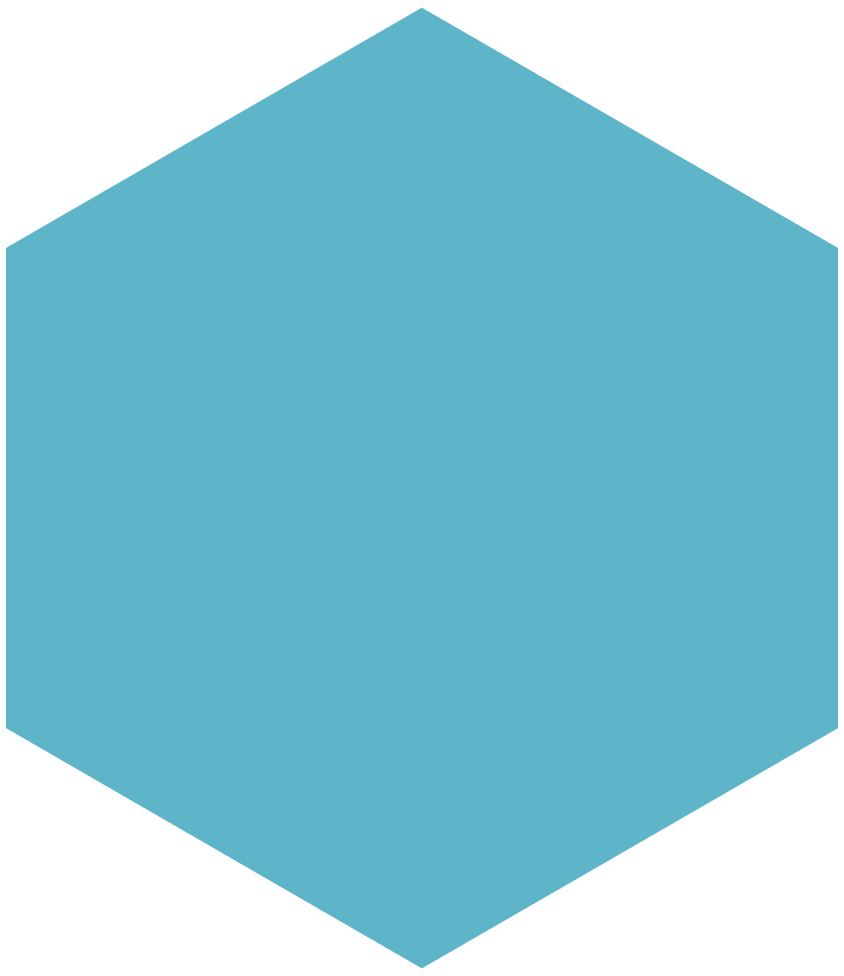


Digital HaïTian Gourde



MASTER 2 MIAGE MBDS

2019-2020

Auteurs :

Thomas BEATINI  
Arnaud FERNANDEZ  
Chloé MACCARINELLI  
Cédric ORTEGA

Tuteurs :

Gabriel MOPOLO-MOKE

Alexandre MAISONOBE

Gaëtan LESCOUFLAIR

Table des matières

[I. Introduction 1](#_Toc25846038)

[II. Etat de l’art 2](#_Toc25846039)

[1) La blockchain 2](#_Toc25846040)

[A. Définition 3](#_Toc25846041)

[B. Les règles de consensus 3](#_Toc25846042)

[C. Les types de blockchains 4](#_Toc25846043)

[1. PUBLIQUE 4](#_Toc25846044)

[2. PRIVE ("DISTRIBUTED LEDGER TECHNOLOGY" (DLT)) 4](#_Toc25846045)

[D. Critères relatifs à notre projet 6](#_Toc25846046)

[2) La crypto-monnaie 6](#_Toc25846047)

[A. Définition 6](#_Toc25846048)

[B. Les différentes crypto-monnaies 7](#_Toc25846049)

[C. Critères relatifs à notre projet 7](#_Toc25846050)

[III. Etude de l’existant 8](#_Toc25846051)

[1) L’environnement 8](#_Toc25846052)

[A. Openchain 8](#_Toc25846053)

[1. Fonctionnement 8](#_Toc25846054)

[2. API 9](#_Toc25846055)

[3. Hyperledger Fabric, une alternative à Openchain 9](#_Toc25846056)

