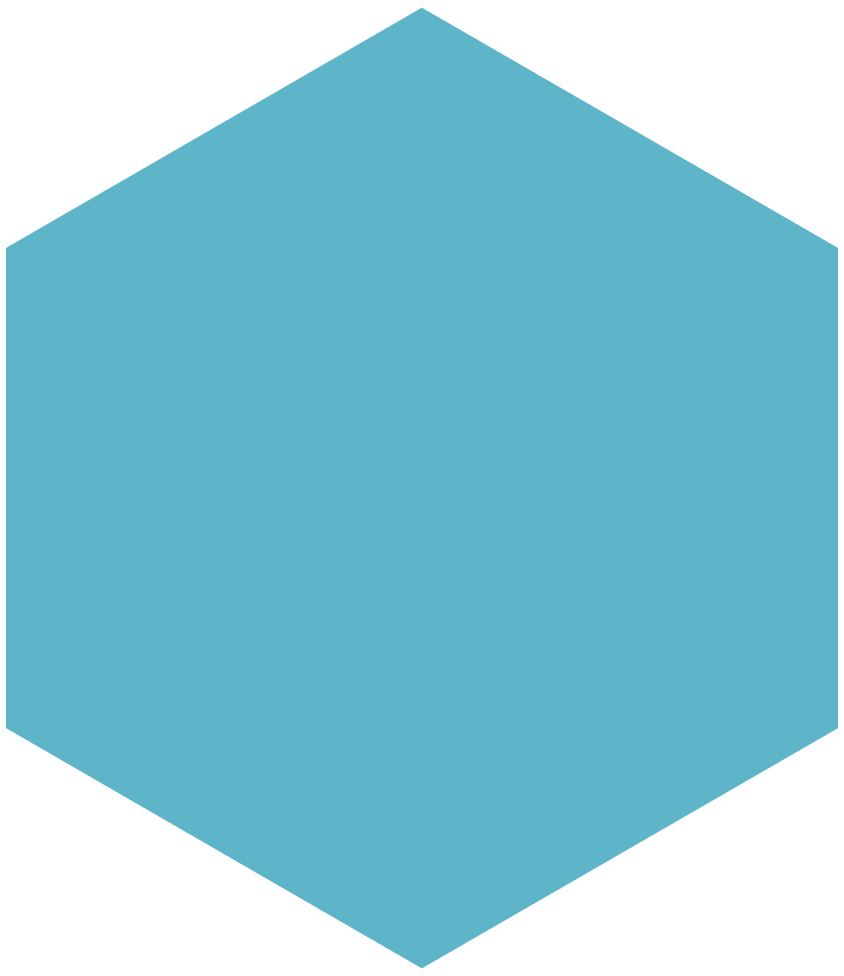


Digital HaïTian Gourde



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 2](#_Toc31181970)

[II. Etat de l’art 2](#_Toc31181971)

[1) La blockchain 2](#_Toc31181972)

[A. Définition 3](#_Toc31181973)

[B. Les règles de consensus 3](#_Toc31181974)

[C. Les types de blockchains 4](#_Toc31181975)

[1. PUBLIQUE 4](#_Toc31181976)

[2. PRIVE ("DISTRIBUTED LEDGER TECHNOLOGY" (DLT)) 4](#_Toc31181977)

[D. Critères relatifs à notre projet 6](#_Toc31181978)

[2) La crypto-monnaie 6](#_Toc31181979)

[A. Définition 6](#_Toc31181980)

[B. Les différentes crypto-monnaies 7](#_Toc31181981)

[C. Critères relatifs à notre projet 7](#_Toc31181982)

[III. Etude de l’existant 8](#_Toc31181983)

[1) L’environnement 8](#_Toc31181984)

[A. Openchain 8](#_Toc31181985)

[1. Fonctionnement 8](#_Toc31181986)

[2. API 9](#_Toc31181987)

[3. Hyperledger Fabric, une alternative à Openchain 9](#_Toc31181988)

