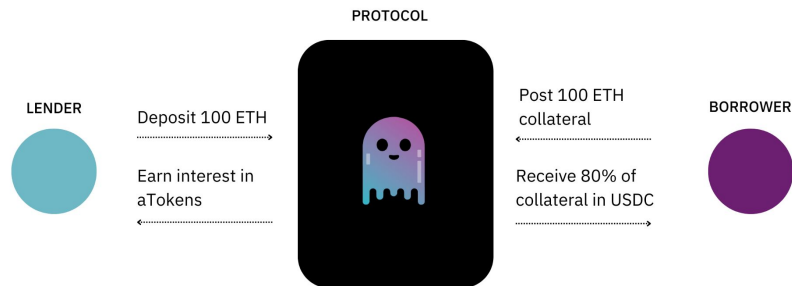
Côté emprunteur

Vous disposez de 100 Éthers... vous voudriez les garder car vous pensez qu'ils vont prendre de la valeur mais vous voudriez investir dans autre chose...

Vous déposez vos 100 Ethers chez AAVE qui va vous donner 80% de vos fonds en USDC.

How Aave works

A simplified explanation

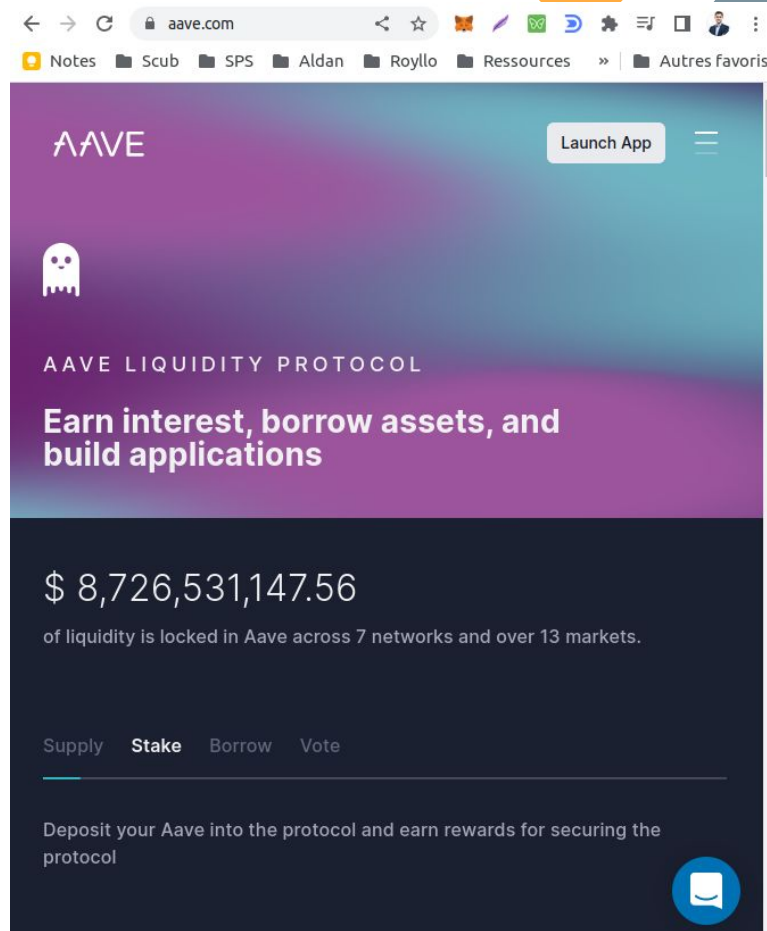


Cela se présente comment ?