[B. MySQL – API REST NodeJs – Angular 7 11](#_Toc25846057)

[2) Les fonctionnalités existantes 11](#_Toc25846058)

[IV. Les Améliorations 12](#_Toc25846059)

[V. L’application Web (PWA) 12](#_Toc25846060)

[VI. Webographie 12](#_Toc25846061)

# Introduction

Pourquoi creation blockchain quand puis quand 1ere crypto

Avec le temps (2015) de plus en plus de blockchain centralisée 🡪 attire les banques (interet)

Go haiti Haiti

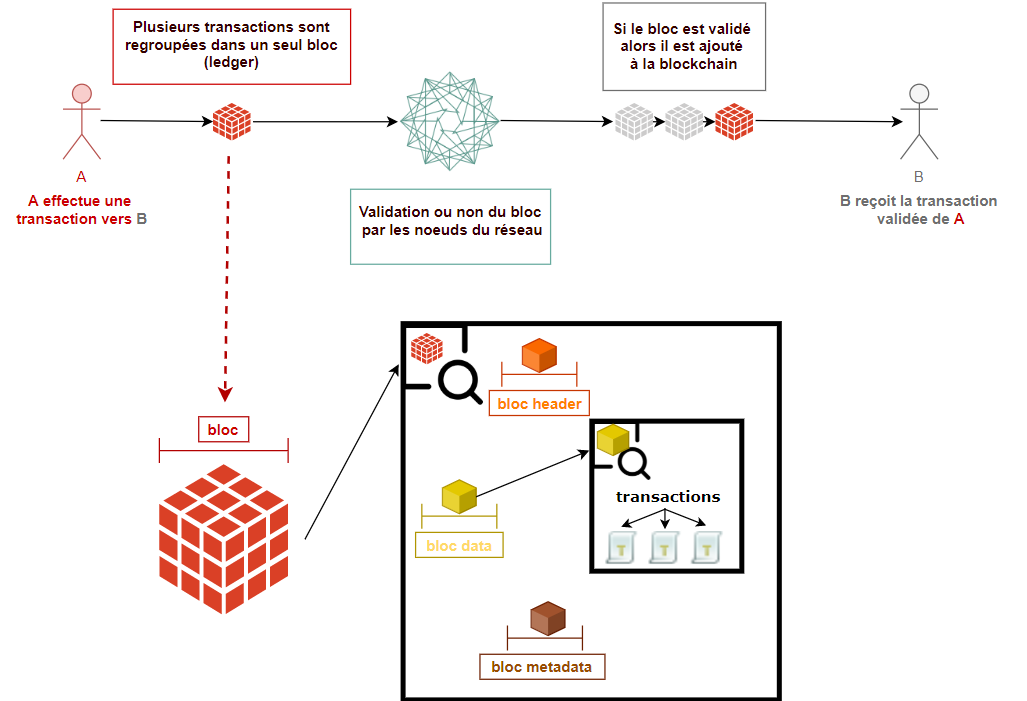
# Etat de l’art

# La blockchain

## Définition

*« La blockchain est une technologie de stockage et de transmission d’informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.*