[B. MySQL – API REST NodeJs – Angular 7 11](#_Toc31181989)

[2) Les fonctionnalités existantes 11](#_Toc31181990)

[IV. Les Améliorations 12](#_Toc31181991)

[A. Sécurité 12](#_Toc31181992)

[V. Dockerisation 12](#_Toc31181993)

[VI. Webographie 12](#_Toc31181994)

# Introduction

La monnaie nationale d’Haïti, la gourde (HTG), de nature très volatile et en dépréciation continue depuis les vingt dernières années le gouvernement Haïtien en collaboration avec la Banque de la République d’Haïti (BRH) cherchent une solution pour relancer l’économie du pays.

La solution proposée par le projet Digital Gourde (DHTG), est la mise en place d’une cryptomonnaie d’état du même nom qui sera gérée, supervisée et distribuée par la BRH et mis à disposition des institutions financières locales.

Les objectifs à long terme du projet sont de :

1. Réduire puis supprimer le coût de fabrique et d’importation de la monnaie physique

2. Permettre aux personnes non-bancarisées d’Haïti de l’être, sans risques pour les institutions financières

3. Augmenter le taux de change de la monnaie nationale pour combler le déficit financier du pays

L’avantage majeur de l’utilisation des cryptomonnaies dans un cas tel que celui-ci est que la création de la monnaie est instantanée et sans frais. Aussi, chaque opération utilisant cette monnaie (distribution, paiement, virement, etc.) aura un coût extrêmement faible et sera instantanée étant donné que la blockchain sur laquelle elle se base utilise une architecture client-serveur plutôt qu’un système de Proof of Work, contrairement aux cryptomonnaies tels que le Bitcoin.