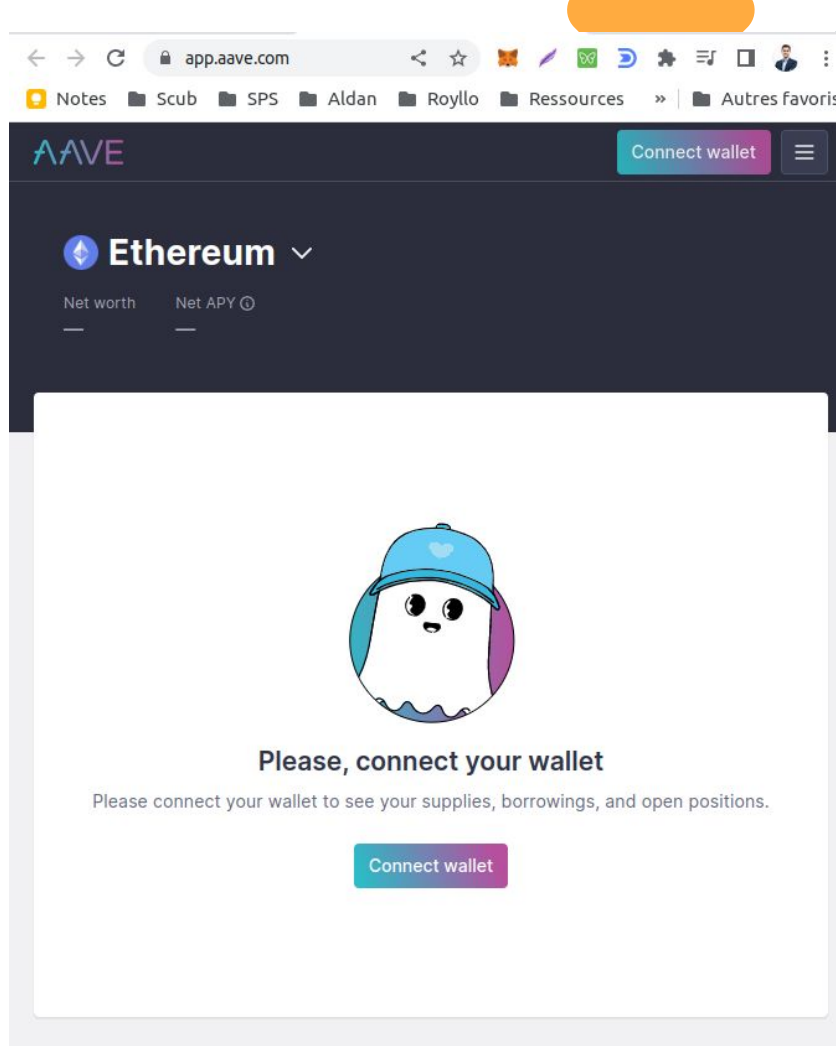
AAVE

**Allez sur aave.com
Cliquez sur launch
APP**



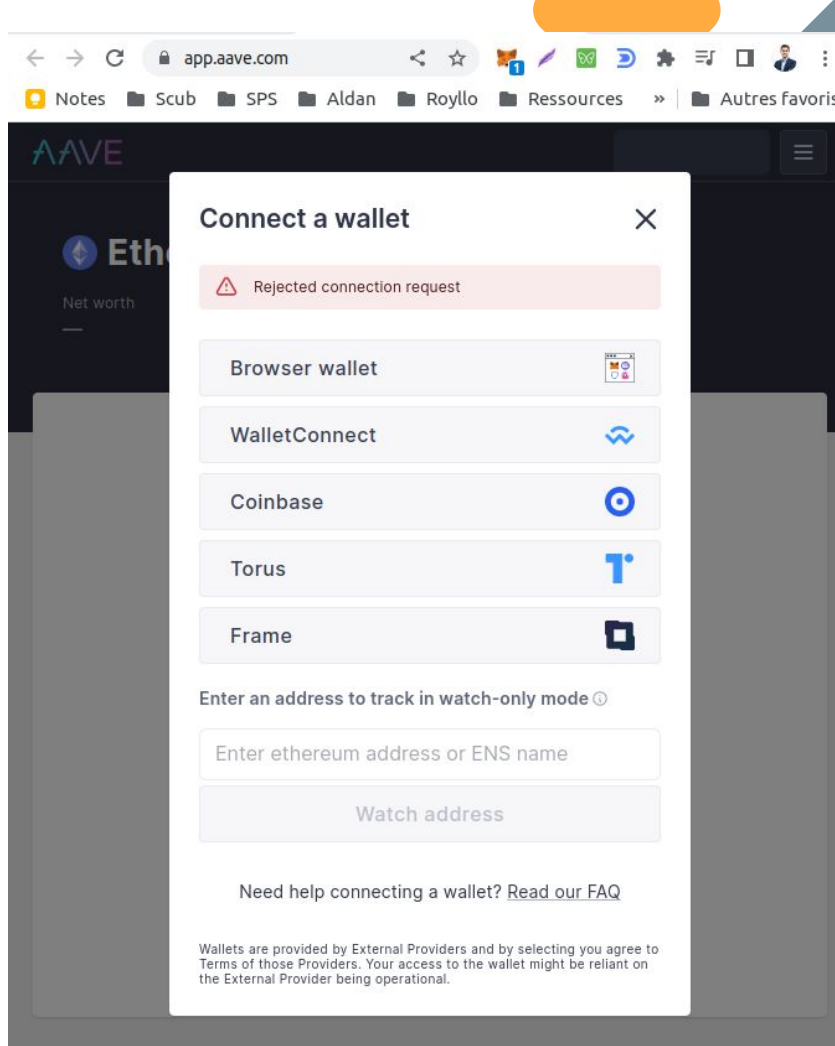
AAVE