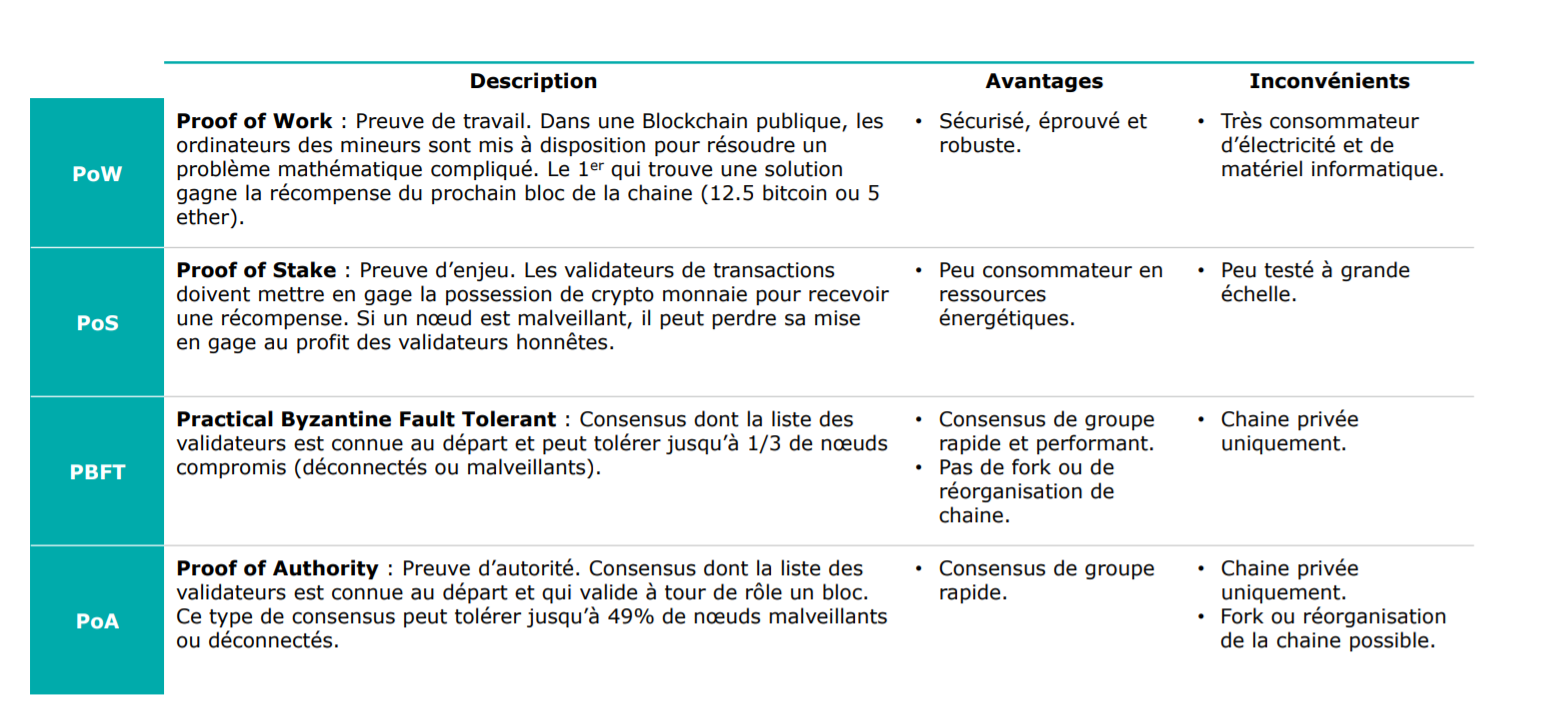
*Par extension, une blockchain constitue une base de données qui contient l’historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. »* *(Définition de Blockchain France)*



**Figure 1 : Fonctionnement d'une blockchain**

## Les règles de consensus

Les règles de consensus désignent le protocole selon lequel un individu sera choisi pour ajouter son bloc à la blockchain. Ce sont les règles de consensus qui assurent la sécurité du réseau et dissuadent la falsification des blocs.



**Figure 2 : Les différentes règles de consensus (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS)**

## Les types de blockchains

### PUBLIQUE

La blockchain dites « publique » est la blockchain d’origine, elle est totalement décentralisée. C’est-à-dire que tout le monde peut lire, effectuer des transactions et participer au processus de validation de blocs, qui seront ou non ajoutés à la blockchain. Tous les acteurs sont égalitaires vis-à-vis de leur participation dans le réseau.

Exemples : Bitcoin, Ethereum, Litecoin, etc.

### PRIVE ("DISTRIBUTED LEDGER TECHNOLOGY" (DLT))

Depuis 2015 les blockchains partiellement décentralisées ou centralisées se développent et offrent de nombreux avantages :

* Gouvernance simplifiée
* Acteurs connus
* Coûts réduits
* Rapidité
* Confidentialité

Exemples : Hyperledger , Corda, monex , B3i, R3, Labchain, etc.

#### BLOCKCHAIN DE CONSORTIUM (SEMI-PRIVE)

La blockchain dites « de consortium » limite et sélectionne le nombre de participants du processus d’approbation et la règles de la majorité ne s’impose pas. La lecture des blocs est publique, réservé aux participants ou hybride. Ce type de blockchain est principalement utilisé dans le secteur bancaire.

