Table des matières

Déclaration i
Remerciements ii
Résumé iii
1. Introduction 1
2. Blockchain 2
2.1 Définition 2
2.2 Fonctionnement 2
2.2.1 Structure 2
2.2.1.1 Transaction 3
2.2.1.2 Bloc 3
2.2.1.3 Nœud 3
2.2.2 Lien entre les blocs 3
2.2.3 Cryptographie asymétrique 3
2.2.3.1 Clé privée 4
2.2.3.2 Clé publique 4
2.2.3.3 Adresse 4
2.2.3.4 Vérification 4
2.2.4 Création et validation des nouveaux blocs 4
2.2.4.1 Preuve de travail 5
2.2.4.2 Preuve d'enjeu 5
2.3 Types de blockchain 6
2.3.1 Blockchain publique 6
2.3.2 Blockchain privée - gouvernance centralisée 6
2.3.3 Blockchain privée – consortium 7
2.4 Avantages sur une base de données classique 7
2.4.1 Immutabilité 7
2.4.2 Absence d'organe de contrôle centralisé 7
2.4.3 Transparence 7
2.4.4 Jetons de valeur 8
2.4.5 Horodatage des blocs 8
2.5 Inconvénients par rapport à une base de données classique 8
2.5.1 Taille des informations stockées 8
2.5.2 Délai de validation 9
2.5.3 Impact écologique 9
2.6 Ethereum 9
2.6.1 Spécificités 9
2.6.1.1 Smart contract 9
2.6.1.2 Gaz 10
2.6.2 Exécution 10

2.6.2.1 Algorithme de consensus 10
2.6.2.2 Ethereum Virtual Machine 10
2.7 Synthèse 11
3. Applications possibles pour l'industrie de la mode 12
3.1 Applications orientées produit 12
3.1.1 Authentification du produit et identification de son propriétaire 13
3.2 Applications orientées production 14
3.2.1 Provenance des matières premières et suivi de la chaîne d'approvisionnement 15
3.3 Applications orientées distribution 17
3.3.1 Restriction de la duplication d'une œuvre numérique 17
3.4 Applications orientées créateur 19
3.4.1 Protection et rémunération des créateurs 19
3.5 Synthèse 20
4. Solution 21
4.1 Concept 21
4.2 Fonctionnement 21
4.2.1 Fonctionnement général 21
4.2.2 Webapp 21
4.2.2.1 Point d'entrée 22
4.2.2.2 Communication avec le smart contract 22
4.2.2.3 Frameworks 22
4.2.3 Smart Contract 23
4.2.3.1 Données 23
4.2.3.2 Contraintes 23
4.2.3.3 Constructeur 24
4.2.3.4 Fonctions 24
4.2.3.4.1 printArtwork 24
4.2.3.4.2 getArtwork 24
4.2.3.4.3 getArtworks 24
4.2.3.5 Instances 25
4.2.4 Ganache-cli 25
4.2.5 Architecture 25
4.3 Déploiement 26
4.3.1 Sur la blockchain Ethereum principale 26
4.3.2 Sur une blockchain Ethereum privée 26
5. Conclusion 28
Bibliographie 30
Annexe 1 : Documentation développeur 34
1. Installation 34
1.1 Prérequis 34

1.2 Installation du nœud Ethereum 34
1.3 Déploiement du smart contract 35
1.4 Lancement de la webapp 37
1.5 Tester la webapp 39
1.5.1 Insérer une nouvelle œuvre 41
2. Structure de la webapp 42
2.1 Répertoire *class* 42
2.1.1 apparel 42
2.1.2 artwork 42
2.1.3 order 42
2.1.4 ordermanager 42
2.1.5 smartcontract 42
2.1.6 const.js 42
2.2 Répertoire *config* 42
2.2.1 config.json 42
2.3 Répertoire data 42
2.3.1 orders.txt 43
2.4 Répertoire *node*_modules 43
2.5 Répertoire *ressources* 43
2.5.1 router.js 43
2.6 Répertoire *views* 43
2.7 package.json 43
2.8 server.js 43
3. Diagrammes 43
Annexe 2 : Glossaire 45
1. Vocabulaire spécifique à l'industrie de la mode 45
2. Vocabulaire spécifique à la technologie blockchain 45

Liste des tableaux

Tableau 1 : Différences call - send 22

Liste des figures

Figure 1 : Structure d'une blockchain 2
Figure 2 : Lien entre les blocks 3
Figure 3 : Validation des blocs par les nœuds du réseau 5
Figure 4 : Blockchain publique - relations entre les nœuds 6
Figure 5 : Blockchain privée avec gouvernance - relations entre les nœuds 6
Figure 6 : Blockchain privée de consortium - relations entre les nœuds 7
Figure 7 : Projet blockchain de Martine Jarlgaard et Provenance 16
Figure 8 : Publicité de la collaboration Kaws - Uniqlo 18
Figure 9 : Représentation de la structure Artwork 23
Figure 10 : Modificateur du smart contract 23
Figure 11 : Constructeur du smart contract 24
Figure 12 : Fonction printArtwork 24
Figure 13 : Fonction getArtwork 24
Figure 14 : Fonction getArtworks 25
Figure 15 : Architecture générale de la solution 25
Figure 16 : Architecture de la solution dans une blockchain publique 26
Figure 17 : Architecture de la solution dans une blockchain privée 27