Vous vous connectez à votre wallet



AAVE

Vous choisissez votre Wallet



AAVE

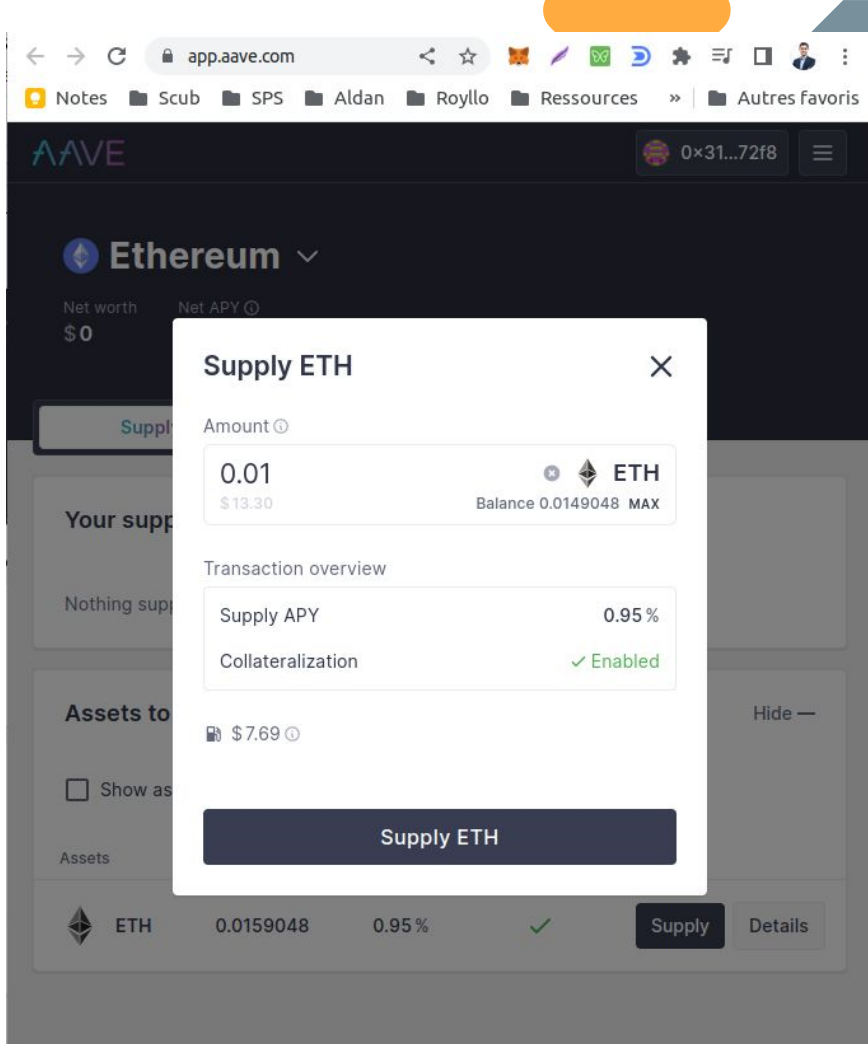
C'est tout...
Vous pouvez
fournir des ethers