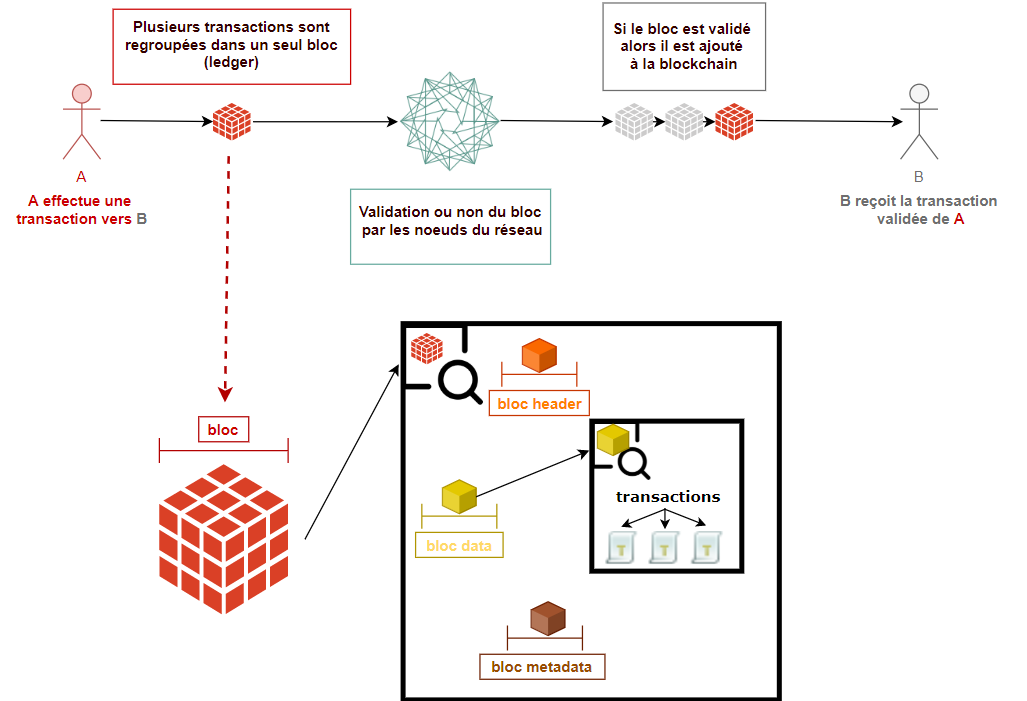
# Etat de l’art

# La blockchain

## Définition

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

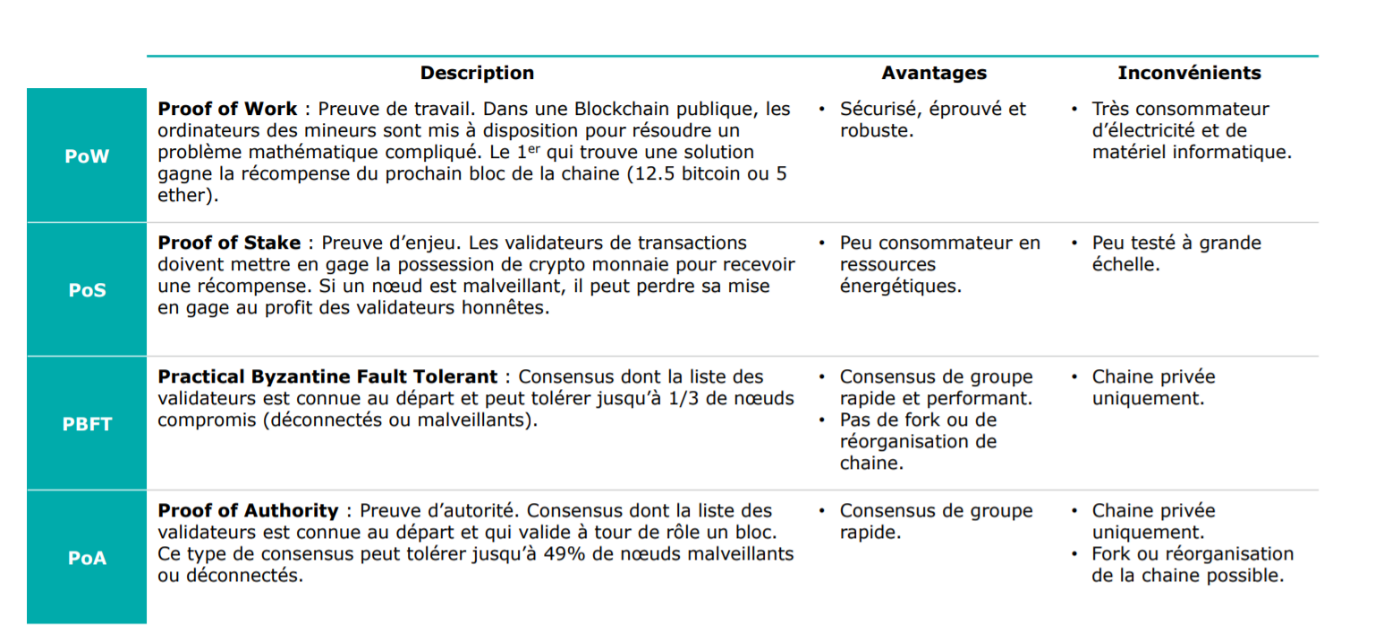
*Par extension, une blockchain constitue une base de données qui contient l’historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun 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 règle de la majorité ne s’impose pas. La lecture des blocs est publique, réservée aux participants ou hybride. Ce type de blockchain est principalement utilisé dans le secteur bancaire.