Liste des figures - Annexe 1 : Documentation développeur

Figure 18 : Installation de ganache 34
Figure 19 : Lancement de ganache-cli 35
Figure 20 : Page d'accueil de Remix 35
Figure 21 : Importer un smart contract 36
Figure 22 : Onglet des plugins 36
Figure 23 : Compiler le smart contract 36
Figure 24 : Modifier l'environnement 37
Figure 25 : Déployer le smart contract 37
Figure 26 : Copier l'adresse du smart contract 38
Figure 27 : Copier l'adresse du compte 38
Figure 28 : Fichier des constantes 38
Figure 29 : Démarrage de la webapp 39
Figure 30 : Page d'accueil 39
Figure 31 : Page des produits 40
Figure 32 : Page de personnalisation 40
Figure 33 : Page de confirmation 41
Figure 34 : Fonction AddArtwork dans Remix 41
Figure 35 : Diagramme des dépendances de *server.js* 43
Figure 36 : Diagramme des dépendances de smartcontract.js 44
Figure 37 : Diagramme des dépendances de router.js 44

Liste des tableaux - Annexe 2 : Glossaire

Tableau 2 : Vocabulaire spécifique à l'industrie de la mode..... 45
Tableau 3 : Vocabulaire spécifique à la technologie blockchain 45

1. Introduction

Le 3 janvier 2009, le premier bloc du réseau Bitcoin est créé par Satoshi Nakamoto (pseudonyme). 6 jours plus tard, cette même entité publie la première version du logiciel Bitcoin sur le site SourceForge.net. La première cryptomonnaie est née, et, avec elle, la première chaîne de blocs décentralisée.

Premièrement utilisée, pour Bitcoin, dans le but de créer une monnaie qui ne soit pas régulée par un unique organisme tel qu'une banque centrale, la technologie blockchain est de plus en plus utilisée à d'autres fins et dans d'autres domaines. Parmi ceux-ci, l'industrie de la mode.

Qu'il s'agisse de luxe ou de prêt-à-porter, les marques doivent s'adapter à de nombreux changements au fil des ans, dont les innovations technologiques. L'arrivée d'internet et particulièrement de l'e-commerce en est un très bon exemple. Cette révolution a progressivement modifié les habitudes des consommateurs, obligeant les marques à adapter et diversifier leurs canaux de vente, mais aussi de communication et de marketing.

Au sein de cet intérêt croissant de la mode pour les nouvelles technologies, certains acteurs commencent à s'intéresser à la blockchain qui comporte de nombreux avantages pour ce secteur. Comme l'affirme Nathan Pacer, créateur de Venture Scanner, une entreprise spécialisée dans la recherche et l'innovation, la Blockchain repose essentiellement sur la preuve de l'exclusivité et de la lutte contre la contrefaçon, des domaines importants pour la mode.[1]

Ce travail se penchera donc sur les possibilités que l'intégration d'une blockchain dans les différents secteurs de l'industrie de la mode peut permettre. Après un tour d'horizon des applications possibles, une solution informatique reprenant certains concepts étudiés sera développée et détaillée afin d'étayer les propos de ce travail.

Cette solution consistera en une application web permettant de personnaliser un vêtement à l'aide d'une œuvre (photographie ou peinture). La plateforme communiquera avec un smart contract dont le rôle est de limiter le nombre d'impression de chaque œuvre.

[1] 6 ways blockchain is changing luxury - https://www.voguebusiness.com/technology/6-ways-blockchain-changing-luxury

2. Blockchain

Bien que la notion de blockchain soit relativement connue, son fonctionnement, lui, n'est pas toujours bien compris de tous. Commençons par nous demander ce qu'est une blockchain.

2.1 Définition

Lors d'une conférence en décembre 2016, Claire Balva, présidente de Blockchain France, donnait la définition suivante :

> *« La Blockchain est une technologie de stockage et de transmission d'information qui est sécurisée, transparente et qui fonctionne sans organe central de contrôle. »*[2]

Une blockchain permet théoriquement à deux entités ne se connaissant pas de se faire confiance sans l'intervention d'un tiers.

Dans ce système, l'intégrité des données n'est plus assurée par un organe central mais par des techniques cryptographiques sur lesquelles nous reviendrons.

2.2 Fonctionnement

Il existe de nombreux protocoles de blockchain différents. Certains concepts varient d'un protocole à un autre. À ce titre, cette section explique le fonctionnement global d'une blockchain.

2.2.1 Structure

Comme son nom l'indique, une blockchain est une suite de blocs. Chaque bloc connait son prédécesseur, formant ainsi une chaine.

Figure 1 : Structure d'une blockchain

(Source : Blockchain France [en ligne]. [Consulté le 6 octobre 2019]. Disponible à l'adresse : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/)

[2] Conférence TEDx Talks de Claire Balva, Lyon, 2 décembre 2016

Rapport-Gratuit.com

2.2.1.1 Transaction

Une transaction est un échange entre deux utilisateurs du réseau. Elle est identifiable par son hash, calculé à partir des données qu'elle contient. Ce hash est l'empreinte unique de la transaction.

2.2.1.2 Bloc

Un bloc est un regroupement de transactions crée tous les *t* temps (*t* varie suivant le protocole de blockchain). En plus des transactions, il contient une date de création et une référence au bloc précédent.

2.2.1.3 Nœud

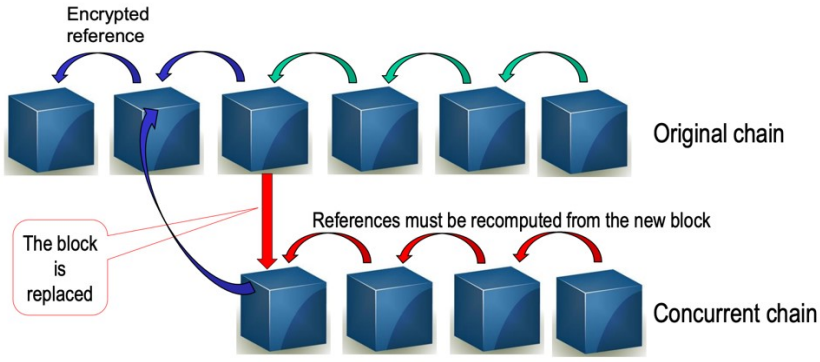
Les nœuds sont les utilisateurs du réseau qui créent et valident les nouveaux blocs. Leur rôle est également de veiller à l'intégrité de la chaîne. Ils possèdent tous une copie complète de la chaîne.