The screenshot shows the Aave web application interface. At the top, the browser address bar displays 'app.aave.com'. Below the browser, the Aave logo is on the left, and the user's profile and wallet address '0x31...72f8' are on the right. The main header shows 'Ethereum' with a dropdown arrow. Below this, the 'Net worth' is '\$0' and the 'Net APY' is '0%'. There are two buttons: 'Supply' (highlighted in light blue) and 'Borrow' (dark blue). The 'Your supplies' section is empty, showing 'Nothing supplied yet'. The 'Assets to supply' section has a 'Hide' button and a checkbox for 'Show assets with 0 balance'. Below this is a table with columns: 'Assets', 'Wallet balance', 'APY', and 'Can be collateral'. The table contains one row for 'ETH' with a balance of '0.0159048', an APY of '0.95%', and a green checkmark indicating it can be collateral. At the bottom right of the table are 'Supply' and 'Details' buttons.

Assets	Wallet balance	APY	Can be collateral
ETH	0.0159048	0.95%	✓

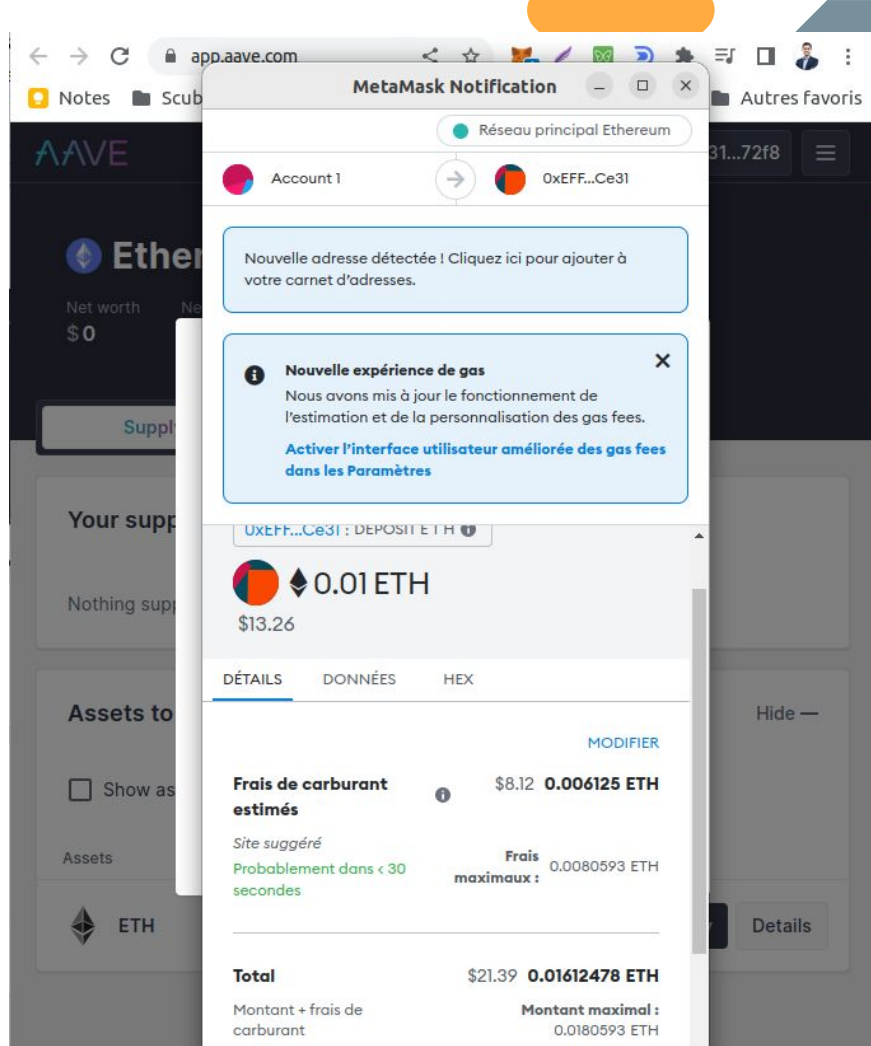
AAVE

**Vous choisissez
combien vous
voulez envoyer**



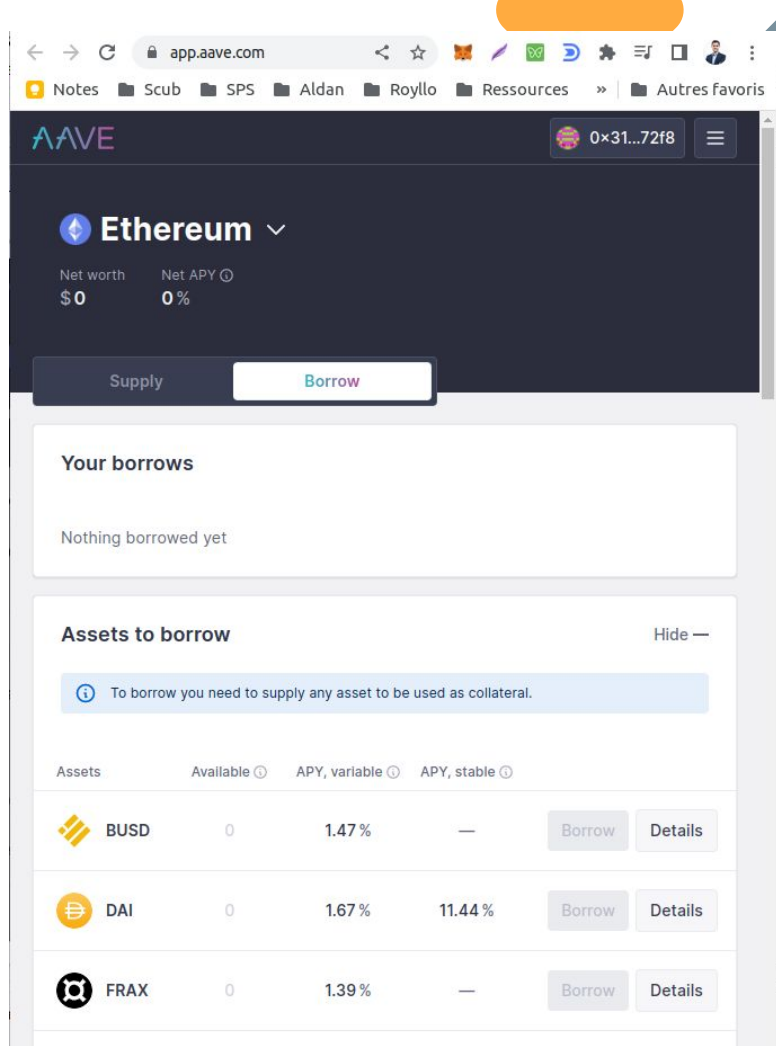
AAVE

Votre wallet reçoit la transaction et vous pouvez la valider (ou pas)



AAVE

**Avec la même
simplicité, vous
pouvez emprunter
d'autres actifs...**



Autres exemples



Exchange

Permettre d'échanger des assets contre des assets de manière décentralisée.

(ex : Uniswap)

Prêt

Emprunter des fonds.

(ex : Notional)

Prédiction

**Faire des prédictions (parier)
sur divers sujets.**

(ex : TotemFi)

Liquidité

Fournir des fonds.