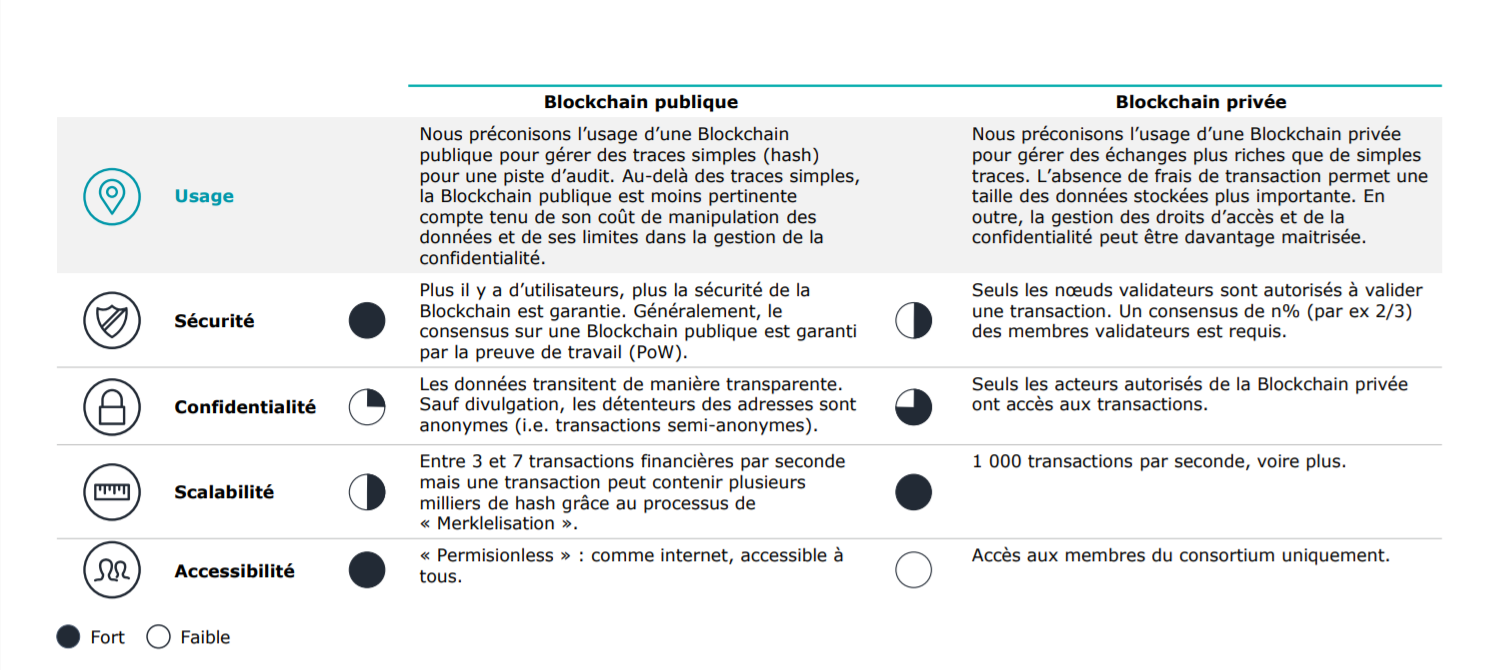
Exemples : R3 (banques), EWF (énergie), B3i (assurance), Corda.

