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
Mail (pro) : mathieu@bour.tech

mewo
INFORMATIQUE

Disclaimer

- 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

mewo
INFORMATIQUE

Sommaire

1. Introduction à la blockchain
   - Définitions générales
   - Cryptographie
   - Exemple du Bitcoin
   - Blockchain
   - Problème du consensus
2. Blockchain Ethereum
3. Smart contracts & Solidity

Objectifs de ce module

1. Comprendre les enjeux basiques de la blockchain
2. Développer des smart-contracts de tokens fongibles et non-fongibles
3. Se sensibiliser à la sécurité de la blockchain

Définitions générales

Contexte historique : origines de la blockchain

- 2008 : Satoshi Nakamoto publie « Bitcoin: A Peer-to-Peer Electronic Cash System »
- Dans ces neuf pages, Nakamoto décris un système financier et introduit les bases de la blockchain
  - Structure en blocs
  - Cryptographie (hachage, asymmétrique, arbres de Merkel...)
  - Transactions
- Fun fact : Satoshi Nakamoto est toujours resté anonyme

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 :

1. Présence d'une cryptomonnaie liée à la blockchain (il existe des blockchains SANS cryptomonnaies)
2. Décentralisation
3. Autonome/sans administration centrale
4. Anonymat/pseudonimat des utilisateurs

Définitions tierces

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.*

Cryptographie

Notations

Je suis désolé, il faut faire un tout petit peu de maths...

Dans la suite, je vais noter :

- $\mathbb{B} = \{0,1\}^{\mathbb{N}}$ l'ensemble des mots binaires
- $\mathbb{B}_{n\in\mathbb{N}} = \{0,1\}^n$ l'ensemble des mots binaires de taille n

Exemples :

- $B_3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- 010010 est un mot binaire de 6 bits, il est donc membre de $\mathbb{B}_6$

Qu'est-ce que la cryptographie ?

TL ;DR = utiliser les mathématiques au service de la sécurité de l'information
Exemples historiques :

- Chiffrement de César : décalage de lettre de 1 à 25
- Chiffrement de Vigenère : sustitions de lettres à partir d'une clé secrète
- Chiffrement affine : subsutition de lettre à l'aide d'une équation affine
- Enigma (seconde guerre modiale) : machine de chiffrement allemande

Figure – Machine Enigma

Somme de contrôle : définition

Définition

Une somme de contrôle est une petite quantité de données additionnelle qui est calculée à partir d'un ensemble plus large de données. Elle est utilisée pour vérifier l'intégrité des données et détecter les erreurs ou les altérations éventuelles.

Somme de contrôle : exemple du numéro de sécurité sociale

Les deux derniers chiffre du numéro de sécurité sociale ne contiennent aucune information mais ils sont utilisés comme somme contrôle, pour limiter les risques de faute d'erreur.

La formule permettant de calculer la clé est la suivante :

$$\text{clé} = 97 - \mathit{NIR} \bmod 97$$

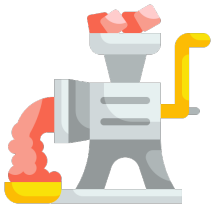
Prenons l'exemple suivant :

$$\underbrace{2690549588157}_{\text{numéro NIR}}\ \underbrace{80}_{\text{clé}}$$

```
>>> 97 - 2690549588157 % 97
80
```

Fonction de hachage : définition

Comment appliquer cette logique à de l'information binaire ? On cherche une somme de contrôle universelle capable de fonctionner sur tout $\mathbb{B}$.
$\Rightarrow$ on les appelle fonction de hachage



Définition

Une fonction de hachage permet de générer un « hash » de n'importe quel mot binaire.

Définition

Un hash est un mot binaire de taille fixe, dont la taille est spécifique à la fonction de hachahe utilisé.