2.2.2 Lien entre les blocs

Chaque bloc possède une signature qui est obtenue par le biais d'une fonction de hachage appliquée à l'ensemble du contenu du bloc. Le résultat obtenu est une valeur à taille fixe. Si le contenu du bloc est modifié, ne serait-ce que très légèrement, sa signature, elle, devient totalement différente.

Un bloc est lié à son prédécesseur via la signature de celui-ci. Par conséquent, si le premier bloc est modifié, sa signature aussi et les blocs suivants doivent tous être recalculés afin de ne pas casser la chaîne.

Figure 2 : Lien entre les blocks



(Source : Dugerdil, Introduction – Principles of Blockchain Architecture [Document PDF]. [Consulté le 14 octobre 2019])

2.2.3 Cryptographie asymétrique

Afin de vérifier l'identité de l'émetteur d'une transaction, la blockchain utilise une paire de clés. Celles-ci permettent de générer une signature numérique unique.

2.2.3.1 Clé privée

Elle est connue uniquement de son propriétaire et ne doit pas être partagée. Elle permet, via des techniques cryptographiques, de créer la clé publique.

2.2.3.2 Clé publique

La clé publique est connue de tous les autres utilisateurs. Elle est générée à partir de la clé privée et à l'aide de la cryptographie asymétrique ce qui veut dire qu'il est impossible d'obtenir la clé privée à partir de la clé publique.

2.2.3.3 Adresse

L'adresse d'un utilisateur est, elle, créée à partir du hash de sa clé publique. Elle est généralement plus courte que les clés car destinée à être manipulée par l'humain.

En conclusion l'utilisateur peut générer son adresse et sa clé publique à partir de sa clé privée mais pas inversement.

2.2.3.4 Vérification

Pour prouver qu'un utilisateur est bien à l'origine d'une transaction, ce dernier fournit une signature numérique unique générée à partir de sa clé privée et du contenu de la transaction. Les nœuds utilisent la clé publique de l'utilisateur pour vérifier la transaction.

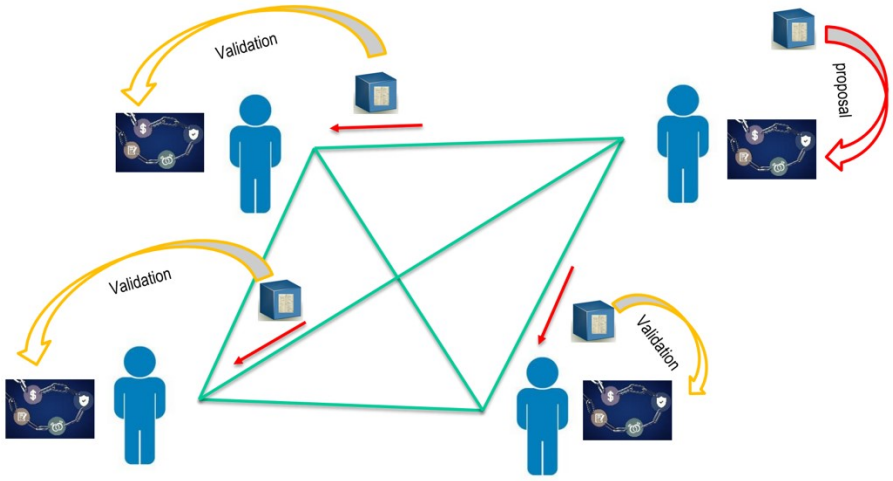
2.2.4 Création et validation des nouveaux blocs

La création de nouveaux blocs est effectuée par les nœuds du réseau. Ces derniers sont en compétition permanente pour insérer leur version d'un bloc et être récompensés en échange. Cette étape s'appelle le minage. Elle consiste en la résolution d'un problème arithmétique, appelé algorithme de consensus. La difficulté introduite par ce concept permet de décourager les nœuds malhonnêtes car cela devient coûteux pour eux d'insérer un bloc corrompu qui risque de ne pas être validé par le reste des nœuds.

Le premier nœud ayant résolu le problème propose son bloc aux autres utilisateurs qui le vérifient et le valident. Après cela le bloc est daté puis publié et ne peut plus être modifié. Les transactions qu'il contient deviennent effectives à ce moment-là.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Figure 3 : Validation des blocs par les nœuds du réseau



(Source : Dugerdil, Introduction – Principles of Blockchain Architecture [Document PDF]. [Consulté le 14 octobre 2019])

L'algorithme de consensus n'est pas le même pour tous les protocoles de blockchain. Nous allons nous intéresser à leurs spécificités. Les principaux algorithmes sont les suivants :

- Algorithme de preuve de travail
- Algorithme de preuve d'enjeu

2.2.4.1 Preuve de travail

La preuve de travail repose sur la résolution d'un problème mathématique. Chaque mineur tente de le résoudre et seul le premier à y parvenir peut ensuite insérer le bloc dans la chaîne. Ce problème mathématique ne peut être résolu qu'en essayant toutes les possibilités ce qui veut dire que plus un mineur possède de puissance de calcul, plus il a de chance de réussir avant les autres. De plus, le problème se complexifie avec le temps. Cela entraîne donc une inévitable course à la puissance de calcul. Pour Bitcoin par exemple, la puissance nécessaire est maintenant telle que miner à l'aide d'un simple ordinateur équipé d'une carte graphique ne suffit largement plus. Au-delà du coup de l'équipement, cet algorithme de consensus pose un réel problème écologique et la validation prend énormément de temps.