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

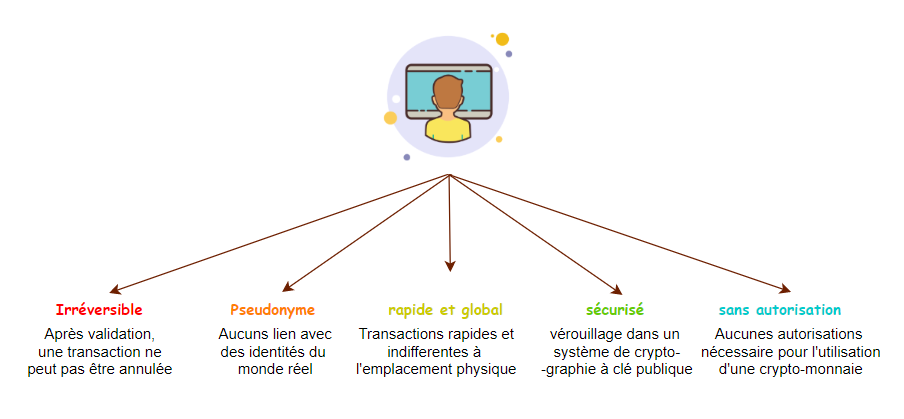
## Définition

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 ?**

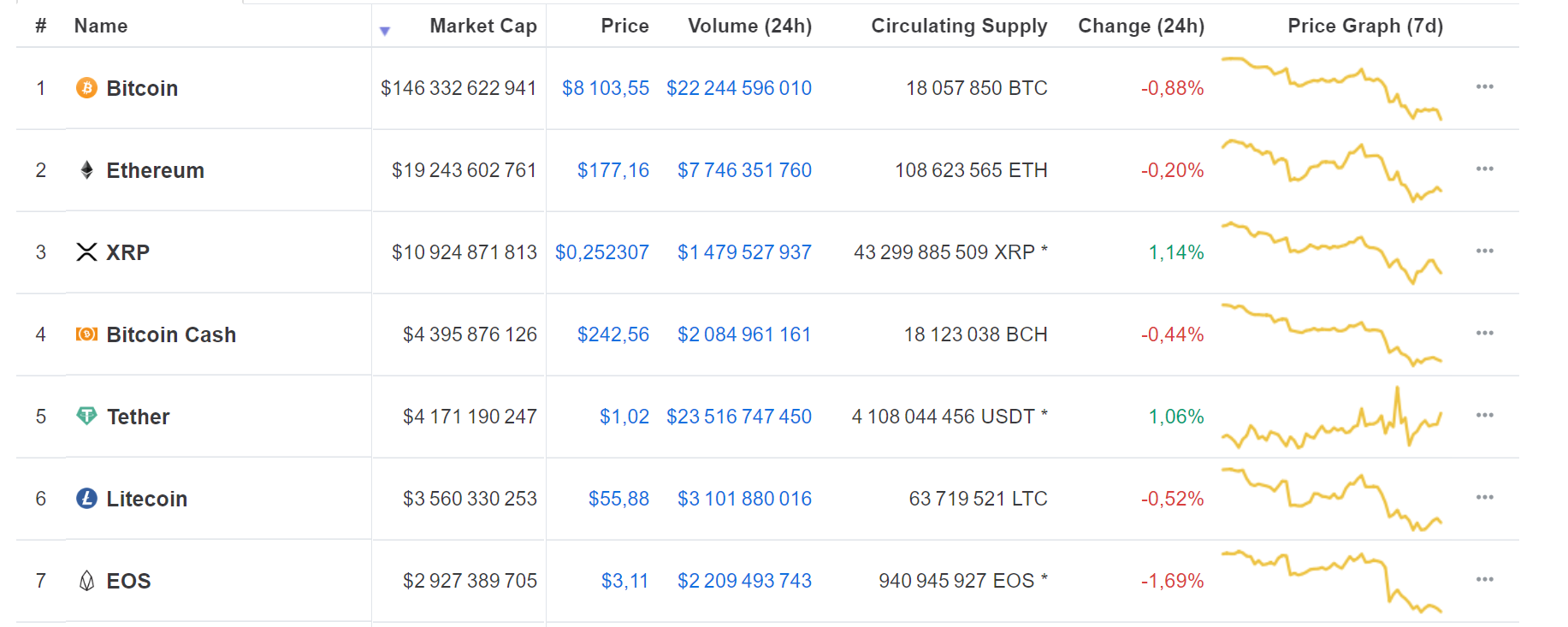
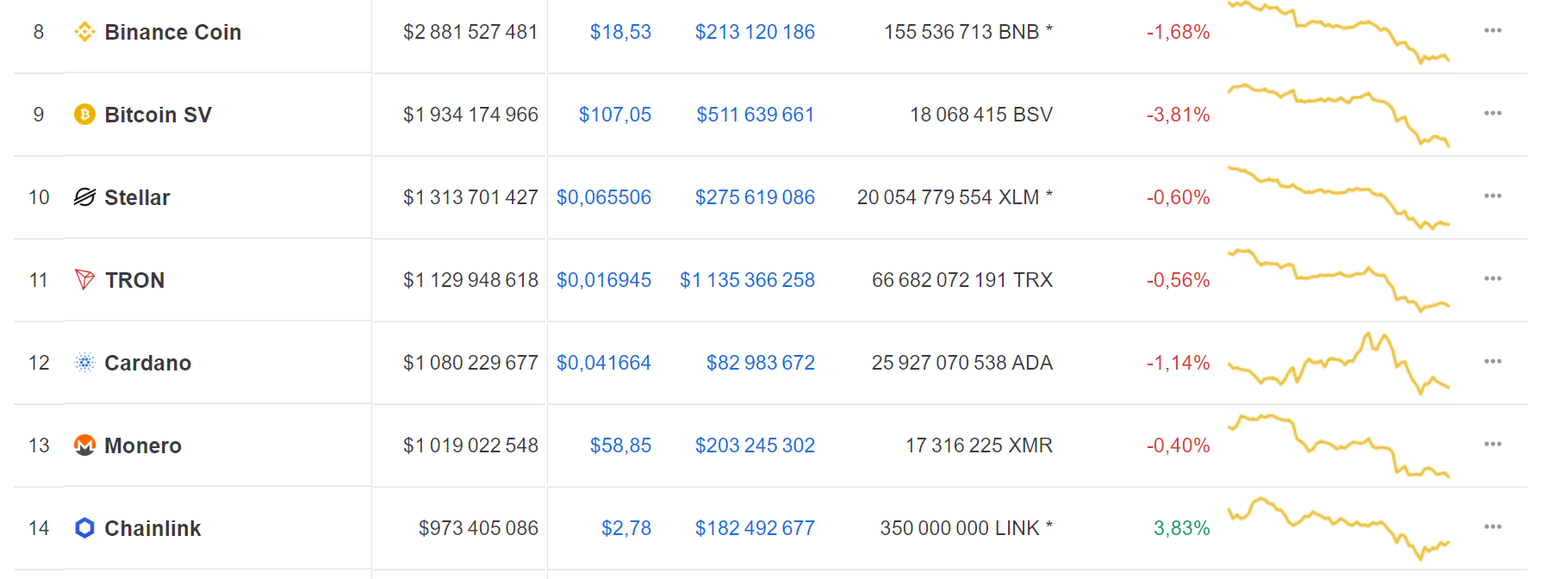
La cryptomonnaie est cryptée et peut être utilisée uniquement par les personnes détenant le code de décryptage. Il peut s’agir d’un mot de passe, d’une empreinte digitale ou de tout autre élément permettant de s’identifier. Contrairement à la monnaie classique, les transactions sont très rapides, très 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 bloc vu plus haut, les transactions sont directement groupées entre elles et non via des blocs. 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