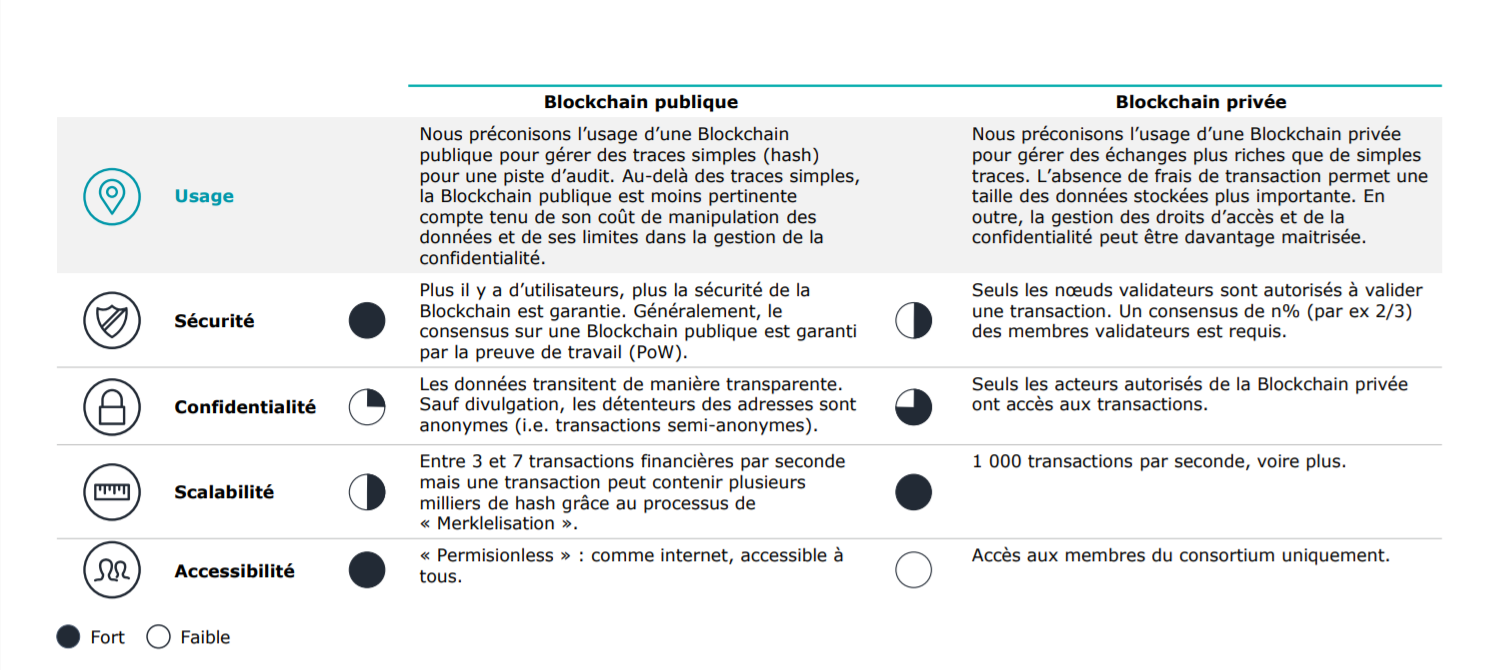
Exemples : R3 (banques), EWF (énergie), B3i (assurance), Corda.

Il y a certains inconvénients, étant donné que la création de bloc est facilitée (une signature suffit), il est possible de créer autant de chaines que possible. De fait si l’on venait à ouvrir la blockchain en lecture à des tiers (clients, auditeurs), ceux-ci n’auraient aucun moyen de vérifier que les données qu’ils consultent soient en provenance de chaine légitime. On pourrait donc se retrouver dans un système de Ponzi (montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants).

#### BLOCKCHAIN TOTALEMENT PRIVEE

La blockchain dites « privée » va autoriser un nombre limité et prédéfini d’acteurs. C’est une seule organisation qui va autoriser ou non la possibilité d’effectuer des transactions ou même de participer à la validation de blocs.

Exemples : Hyperledger Fabric, Corda, OpenChain, etc.



**Figure 3  : Différences entre blockchain privée et publique (La Blockchain- Panorama des technologies existantes © 2017 Deloitte SAS)**

## Critères relatifs à notre projet

Nous nous basons sur des blockchains existantes.