2.2.4.2 Preuve d'enjeu

La preuve d'enjeu, elle, ne repose pas sur la puissance de calcul. Avec cette méthode, le mineur doit prouver qu'il est en possession d'un certain nombre de tokens. Cela vise à démontrer l'investissement du mineur dans la blockchain en partant du principe qu'un acteur investi dans un protocole n'a pas intérêt à ce que ce dernier soit corrompu. Plus

le mineur possède de token, plus il a de chances de se voir attribuer un bloc à miner. Pour éviter un effet de centralisation, c'est-à-dire que le plus riche mine la majorité des blocs, une pondération est mise en place dont les critères varient suivant la chaîne de blocs.

2.3 Types de blockchain

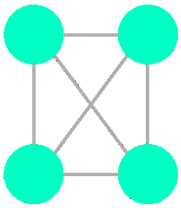
Il existe plusieurs types de blockchain voués à différents cas d'utilisation.

2.3.1 Blockchain publique

Une blockchain peut être public, comme le sont les protocoles les plus connus tel Bitcoin. Dans ce cas, le registre est consultable par toute personne le désirant.

Une blockchain publique met en œuvre le principe de transparence.

Figure 4 : Blockchain publique - relations entre les nœuds

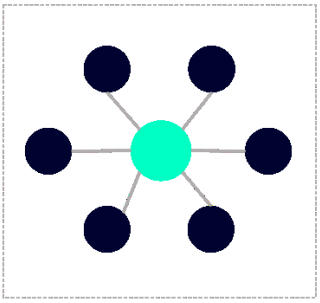


(Source : Blockchain privée : illusion ou innovation ? [en ligne]. [Consulté le 17 octobre 2019]. Disponible à l'adresse : https://medium.com/blocsnews/blockchain-priv%C3%A9e-illusion-ou-innovation-7bbedefa4b4e)

2.3.2 Blockchain privée - gouvernance centralisée

Dans cette configuration, les participants doivent avoir été acceptés par l'entité gouvernante. Le principe de base d'une blockchain, à savoir se passer d'un organe de contrôle, est ici bafoué. Ce type de blockchain est donc sujet à débat mais peut convenir à certains cas d'utilisation spécifiques.

Figure 5 : Blockchain privée avec gouvernance - relations entre les nœuds

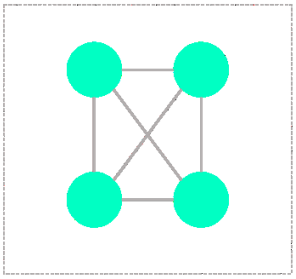


(Source : Blockchain privée : illusion ou innovation ? [en ligne]. [Consulté le 17 octobre 2019]. Disponible à l'adresse : https://medium.com/blocsnews/blockchain-priv%C3%A9e-illusion-ou-innovation-7bbedefa4b4e)

2.3.3 Blockchain privée – consortium

Ce type de blockchain définit un certain nombre de nœuds réputés comme fiables. Le schéma de la blockchain publique est appliqué mais uniquement à un nombre de participants restreint. Ce type de blockchain peut être utilisé pour les processus internes d'une entreprise afin de n'autoriser la lecture de la chaîne qu'aux collaborateurs de celle-ci.

Figure 6 : Blockchain privée de consortium - relations entre les nœuds



(Source : Blockchain privée : illusion ou innovation ? [en ligne]. [Consulté le 17 octobre 2019]. Disponible à l'adresse : https://medium.com/blocsnews/blockchain-priv%C3%A9e-illusion-ou-innovation-7bbedefa4b4e)

2.4 Avantages sur une base de données classique

2.4.1 Immutabilité

Dans un système blockchain, les nœuds du réseau détiennent tous une copie complète de la chaîne qu'ils mettent à jour au fil des nouveaux blocs. Si, pour une quelconque raison, un des nœuds partage une chaîne contenant un bloc modifié, la signature de ce bloc change également, ce qui casse le lien avec le bloc suivant car ce dernier ne connaît son prédécesseur que par sa signature. À ce moment, la copie de la chaîne n'est plus identique à celle des autres nœuds et est, de fait, considérée comme corrompue. Le principe d'immutabilité est ainsi assuré.

2.4.2 Absence d'organe de contrôle centralisé

Étant donné que les nœuds contrôlent la bonne évolution de la chaîne, le rôle qu'aurait un organe de contrôle unique au sein d'une base de données classique est ici délégué à l'ensemble des nœuds. Chaque nœud possédant une version de la chaîne identique à celle détenue par la majorité fait partie de l'autorité en vigueur.

2.4.3 Transparence

Le registre d'une blockchain étant ouvert, chacun peut le consulter.

Prenons l'exemple d'un portefeuille électronique et son solde. Ce solde représente l'addition ou la soustraction de toutes les transactions effectuées qui concernent

l'adresse du portefeuille. Étant donné que ces mouvements sont inscrits dans la blockchain, qui est consultable à souhait, le solde exact peut être vérifié en tout temps.

Ce principe s'applique uniquement aux blockchains publiques. Les blockchains privées recherchant logiquement l'objectif contraire dans un but précis.

2.4.4 Jetons de valeur

La blockchain introduit la notion de tokens ou jetons de valeur en français. En tant qu'unité de compte, le jeton est utilisé comme moyen de paiement au sein d'une blockchain.

Il permet de rémunérer les nœuds pour le minage des blocs qu'ils effectuent mais pas uniquement. Grâce à lui, il est possible d'effectuer des paiements de façon anonyme. Ces transactions peuvent être spontanées, par exemple, dans le cas d'un échange de bien physique contre une certaine somme en Bitcoin. Elles peuvent également être automatisées dans un smart contract où la transaction peut intervenir lorsque les conditions préalablement définies sont remplies. Nous reviendrons sur les smart contracts plus tard dans ce chapitre.