(ex : Uniswap)



Intro

Les concepts de base

Assets

Les différents types
d'actifs

Defi

Les possibilités de la
finance décentralisée

DAO

Les possibilités des
organisations distribuées

Qu'est ce qu'une DAO ?

Une organisation autonome décentralisée est une organisation qui se fixe une mission et qui fonctionne grâce à un ensemble de smart contracts permettant d'établir et de fournir des règles de gouvernance à une organisation.

Les bases d'une DAO

Pour faire certaines choses, les humains se sont organisés en groupes, tribus, escouades, équipages, équipes, états, entreprises...

Les DAO sont une manière de s'organiser.

Cela peut servir à des développeurs, des investisseurs, des activistes...

Pour en faire partie, vous devez posséder des tokens de cette organisation.

Decentralized = Online, global, uncensorable.

Autonomous = Self-governing.

Organization = Coordination & collaboration.

Les bases d'une DAO

La manière la plus courante pour les DAO de prendre des décisions consiste à utiliser des mécanismes de vote basés sur des jetons de gouvernance.

Plus vous possédez de jetons de gouvernance, plus vous avez de pouvoir de vote.

Certains DAO permettent à tout membre de faire une proposition, tandis que d'autres peuvent limiter ce droit à un groupe spécifique.

Decentralized = Online, global, uncensorable.

Autonomous = Self-governing.

Organization = Coordination & collaboration.

Exemples de DAO

The LAO

<https://www.thelao.io>

"The LAO allows Members to pool capital, invest in projects, and share in any proceeds from the investment"

"The LAO is organized as a legal entity (a Delaware limited liability company) primarily administered via an online application (a "DApp") and related smart contracts"



Créer et tout savoir sur les DAO

Aragon

<https://aragon.org/>

Ils expliquent TOUT

Et vont permettre de créer votre propre
organisation à partir de modèles.



Cela se présente comment ?



DAO

Trouvez une DAO

Organizations

4829 Organizations, 2275 Enriched by DeepDAO, Oct. 3rd, 6:02

Total treasury USD

\$ 9.5B

↗ \$ 27.3M
1 week

vesting \$3.1B
liquid \$6.4B

↘ \$ -683.5M
1 month



Orgs. over threshold AUM USD

Total 2275



top organizations



categories ▾

rank	organization	treasury	last 24hrs	top treasury tokens
1	 Uniswap	\$2.6B	↘ -3.3%	    
2	 BitDAO	\$1.3B	↘ -0.2%	    
3	 ENS	\$1.1B	↘ -3.3%	    

DAO

Trouvez son token

PARTNERSHIPS GOVERNED BY \$BIT

BitDAO is a collective of builders, products, and mutually beneficial ecosystems governed by \$BIT token holders.

DOCUMENTS ↗

FORUM ↗

DAO

Achetez des tokens !

Échanger

0.01

\$13.04

ETH

Solde : 0.0159 MAX

↓

27.1473

\$13.00 (-0.3%)

Bit BIT

Solde : 0

1 BIT = 0.0003684 ETH (\$0.4790)

\$3.54

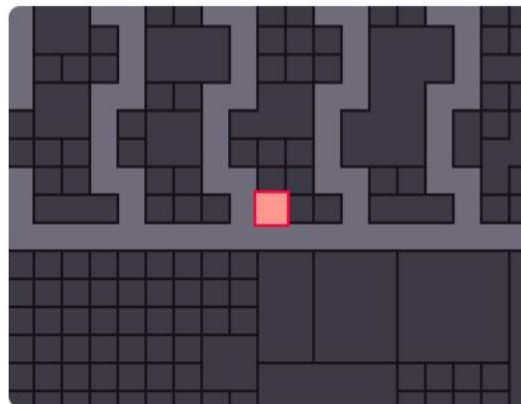
Échanger

Uniswap disponible en : [English](#)

Add the location -30,-108 to the Points of Interest

ACTIVE

POI



Should the scene located at -30,-108 be added to the Point of Interest list?