Les critères de comparaisons seront les suivants :

1. Type blockchain
2. Accès en lecture
3. Accès en écriture
4. Accès en modification

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type de blockchain | Lecture | Ecriture | Modification | Exemples d’utilisation |
| Publique | Tout public | Tout public | Tout public | Bitcoin |
| Consortium | Public restreint | Public restreint | Tout public ou Public restreint | Transactions entre plusieurs banques |
| Privé | Public restreint | Administrateur | Administrateur | Transaction au sein d’une seule banque |

# La crypto-monnaie

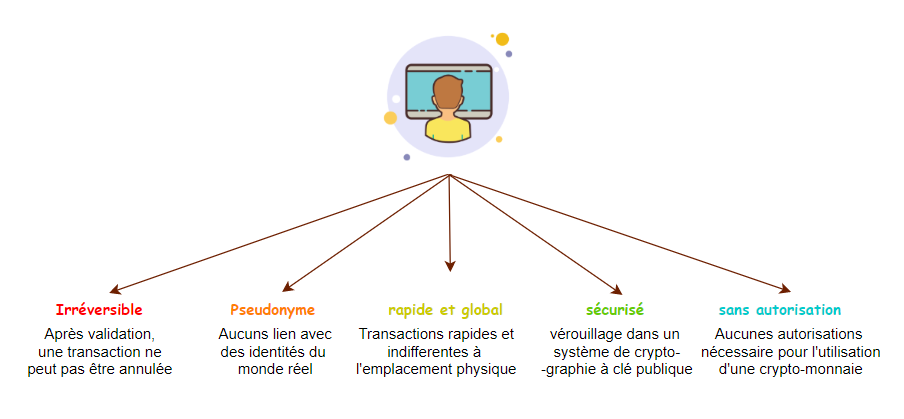
## Définition

Une cryptomonnaie est une monnaie virtuelle, elle ne dispose donc pas de support physique. Elle permet de réaliser des transactions financières, des achats, des virements, ou du stockage de valeur, comme la monnaie traditionnelle.