2.4.5 Horodatage des blocs

Chaque bloc inséré dans la blockchain est horodaté. Grâce au principe d'immutabilité évoqué précédemment, cette date représente donc une preuve qu'une transaction a été effectuée à l'instant T. On peut par exemple avoir la certitude qu'un fichier numérique existait bien à un certain moment. Nous y reviendrons plus en détails par la suite.

2.5 Inconvénients par rapport à une base de données classique

2.5.1 Taille des informations stockées

Comme évoqué précédemment, les nœuds détiennent tous une copie complète de la chaîne. Cette dernière est amenée à s'allonger au fil du temps et de l'arrivée des nouveaux blocs. La chaîne est donc de plus en plus lourde et cela a un impact sur les performances du réseau.

Dans une base de données classique, la capacité de stockage dépend simplement de l'espace alloué et les performances ne sont que très peu affectées par la taille des données.

Une blockchain ne peut donc pas stocker de gros fichiers mais uniquement des écritures élémentaires.

2.5.2 Délai de validation

Une transaction n'est effective que lorsque le bloc le contenant a été miné puis validé par le reste du réseau. Il y a donc un délai. Celui-ci dépend de la blockchain et de l'encombrement du réseau.

2.5.3 Impact écologique

Les blockchains, et particulièrement celles qui utilisent la preuve de travail comme algorithme de consensus, sont extrêmement gourmandes en énergie. La complexité du minage augmente avec le temps, entraînant l'inévitable course à la puissance de calcul évoquée précédemment. Dans une époque où la question du réchauffement climatique est omniprésente, les protocoles qui utilisent ce type de validation doivent évoluer afin de prendre tout leur sens. C'est le cas d'Ethereum que nous allons étudier en détail.

2.6 Ethereum

2.6.1 Spécificités

La technologie Ethereum possède une base semblable à celle de Bitcoin mais utilise l'Ether comme token et introduit de nouvelles notions intéressantes détaillées ci-dessous. J'ai choisi de m'intéresser plus particulièrement à ce protocole car il est à mon sens un des plus aboutis.

2.6.1.1 Smart contract

Un smart contract est un programme, une suite d'instructions permettant d'interagir avec la blockchain Ethereum. Il est exécuté automatiquement par les nœuds du réseau lorsqu'une nouvelle transaction le concernant apparaît.

Sa première particularité est de ne pas pouvoir être modifié une fois publié sur le réseau Ethereum. Grâce à cela, les différents partis s'assurent que les termes du contrat ne changent pas. Par conséquent, il est vital pour le développeur de traquer le moindre bug potentiel avant de publier son travail. Évidemment, ce dernier peut tester son code en local autant de fois qu'il le souhaite.

De cette première particularité en découle une seconde appelée couramment « Code is law » qui signifie que la seule autorité compétente à l'exécution du contrat est le code de ce dernier. Contrairement à un contrat classique où l'interprétation peut différer, par exemple, d'un juge à un autre dans le cas d'un désaccord à régler au tribunal, le smart contract, lui, s'exécute automatiquement même si le résultat de cette exécution ne convient à aucun des partis. Un smart contract est donc déterministe et doit prévoir tous les cas de figure.

2.6.1.2 Gaz

L'exécution d'un smart contract, comme toute transaction sur le réseau, implique de rémunérer le mineur pour le travail accomplit. Cette rémunération se fait en Ether mais est appelée gaz et possède son propre cours. Lors de la publication d'un smart contract, le développeur peut définir deux paramètres : le prix maximum du gaz autorisé et le nombre de gaz total à dépenser.

Combinés, ces deux paramètres apportent les avantages suivants :

- Le développeur s'assure que son contrat ne devient pas hors-de-prix. Le cours de l'Ether peut varier sensiblement et est régulièrement sujet à la spéculation. À ce titre, Il est donc important de définir un plafond à ne pas dépasser.
- Le développeur s'assure que son contrat n'entre pas dans une boucle infinie. Certains contrats n'ont pas besoin d'être effectifs plusieurs décennies. Or, ce qui est publié sur le réseau ne peut être supprimé. En limitant le nombre de gaz disponible pour un contrat, son propriétaire peut donc le limiter dans le temps en bloquant son exécution.
- Le mineur, qui peut lui aussi définir son propre prix du gaz, peut refuser de traîter une opération trop lourde si celle-ci n'est pas assez rémunératrice pour lui.

2.6.2 Exécution

2.6.2.1 Algorithme de consensus

L'algorithme de consensus est sujet à débat au sein de la communauté Ethereum. Actuellement, celui-ci est de type preuve de travail mais est extrêmement coûteux en énergie. Afin de changer cela, la transition vers un algorithme de preuve d'enjeu devrait se faire courant 2020.

2.6.2.2 Ethereum Virtual Machine

La machine virtuelle Ethereum est l'environnement d'exécution d'Ethereum. Elle est isolée du réseau et permet de garantir la sécurité des smart contracts ainsi que la compilation et l'exécution de ces derniers. C'est donc elle qui interprète le code d'un smart contract.

Cette machine est également capable de :

- Valider les transactions ainsi que les signatures et adresses de celles-ci
- Calculer les frais de transactions
- Réaliser des transactions

2.7 Synthèse

Dans ce chapitre nous avons étudié la structure, le fonctionnement général d'une blockchain, ses propriétés, ses qualités et ses défauts. Nous nous sommes ensuite intéressés aux spécificités d'Ethereum dont la notion de smart contract. Le chapitre suivant sera consacré à l'application concrète de ces éléments au sein de l'industrie de la mode.

3. Applications possibles pour l'industrie de la mode

La blockchain apporte des possibilités nouvelles pour beaucoup de secteurs et pas uniquement celui de la mode. En effet, dès lors qu'une entreprise partage de l'information, elle pourrait le faire à l'aide de cette technologie. Bien évidemment, la mise en place d'un tel système n'est pas toujours justifiée et certains projets axés blockchain ont été décidés comme tels uniquement à cause d'un effet de mode dû à la jeunesse de cette technologie.