Fonction de hachage : exemples

```
1 >>> import hashlib
2 >>> hashlib.sha256(b"Mathieu").hexdigest()
3 'f5e088d29801ebb822251d7751bc4b8ff28c50132d8b0a95614b5f048a1d01b6'
```

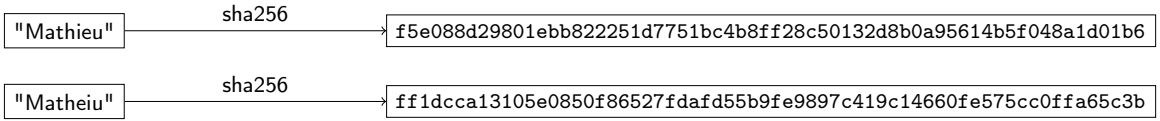


Figure – Hachage avec SHA-256

Caractéristiques d'une fonction de hachage

Collision

Une fonction de hachage h de taille n entraîne obligatoirement des collisions car la taille de $\mathbb{B}$ est infinie alors que $\mathbb{B}_n$ n'est « que » de 2^n. Une collision existe quand deux mots binaires a et b engendrent le même hash, c'est-à-dire :

$$h(a) = h(b)$$

$\Rightarrow$ une « bonne » fonction de hachage ne possède pas de hash connu.

Les alorithme md4, md5 et sha1 ne sont à jour plus considérés comme sûrs.

Exemple du Bitcoin

Centralisation

Exemples :

1. L'Euro : la banque centrale européenne est souveraine et peut émettre des euros
2. La force nucléaire en France : contrôlée par l'armée
3. Twitter : la direction peut décider de retirer des privilèges sans l'approbation des utilisateurs (arrivée d'Elon Musk...)

⇒ La centralisation place un privilège/pouvoir entre les mains d'un petit groupe

⇒ Inversement, les utilisateurs sont tributaire du bon vouloir/bon fonctionement des systèmes

⇒ Une relation de **confiance** est nécessaire

Bitcoin : décentralisation

- La blockchain Bitcoin est un réseau peer-to-peer décentralisé
- Le réseau Bitcoin **toujours en ligne** (tant qu'il y a des noeuds)
- Pas d'administration centrale (donc pas de Bitcoin Corp. Limited)
- Tout individu peut y participer en créant un « nœud » = démarrer un logiciel en CLI

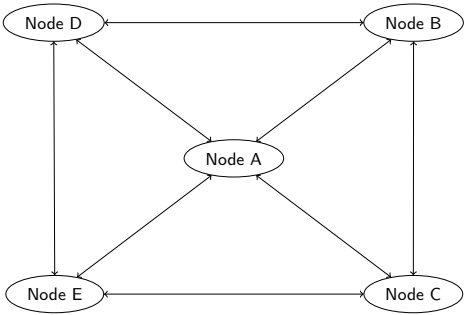


Figure – Réseau peer-to-peer

Bitcoin : livre de comptes

La blockchain Bitcoin est un système décentralisé permettant aux utilisateurs d'échanger une monnaie numérique, le Bitcoin.

- Les Bitcoin (BTC) sont stockés dans des comptes, identifiés par une adresse
- L'ensemble des soldes des comptes, le « livre de comptes » est stocké à de multiples endroits
- Tout individu peut obtenir un compte gratuitement (on en parle plus tard)
- Envoyer des x BTC d'une adresse a à une adresse b revient à faire

```
1  solde_a -= x
2  solde_b += x
```

Compte	Solde
0001	12
0002	3.42
0003	4.4
0004	3.6
0005	5
⋮	
1231	0
1232	30.45
1233	0.34
1234	113.3
1235	4.97

Bitcoin : opérer un node

- Opérer un node = particper à la blockchain = augmenter la décentralisation
- « Relativement léger » : 2 Go de RAM, 7 Go de disque, connexion 400 kilobits/sec
- Attention, certains pays interdisent d'opérer un node : Afghanistan, Algérie, Bangladesh, Bolivie, Chine, Égypte, Kosovo, Maroc, Népal

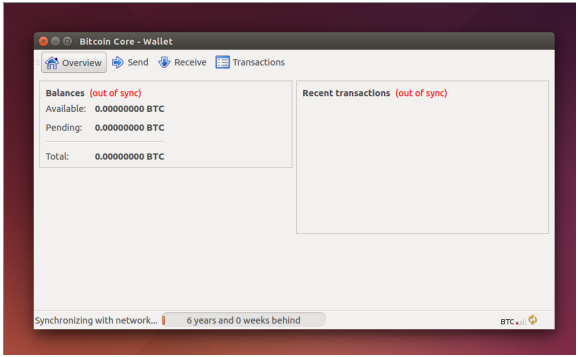


Figure – Bitcoin Core GUI

Blockchain

mewo
INFORMATIQUE

Par développer nos smart-contracts, nous allons utiliser la blockchain Polygon et le framwork 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  }
```