

# Blockchain - Web2

Mathieu Bour

Mewo Informatique



# Le (sublime) formateur (c'est moi !)

- Ingénieur spécialisé en Blockchain/Web3
- Investisseur dans les cryptomonnaies depuis 2013
- Auditeur de smart-contracts depuis 2021
- (accessoirement) diplômé des Mines de Saint-Étienne en 2020
- Levé \$3M avec DeepSquare sur la blockchain Avalanche
- Actuellement chez Pooky, un jeu de prédiction de match de foot



Mathieu Bour

Tél : 06.95.39.72.53

Mail (Mewo) : [mathieu.bour@mewo-campus.fr](mailto:mathieu.bour@mewo-campus.fr)

Mail (pro) : [mathieu@bour.tech](mailto:mathieu@bour.tech)

- DYOR = « Do Your Own Research » : bien que ce cours soit à jour en mai 2023, je peux m'être trompé. La blockchain n'autorisant pas l'erreur, prenez le temps de faire vos propres recherches.
- La blockchain peut permettre de gagner beaucoup d'argent, mais la très grande majorité des investisseurs perdent leur mise. DYOR.
- En tant que pro-décentralisation, certaines slides peuvent ne pas être objectives, voire tomber dans la poilitique. DYOR.
- Bien que nous évoquerons l'ensemble des types de blockchains, nous utiliserons uniquement les blockchains publiques et décentralisées dans ce cours.

# Plan de la Présentation

- 1 Introduction à la blockchain
- 2 Blockchain Ethereum
- 3 Smart contracts & Solidity

# Introduction à la blockchain

- 1 Introduction à la blockchain
- 2 Blockchain Ethereum
- 3 Smart contracts & Solidity

# Objectifs de ce module

- ➊ Comprendre les enjeux basiques de la blockchain
- ➋ Développer des smart-contracts de tokens fongibles et non-fongibles
- ➌ Se sensibiliser à la sécurité de la blockchain

# Blockchain : définitions



# Définition générale

Blockchain se traduit par « chaîne de blocs ». Il s'agit donc d'un système permettant de stocker et de partager de l'information au travers d'un **structure de données bien choisie construite à partir de plusieurs blocs** (et c'est tout).

La majorité des systèmes de blockchain possèdent des caractéristiques supplémentaires qui sont utilisées par abus de langage :

- ❶ Présence d'une cryptomonnaie liée à la blockchain (il existe des blockchains SANS cryptomonnaies)
- ❷ Décentralisation
- ❸ Autonome/sans administration centrale
- ❹ Anonymat/pseudonymat des utilisateurs

economie.gouv.fr

*Développée à partir de 2008, c'est, en premier lieu, une technologie de stockage et de transmission d'informations. Cette technologie offre de hauts standards de transparence et de sécurité car elle fonctionne sans organe central de contrôle.*

*Plus concrètement, la chaîne de blocs permet à ses utilisateurs - connectés en réseau - de partager des données sans intermédiaire.*

Wikipédia

*Une blockchain, ou chaîne de blocs, est une technologie de stockage et de transmission d'informations sans autorité centrale. Techniquement, il s'agit d'une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne.*

(Dé)centralisation



# Cryptographie

# Blockchain

Par développer nos smart-contracts, nous allons utiliser la blockchain Polygon et le framework Foundry.

```
1  pragma solidity 0.8.19;  
2  
3  contract Counter {  
4      uint256 public value;  
5  
6      function set(uint256 _value) external {  
7          value = _value;  
8      }  
9  }
```