Lors d'une conférence durant le Polish Bitcoin Congress, Andreas Antonopoulos énonce ceci :

> *« Si quelqu'un vient vous voir, et vous demande "Est-ce que j'ai besoin d'une blockchain pour mon business ?", demandez-leur : "Est-ce que vous avez besoin de quelque chose d'ouvert, neutre, sans frontières, que personne ne contrôle et qui résiste à la censure ? […] Si vous n'avez pas besoin de tout cela, ce que vous demandez, c'est une base de données. Installez-en une, vous n'avez pas besoin de blockchain. »*[3]

On constate donc que les bases de données ne sont pas pour autant en voie de disparition et qu'il convient de se poser les bonnes questions avant de décider de sa technologie de stockage.

Comme nous l'avons vu, la blockchain possède des propriétés de transparence, d'immutabilité, d'automatisation et permet d'accorder sa confiance aux autres utilisateurs. Dès lors qu'une entreprise souhaite lancer un projet requérant un de ces aspects, elle doit vraisemblablement s'orienter sur une solution basée blockchain.

Les possibilités d'applications de ces points sont nombreuses pour l'industrie de la mode. La suite de ce chapitre s'intéressera aux différents cas de figure envisageables ou existants.

Au fil de mes recherches, j'ai pu observer que ces applications se regroupaient sous différentes catégories.

3.1 Applications orientées produit

Le premier axe que j'ai défini se concentre sur le produit et sur ce que la décentralisation peut lui apporter en termes de valeur ajoutée.

[3] Polish Bitcoin Congress 2018, Varsovie, 12 mai 2018

Rapport-Gratuit.com

3.1.1 Authentification du produit et identification de son propriétaire

La contrefaçon est un problème majeur pour toutes les grandes marques. Ce phénomène leur fait non seulement perdre de l'argent, mais nuit également à leur image.

En France, d'après le site du gouvernement, le nombre de saisies de produits de contrefaçons, rien que pour le textile, a été multiplié par 45 entre 1994 et 2011.[4] L'essor d'internet y a joué un grand rôle. Et ce phénomène est également observable à plus grande échelle. Toujours d'après les chiffres du gouvernement français, entre 2009 et 2010, le nombre de saisies a doublé en Europe, passant la barre de la centaine de millions d'articles confisqués dont la valeur totale représente 1,1 milliards d'euros.

On peut donc en tirer les conclusions suivantes : le manque à gagner est énorme pour les marques victimes de ce marché parallèle et ces dernières ne semblent toujours pas avoir trouvé la solution pour répondre à ce problème de taille.

En plus de ce manque à gagner, la mauvaise qualité de ces répliques peut également poser un problème pour la sécurité du consommateur. En effet, un produit de contrefaçon ne répond à aucune norme de sécurité. De par ce fait, il peut s'avérer dangereux pour la santé de son propriétaire.

Les gouvernements font également partie des victimes de ce marché parallèle. Un produit contrefait n'est pas soumis aux différentes taxes en vigueur dans chaque pays, comme la TVA par exemple. Cela représente un manque à gagner énorme au vu de la taille de ce marché.

Il est donc important de limiter au mieux la production de contrefaçon car tous les partis évoqués, hormis évidemment les faussaires, sont les grands perdants de ce marché parallèle.

Pour ce faire, les créateurs peuvent par exemple utiliser des matériaux plus nobles, donc difficilement trouvables pour les fabricants de faux afin de compliquer la reproduction de leurs produits. Ils peuvent également signaler les boutiques en ligne proposant des répliques de leurs produits aux autorités compétentes. Malheureusement, les chiffres présentés dans cette section précédemment démontrent que ces mesures ne suffisent de loin pas à éradiquer ce fléau. C'est ici que l'informatique intervient.

[4] Site référence : https://www.entreprises.gouv.fr/secteurs-professionnels/la-contrefacon-dans-domaines-la-mode-et-luxe

Dans le but d'être totalement persuadé de l'authenticité d'une pièce, la mise en place d'une blockchain permet d'aller bien plus loin. En y inscrivant l'identifiant de chaque vêtement créé, une marque peut ensuite permettre à ses clients de vérifier que le produit qu'ils achètent est bien enregistré puisque la chaîne est consultable par tous.

Pour ce faire, il faut premièrement pouvoir identifier chaque produit de façon unique et certaine. NFC permet cela.

NFC est une technologie de communication sans fil à très courte distance. Elle permet à un terminal compatible de lire des données contenues sur une puce ou un tag de petite taille. Elle est notamment utilisée pour les paiements sans contact et possède certaines propriétés intéressantes que nous allons voir :

- La première est qu'elle ne nécessite pas d'alimentation. Une puce NFC est alimentée par le terminal qui tente d'y accéder. Elle peut donc être utilisée pendant plusieurs années sans problème.
- La seconde est ce qu'on appelle l'UID, qui est l'identifiant unique de la puce. Ce dernier ne peut pas être modifié et permet d'identifier chaque puce distinctement.
- La dernière est que la puce peut être étanche, ce qui résout un problème non négligeable pour un produit destiné à être passé en machine un grand nombre de fois.

En intégrant une telle puce dans l'étiquette d'un vêtement, son fabriquant s'assure donc qu'aucune contrefaçon ne pourra être reproduite à l'identique étant donné que cela impliquerait de dupliquer la puce à l'identique elle aussi, chose impossible. Il s'assure également de pouvoir identifier distinctement chaque produit afin de le tracer.

En parallèle, une plateforme doit faire le lien entre le consommateur et la blockchain afin de simplifier son utilisation. Une fois l'étiquette NFC scannée, l'utilisateur est redirigé sur la plateforme qui lui indique l'authenticité de son produit.