**Figure 4 : Qu'est-ce que la crypto-monnaie ?**

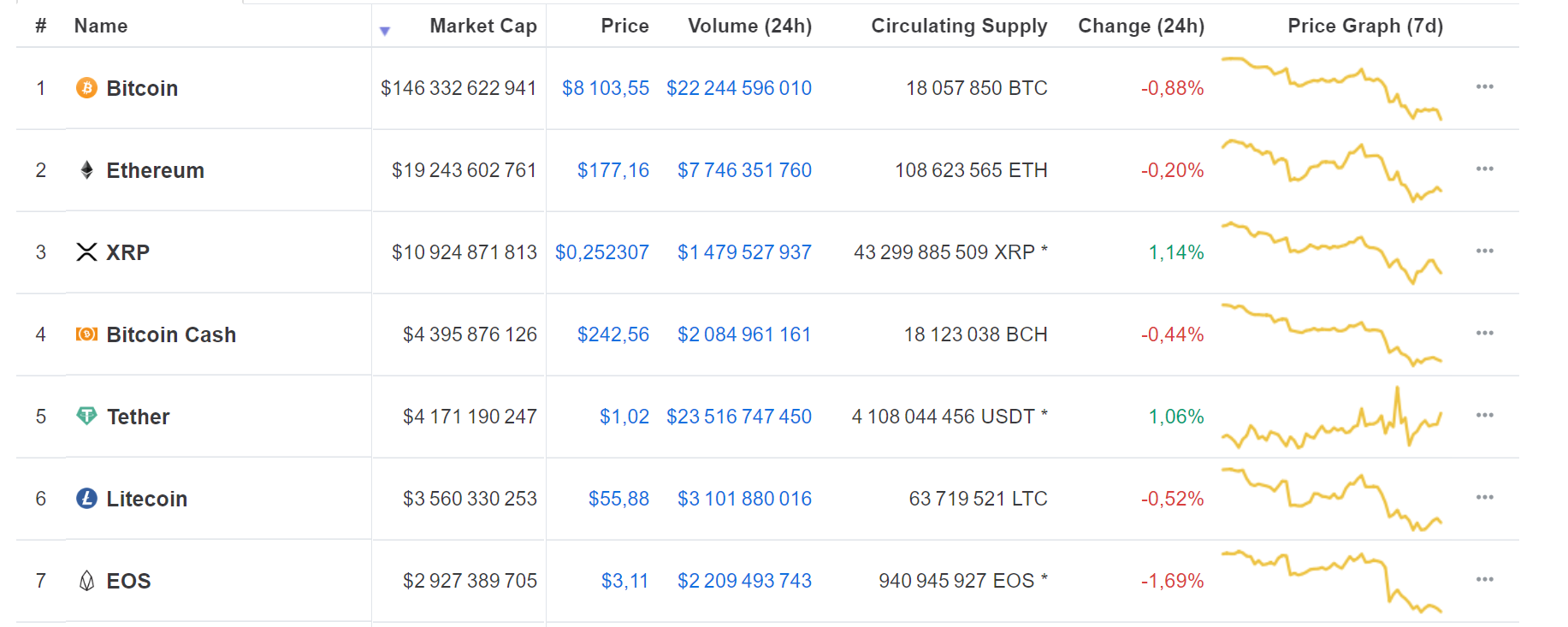
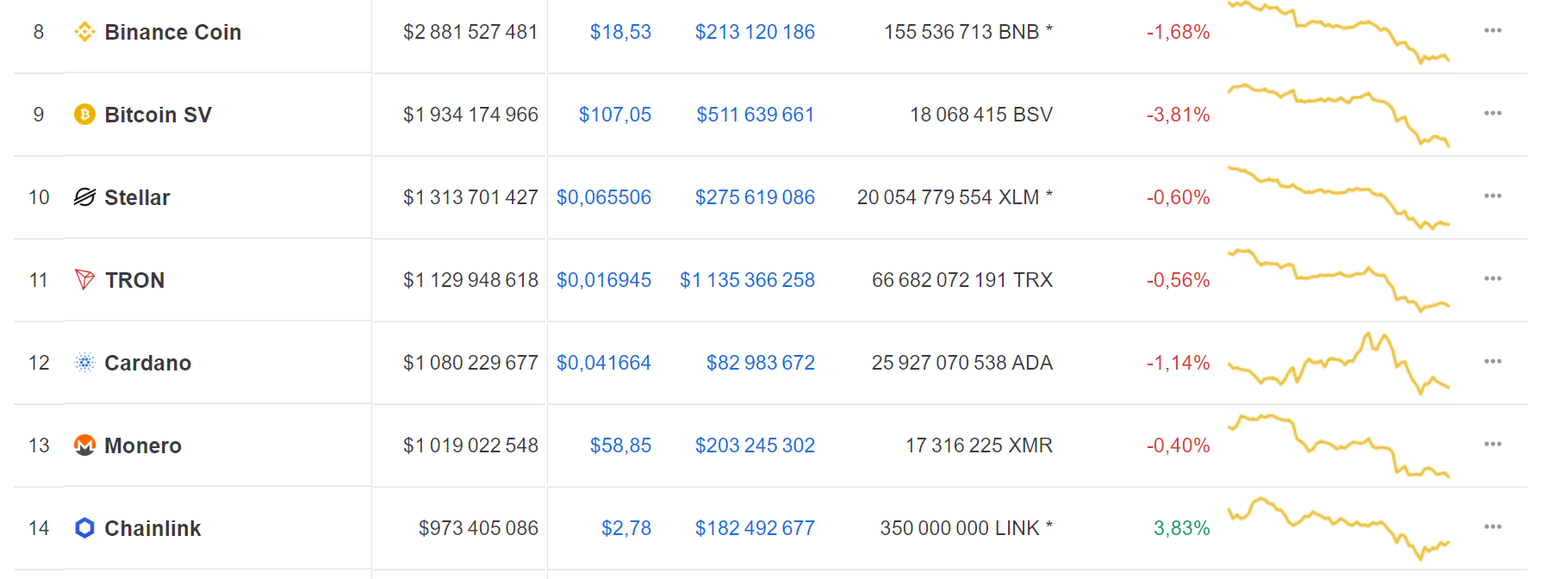
La cryptomonnaie est cryptée et peut être utilisée uniquement par les personnes détenant le code de décryptage. Il peut s’agir d’un mot de passe, d’une empreinte digitale ou de tout autre élément permettant de s’identifier. Contrairement à la monnaie classique, les transactions sont très rapides, très peu couteuses et se font dans l’anonymat total. Grâce au système de cryptographie, les transactions ne peuvent pas non plus être falsifiées.