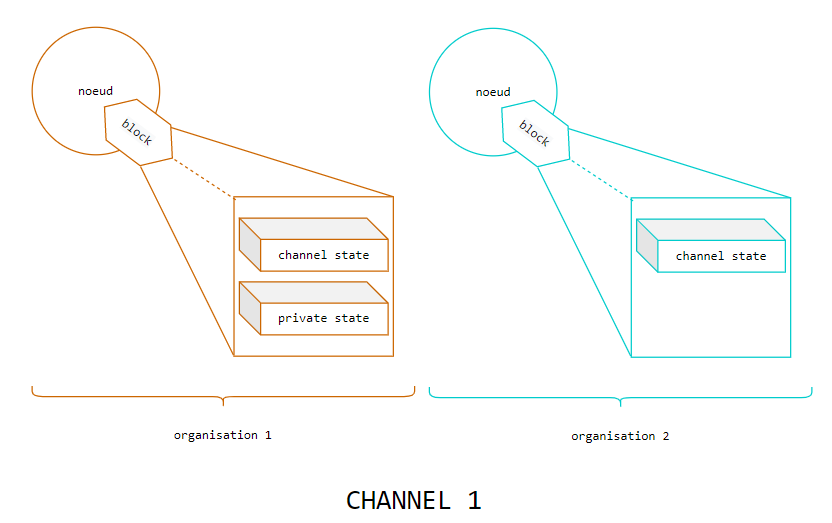
2. Une base de données MySQL

### 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 blocs en fonction du sujet
* CA : brick chargée de vérifier les certificats
  + Ajouter des identités
  + Générer des certificats
  + Renouveler ou révoquer des certificats
* Blocs 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**