Il est également envisageable d'établir un historique des propriétaires du produit. À sa sortie de l'usine, celui-ci est enregistré comme appartenant à la marque. Lorsqu'il est vendu, une transaction mentionnant le nouvel acquéreur est effectuée. Celui-ci peut à son tour le revendre s'il le souhaite et l'inscrire dans la chaîne.

Ce système nécessite que les utilisateurs jouent le jeu. Afin d'y arriver, la plateforme mise en place doit être la plus simple d'utilisation possible.

3.2 Applications orientées production

Cet axe se penchera sur les possibilités concernant la phase de production d'un produit.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

3.2.1 Provenance des matières premières et suivi de la chaîne d'approvisionnement

A l'heure où la conscience écologique prend de plus en plus d'importance, la transparence sur la provenance des matériaux ainsi que sur les lieux de confection est un point important de l'étape de production. Certaines marques récentes sont mêmes nées du désir de stopper cette mode rapide et de repenser plus local.

C'est le cas de « La vie est belt » une marque lilloise qui recycle des pneus de vélo en ceinture. Hubert Motte, créateur de la marque explique sur son site la réflexion qui l'a poussé à quitter son poste chez Décathlon pour lancer sa propre affaire :

> *« Généré par une envie certaine d'entreprendre tout en réduisant l'exclusion sociale et la pollution, c'est une initiative optimiste, souhaitant prouver qu'un monde meilleur est possible pour l'Homme et la planète, tout simplement. ».*[5]

C'est pourquoi il travaille avec des matières recyclées, de façon locale et avec des personnes en situation d'handicap.

Certes, les grandes marques ne peuvent pas imiter le modèle d'Hubert Motte car elles produisent à bien plus grande échelle. Cependant, elles peuvent évoluer vers une meilleure transparence des processus de fabrication.

En proposant au consommateur de consulter ces processus, celui-ci peut alors connaître le parcours du produit, la provenance des différents éléments le composant et les étapes de transformation. Grâce à ces données, il peut acheter de façon plus responsable.

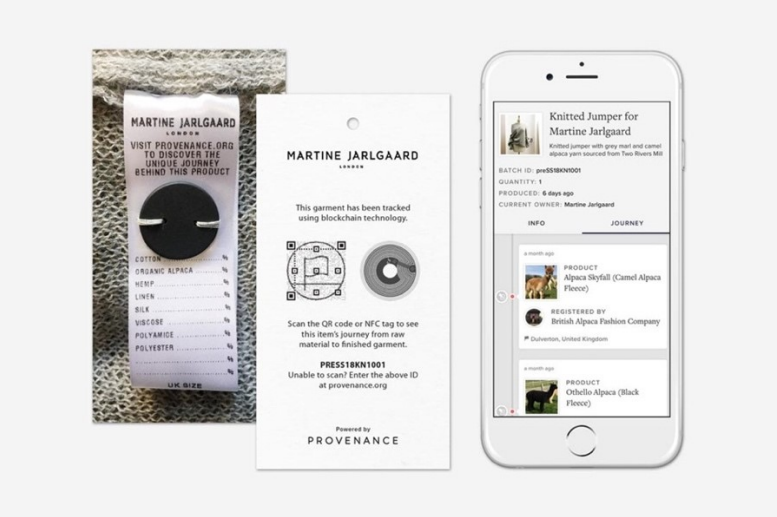
Les entreprises sont également gagnantes. Premièrement, proposer un tel service influe positivement sur l'image de marque. Cela peut être utilisé comme outil de marketing dans le but de cibler l'esprit écoresponsable du consommateur. Deuxièmement, centraliser les données de l'ensemble des fournisseurs permet de standardiser l'échange de données avec ceux-ci.

En 2017, la créatrice danoise Martine Jarlgaard, a collaboré avec la startup Provenance, spécialisée dans la blockchain au sein des chaînes d'approvisionnement, sur un projet de ce type.

A l'aide d'un QR code et d'un tag NFC que nous avons étudié précédemment, l'utilisateur scan le produit. Il est redirigé sur la plateforme de Provenance d'où il peut consulter l'emplacement, le contenu et l'horodatage de chaque étape de la production.

[5] Site référence : https://lavieestbelt.fr/fr/content/12-l-aventure

Figure 7 : Projet blockchain de Martine Jarlgaard et Provenance



(Source : Provenance [en ligne]. [Consulté le 16 octobre 2019]. Disponible à l'adresse : https://www.provenance.org/stories/martine-jarlgaard-alpaca-mirror-top)

Dans un article, Susana Nakatani relaie les propos de Martine Jarlgaard à propos de l'idée derrière ce projet :

> *« Quand je pense à notre monde et à la sous-traitance maintenant, nous avons pris beaucoup de distance par rapport à la façon dont les choses sont fabriquées. Nous devons nous rééduquer. La technologie nous aidera à nous reconnecter avec les gens et les lieux concernés, et cette information augmentera les attentes des consommateurs, ce qui exercera davantage de pression sur les grandes entreprises. »*[6]

Ce projet pilote constitue un premier pas vers la transparence des chaînes d'approvisionnement et permet également d'authentifier le produit. Étant donné qu'il se base aussi sur une puce NFC comme identifiant unique du produit, il pourrait parfaitement être combiné à l'application proposée précédemment permettant d'identifier le propriétaire.

D'après moi, la collaboration entre tous les acteurs concernés reste le principal obstacle à la mise en place de cette application. Une chaîne d'approvisionnement peut impliquer beaucoup d'entités différentes suivant la complexité d'une pièce (tissu, boutons, plumes, ornements et autres). La coopération de tous les partis est essentielle pour que l'utilisateur final bénéficie d'une vue d'ensemble complète et transparente vis-à-vis de la provenance du produit.