DESCRIPTION

The BVERSE HQ is used for hosting business networking & DCL community events. We are a metaverse consulting company & network of metaverse business professionals. We strive to host more educational events to our DCL & LinkedIn community.

JUMP IN →

Discuss in the forum

Add to my Watchlist

CURRENT RESULT

SEE VOTES

yes 99%

2,975,317 VP (79 votes)

no 1%

1 VP (1 vote)

500k VP Threshold reached

Voting ends in 4 hours

VOTE YES

VOTE NO

You need at least **1 VP** to vote

[Get VP](#)

Aller plus loin

La blockchain est une nouvelle forme d'ordinateur qui permet une nouvelle évolution :

- L'ère "Lire" (Read) : Les premières années d'Internet ont démocratisé l'accès à l'information, permettant aux utilisateurs de consulter des contenus en ligne.
- L'ère "Lire-Écrire" (Read-Write) : Avec l'avènement des plateformes interactives, les utilisateurs ont pu non seulement consommer, mais aussi créer et publier leurs propres contenus.
- L'ère "Lire-Écrire-Posséder" (Read-Write-Own) : Dixon soutient que nous entrons désormais dans une nouvelle phase, souvent appelée Web3, où les technologies blockchain redonnent aux utilisateurs le contrôle et la propriété de leurs données et créations numériques.

Read Write Own
Building the Next Era
of the Internet
Chris Dixon

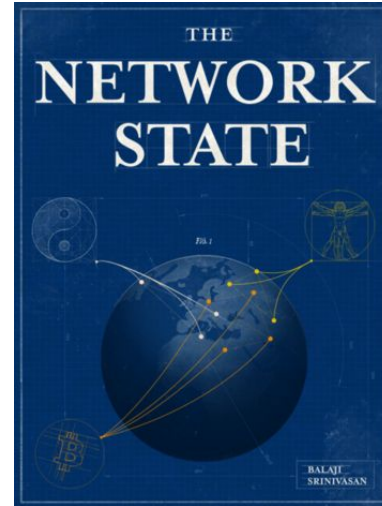


Aller plus loin

La technologie nous a permis de créer de nouvelles entreprises, de nouvelles communautés et de nouvelles devises. Mais peut-on l'utiliser pour démarrer de nouvelles villes, voire de nouveaux pays ?

Ce livre explique comment construire le successeur de l'État-nation, un concept que appelé l'État-réseau.

(Niveau science fiction!)





www.scub.net

contact@scub.net

05 45 373 373

Merci
de votre écoute.



SCAN ME

Le fonctionnement détailé de Bitcoin



Le hachage

Le hachage

Un algorithme de **hachage** prend n'importe quelle donnée de “n'importe quelle taille” en entrée et produit une chaîne de caractère “unique” qui fera toujours la même taille et qui sera une sorte d'empreinte de vos données d'entrées.

Si un seul caractère de votre texte est changé, le hachage va complètement changer.

Exemple

“Je m’appelle Stéphane Traumat”

Devient

607af60dbf07e5c08d985e2c794624b8c05b77a5235c8071e0243baeb547906b

“Je m’appelle Stéphane Traumat!”

Devient

a7b5b4dbae0800a23a47f5abf7cb7bf12999cebfbf3e8ac199ea96c93be4802

A quoi cela sert-il ?

Les fonctions de **hachage** permettent de **vérifier** très rapidement **si un contenu, quelle que soit sa taille, a été modifié.**

La blockchain

La blockchain

La blockchain est le **registre global de toutes les transactions** qui ont eu lieu depuis la création de Bitcoin.

On peut se le représenter comme un fichier dans lequel vont s'empiler, les uns sur les autres, des groupes de transactions validées (appelés blocs).