**Figure 5: Des possibilités technologiques révolutionnaires**

## Les différentes crypto-monnaies

Ci-dessous un classement des crypto-monnaies en fonction de leur valorisation boursière.



## Critères relatifs à notre projet

Nous nous basons sur des crypto-monnaies d’états en circulation.

Les critères de comparaisons seront les suivants :

* Plateforme : indique sur quelle blockchain la crypto-monnaie s’appuie
* Objectif : indique dans quel cadre la crypto-monnaie a été créée et quels sont les objectifs du projet
* Type blockchain : privée, publique ou de consortium
* Caractère social : indique si le projet pour lequel a été créé la crypto-monnaie est à but non lucratif



# Etude de l’existant

# L’environnement

## Openchain

En se basant sur les versions précédentes du projet, la blockchain choisie est Openchain.

### Fonctionnement

Openchain est une technologie de blockchain open source, ou plutôt chaîne de transaction. En effet, Openchain n’utilise pas le concept de block vu plus haut, les transactions sont directement groupées entre elles et non via des blocks. Cela permet de gagner en temps et les transactions sont validées en (quasi) temps réel.

**Caractéristiques propres à Openchain :**

* Validation instantanée des transactions
* Pas de frais de minage
* Scalabilité extrêmement élevée
* Sécurisé via signatures numériques
* Immutabilité ***(1)***
* Attribution d’alias aux utilisateurs au lieu d'utiliser des adresses en base 58
* Plusieurs niveaux de contrôle :
  + Un registre entièrement ouvert pouvant être rejoint anonymement
  + Les participants doivent être approuvés par l'administrateur
  + Certains utilisateurs jouissent de plus de droits que les utilisateurs anonymes
* Système de hiérarchie
* Transparence des transactions
* Gestion de la perte ou du vol de clés privées pour les utilisateurs finaux
* Possibilité d'avoir plusieurs instances d'Openchain

***(1) Engager une ancre dans la blockchain Bitcoin à l'irréversibilité de sa PoW***

### API

Le serveur Openchain expose une API HTTP pouvant être utilisée pour interagir avec les données. L'URL d'une opération est construite à partir de l'URL de base du nœud final et du chemin d'accès relatif de l'opération.

Par exemple, si l'URL de base est https://www.openchain.org/endpoint/, pour appeler l'opération/record (interroger un enregistrement), l'URL complète sera <https://www.openchain.org/endpoint/record> .

**Quelques opérations utiles :**

* Soumettre une transaction (/submit)
* Interroger un enregistrement (/record)
* Flux de transactions (/stream)
* Récupérer les informations sur la chaîne (/info)
* Interroger un compte (/query/account)
* Interroger une transaction (/query/transaction)
* Interroger une version spécifique d'un enregistrement (/query/recordversion)
* Interroger toutes les mutations ayant affecté un enregistrement (/query/recordmutations)
* Interroger les enregistrements dans un compte et ses sous-comptes (/query/subaccounts)
* Interroger tous les enregistrements avec un type et un nom donné (/query/recordsbyname)

Dans ce projet, le traitement des requêtes HTTP venant du client AngularJS passe par une API Restful constituée de :

1. Un serveur avec Node.js et le framework Express.js

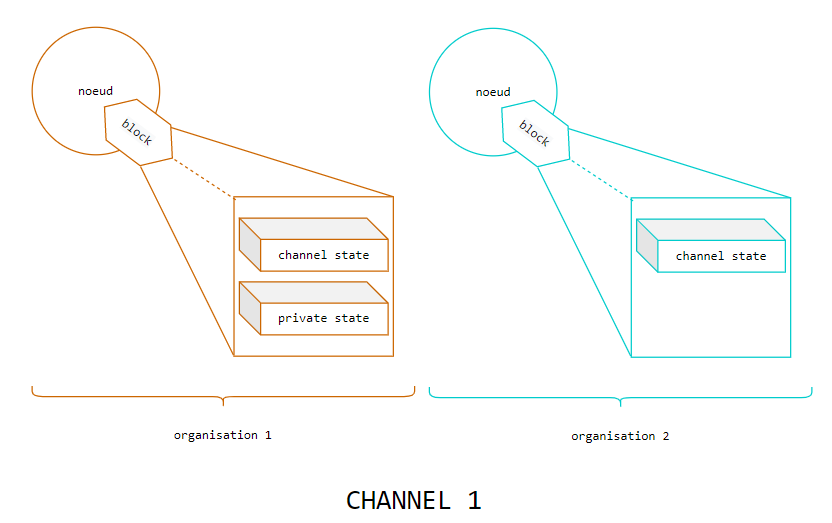
2. Une base de données MySQL

### Hyperledger Fabric, une alternative à Openchain

#### Concepts

Hyperledger Fabric est une blockchain Open Source, extrêmement modulaire, proposée par la Linux Foundation et spécialement conçue pour un usage privé et professionnel. Elle s’organise autour de plusieurs concepts :