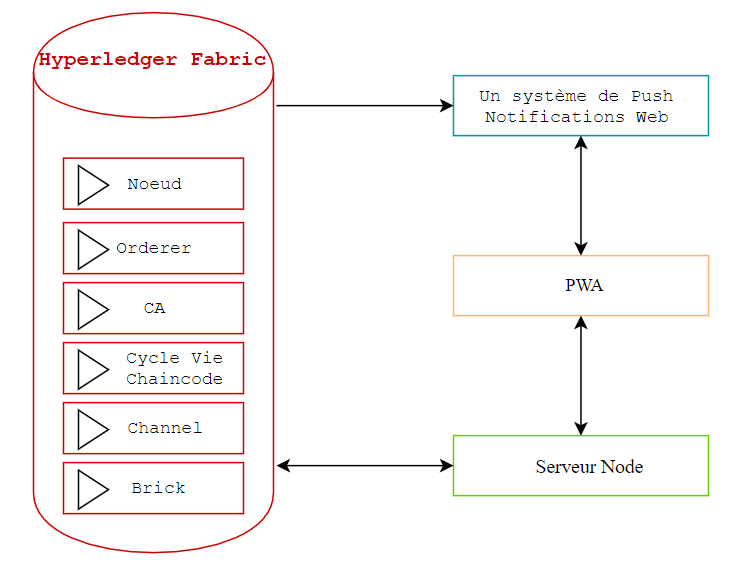
#### Architecture



**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 tous 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.

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

## Profil BRH

## Profil Particulier

## Profil Commerçant

## Profil Institutions Financières

# Les Améliorations

# Sécurité

Dans l’application existante, un seul portail permet d’accéder à la fois à l’espace administrateur et particulier/commerçant.

En séparant les deux interfaces on assure une première couche de protection.

url*/portail : espace particuliers*

url*/brh/accueil : espace BRH*

# Client Web et mobile

Afin d’optimiser au mieux le temps de développement de la solution, ainsi que le coût de développement, nous avons décidé d’utiliser le framework « Flutter » qui nous permet de développer une seule application qui sera utilisable sur tous les supports (Client Web, mobile, tablette, …).

Le design initial de l’application ne permettait pas une expérience utilisateur satisfaisante, d’une part sur l’application web, et une quasi non-utilisation sur des appareils mobile.

Dans un premier temps, nous développerons les fonctionnalités de base sur Flutter pour permettre de tester son utilisation.

## Framework Flutter

Flutter, est un Framework open source développé par Google qui a pour objectif de rassembler les points fort de nombreux outils existants. Flutter se fait connaître pour sa capacité à concevoir des applications natives multiplateforme (Android, IOS, Windows, Mac, Linux).

## Langage Dart

Ce langage « oublié » a comme principale avantage d’offrir deux modes de fonctionnement

* AOT (Ahead Of Time)
* JIT (Just In Time)

### AOT

Dart permet de générer une application native pour chaque plateforme. Le code est donc optimisé pour l’architecture sur laquelle il fonctionne.

### JIT

Dart propose la fonctionnalité de Hot Reaload qui permet de réduire considérablement le temps de développement. En effet, le principe de Hot Reload est de réduire le temps entre chaque build, qui est relativement long quand l’on développe une application Android native. On passe donc à quelques millisecondes (pire des cas) entre chaque build.

De plus Dart est performant pour gérer les allocations mémoire et le « Garbage collector ».

# Dockerisation

Après avoir récupérer le projet nous avons rencontré de nombreuses difficultés à le faire fonctionner. La solution la plus simple est donc de le dockeriser.

Avantages :

* L’application est isolée
* Possibilité de création d’un réseau de containers
* Léger
* Lancement de l’application simplifié

# 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
* <https://flutter.dev/> , site web officiel de Flutter