La blockchain

Bloc 9

Contenu transaction 1

Contenu transaction 2

Contenu transaction 3

Résumé (hachage) du block précédent

Résumé de l'ensemble du contenu du block

La blockchain

Bloc 10

Contenu transaction 4

Contenu transaction 5

Contenu transaction 6

Résumé (hachage) du block précédent

Résumé de l'ensemble du contenu du block

Bloc 9

Contenu transaction 1

Contenu transaction 2

Contenu transaction 3

Résumé (hachage) du block précédent

Résumé de l'ensemble du contenu du block

La blockchain

- Chaque bloc de transactions est identifié par un hash calculé qui représente son contenu.
- Chaque bloc sert de fondation au bloc suivant car il référence dans son entête le hash de son père.
- Si vous changez le contenu d'un ancien bloc, il vous faudrait recalculer tous les blocs qui se trouvent au-dessus de lui.

Le minage

Le minage

Le **minage** (mining) est le processus qui **sécurise** le système et rend la blockchain **infalsifiable**.

En contrepartie de ce travail, les mineurs se voient octroyer de la monnaie créée pour l'occasion (en plus des frais inclus dans chaque transaction).

Exemples de mineurs



La problématique

La problématique à traiter est la suivante :

Comment mettre d'accord un réseau d'inconnus sur une vérité universelle en sachant que, dans un réseau d'inconnus, on ne peut faire confiance à personne ?

Il va falloir faire en sorte qu'une machine qui lise le solde d'un compte dans la blockchain ait confiance en son contenu... sans pouvoir demander à une autorité centrale.

Une vue d'ensemble

- Chaque nœud du réseau qui fait du minage stocke les transactions qui sont arrivées depuis l'ajout du dernier block au blockchain.
- Dès qu'un block est validé et ajouté (environ toutes les 10 minutes), chaque nœud de minage va essayer de créer un nouveau bloc avec les transactions en attente. Ce bloc, pour être accepté par les autres, devra contenir la solution à un problème. Ce qui nécessite d'essayer beaucoup de combinaisons.
- Le premier nœud qui réussit à résoudre le problème va envoyer son block aux autres et va remporter les 6,25 bitcoins plus les frais de transactions !

Création d'un bloc

La règle du jeu pour tous les mineurs est simple :

- Vous prenez le contenu de toutes les transactions et vous le mettez dans un bloc.
- Dans ce bloc, vous n'avez le droit de faire varier que la valeur d'une variable appelée "Nonce".
- Sur le contenu du bloc (avec la variable "Nonce"), vous utilisez la fonction de hachage SHA-256.
- Le premier qui a trouvé la valeur de "Nonce" pour laquelle le hachage commence par un certain nombre de zéro a gagné !

La blockchain

Bloc 10

Contenu transaction 4

Contenu transaction 5

nonce : 54561247846

Résumé (hachage) du block précédent

Résumé de l'ensemble du contenu du block commençant par un certain nombre de 0

Bloc 9

Contenu transaction 1

Contenu transaction 2

Nonce : 836248764865645874

Résumé (hachage) du block précédent

Résumé de l'ensemble du contenu du block commençant par un certain nombre de 0

Ce qui va se passer chez tout le monde

Ce qui va se passer est au final assez simple :

- Notre nœud de minage va mettre la valeur “1” dans le champs “Nonce”, puis va concaténer tous les autres champs et calculer la valeur sha256 de l’ensemble de cette chaîne.
- Si le résultat ne commence pas par le bon nombre de “0”, il va mettre la valeur “2” dans le champ “Nonce”, concaténer tous les champs, calculer la valeur sha-256 et vérifier si le résultat commence par cinq “0”
- Ainsi de suite jusqu’à ce que quelqu’un dans le réseau bitcoin y arrive.

Quand le bloc est créé

C'est donc une compétition mondiale entre des milliers de machines qui effectuent des calculs "complexes" afin de trouver une valeur particulière à partir des données du nouveau bloc à valider.

Lorsqu'un nœud a trouvé la valeur de "Nonce" qui convient pour en faire un bloc valide, il transmet le bloc aux autres membres du réseau qui vont le vérifier et le transmettre aux autres et ainsi de suite jusqu'à ce que tout le réseau le reçoive et l'ajoute au blockchain.