* Organisation : acteur de la chaîne
* Noeud : un nœud du réseau, appartient à une organisation qui est chargée de maintenir son fonctionnement
* Brick : chargée d’organiser la vie du réseau
* Channel : « sous blockchain » dans laquelle sont inscris les blocks en fonction du sujet
* CA : brick chargée de vérifier les certificats
  + Ajouter des identités
  + Générer des certificats
  + Renouveler ou révoquer des certificats
* Blocks cachés (private data) : permet de créer des données privées dans un channel au lieu de créer un nouveau channel, on peut donc partager un même channel entre plusieurs organisations
* Cycle de vie du Chaincode



**Figure 6 : Schématisation d'un bloc caché**

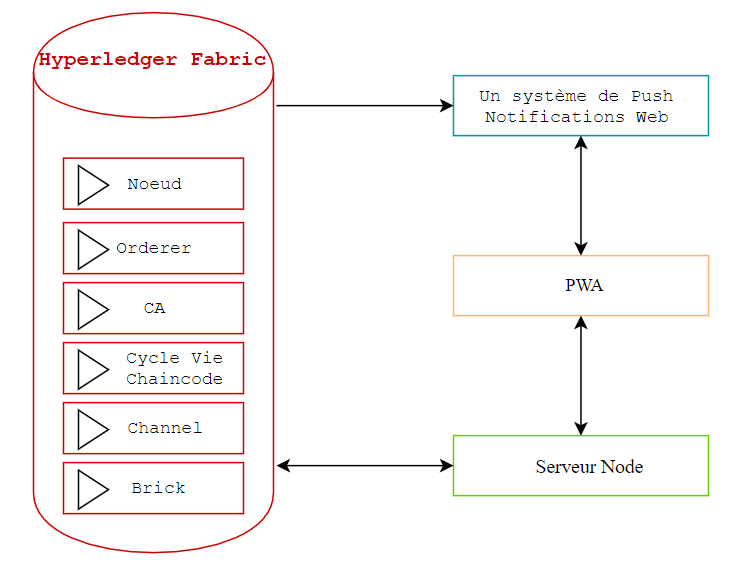
#### Architecture



**Figure 7 : Architecture Hyperledger Fabric**

A la différence de OpenChain, Hyperledger Fabric contient un « bloc » contenant les états finaux de chaque objet afin d’alléger la charge d’un bloc (contient tout les fichiers, transactions, etc.)

#### Architecture du PoC



**Figure 8 : Fonctionnement PoC**

Le POC est composé de différents éléments :

* Une instance Hyperledger vierge
* Un server Node.js
* Un système de Push Notifications Web
* Une PWA

#### Conclusion

Hyperledger Fabric semble convenir parfaitement à ce que nous voulons dans notre projet. De plus, elle permet d’implémenter plus facilement la partie mobile puisqu’elle interagie déjà avec une PWA.

Dans notre cas la blockchain est déjà implémentée et le temps imparti ne nous permet pas de changer de technologie. Or, elle serait intéressante à mettre en place dans une future version de l’application.

## MySQL – API REST NodeJs – Angular 7

Les détails des environnements utilisés sont disponibles en [Annexe : Documentation Technique de l’environnement existant](Annexes.docx)

# Les fonctionnalités existantes

Les détails des fonctionnalités existantes sont disponibles en [Annexe : Documentation Profil BRH](Annexes.docx)

# Les Améliorations

# L’application Web (PWA)

# Webographie

* <https://blockchainfrance.net> , Blockchain France
* [https://docs.openchain.org/](https://docs.openchain.org/en/latest/index.html) , documentation OpenChain
* [https://hyperledger-fabric.readthedocs.io/](https://hyperledger-fabric.readthedocs.io/en/release-1.4/) , documentation Hyperledger Fabric