[6] Blockchain and sustainability - https://slowfashionworld.com/blockchain-and-sustainability/

3.3 Applications orientées distribution

Intéressons-nous maintenant à l'aspect de distribution. Bien qu'il soit théoriquement possible d'intégrer le paiement en monnaie cryptographique sur les sites d'e-commerce, je n'ai pas souhaité m'attarder sur cet axe pour deux raisons.

La première est que ce cas de figure est applicable pour toute entreprise vendant des biens en ligne et n'est donc pas spécifique à l'industrie de la mode.

La deuxième raison est la volatilité du cours des différentes monnaies cryptographiques. À l'heure actuelle, il paraît compliqué de proposer une gamme de produits dont les prix varient constamment et parfois de façon significative.

C'est pourquoi je me suis tourné vers l'aspect d'exclusivité, que partagent mode et blockchain, évoqué dans l'introduction avec les propos de Nathan Pacer.

3.3.1 Restriction de la duplication d'une œuvre numérique

Quel que soit leur secteur (luxe, prêt-à-porter), les marques ont de plus en plus recourt à des collaborations avec d'autres entités (autres marques, sportifs, célébrités) afin de proposer des produits exclusifs. Ces produits sont souvent fabriqués dans une quantité limitée afin de générer un engouement du public.

Parmi ces nombreuses collaborations, il n'est pas rare qu'une marque utilise une photographie, un tableau ou tout autre visuel de l'artiste avec qui elle collabore.

Cela a été le cas en 2019, lorsque l'artiste Kaws, mondialement connu pour ses figurines « Medicom Toys », a collaboré avec la marque japonaise Uniqlo afin de proposer une collection de t-shirts reprenant le visuel de ses figurines. La commercialisation de cette collaboration a provoqué des débordements en Chine, preuve malheureuse du succès de celle-ci.[7]

[7] Site référence : https://www.gqmagazine.fr/style/article/la-sortie-de-la-derniere-collaboration-uniqlo-a-declenche-des-scenes-demeute-en-chine

Figure 8 : Publicité de la collaboration Kaws - Uniqlo

(Source : Site web d'Uniqlo [en ligne]. [Consulté le 16 octobre 2019]. Disponible à l'adresse : https://www.uniqlo.com/fr/fr/collaborations/kaws-summer)

Dans le cas de cette collaboration, le nombre d'exemplaires produits n'a pas été communiqué officiellement par Uniqlo. C'est donc une donnée dont le consommateur n'a pas connaissance.

Pourtant, il serait tout à fait possible d'avoir recourt à un smart contract afin de déterminer les termes de la collaboration. Il permettrait de limiter le nombre de pièces produites de façon certaine et d'inscrire cette information dans la blockchain. Elle serait donc consultable par tous.

Cependant, il reste un certain nombre de questions juridiques à prendre en compte. Christophe Müller, Professeur à l'Université de Neuchâtel explique (Les Smart Contracts en droit des obligations suisse, p.66) :

> *« Les Smart Contracts sont par nature déterministes (« if-then ») et ne laissent ainsi aucune place à la prise en compte de notions juridiques indéterminées telles que l'exécution dans un délai raisonnable, la résiliation pour justes motifs ou encore des concepts comme la bonne foi ou les best efforts ».*

Un smart contract n'a donc pas de valeur juridique, du moins pour le moment. Malgré tout, Christophe Müller ajoute qu'un smart contract peut permettre de conclure ou d'exécuter un contrat classique.

Cela signifie que l'un et l'autre ne sont pas en concurrence mais destinés à se compléter. Bien que l'idée des smart contracts ait été formulée pour la première fois par Nick Szabo dans les années 1990[8], leur utilisation ne s'est répandue qu'après l'arrivée de la technologie blockchain, elle-même relativement récente. Le défi dans les années à venir sera de leur trouver une place dans le monde juridique en adaptant certains textes de loi.

[8] The Idea of Smart Contracts, 1997

Néanmoins, j'ai décidé de retenir cet axe pour développer ma solution tout en mettant de côté l'aspect juridique qui sort du cadre de ma formation.

3.4 Applications orientées créateur

Le dernier axe de ce chapitre s'intéressera à la possibilité d'utiliser la blockchain comme preuve de création afin de protéger le travail des créateurs de mode.

3.4.1 Protection et rémunération des créateurs

Pour se démarquer de la concurrence, beaucoup de marques créent des visuels qu'elles réutilisent au fil de leurs collections dans le but de construire un univers, une identité que le consommateur reconnaît sans que le nom de la marque en question n'apparaisse pour autant. L'un de ces visuels les plus célèbres est sans aucun doute le monogramme Louis Vuitton, créé il y a plus de 120 ans[9] et connu dans le monde entier, qui a permis à l'entreprise d'arriver là où elle se trouve aujourd'hui.

Évidemment, les marques de luxe comme Louis Vuitton possèdent bon nombre de brevets ainsi que les moyens financiers pour protéger leurs créations mais ce n'est pas le cas de tous.

Pour les plus petits créateurs, la blockchain peut être une alternative. En insérant son travail dans une blockchain dédiée, un créateur peut prouver, par la propriété d'horodatage du bloc que nous avons étudié, qu'il en est bien le propriétaire et que tout autre visuel reprenant son travail et produit après la création de ce bloc est, par conséquent, une copie non autorisée.

En plus de se protéger, un créateur peut également gérer l'utilisation de son travail par d'autres. Par exemple, il serait possible pour lui de prêter ses créations à un musée afin de les exposer pendant une durée prédéfinie. Les termes de l'accord, autrement dit le type de licence accordée, seraient inscrits dans la blockchain. Dès lors, le créateur peut facilement prouver que son travail est utilisé sans autorisation si tel devait être le cas. S'il n'existe pas de licence liant l'œuvre en question à l'exploitant, c'est que ce dernier l'utilise sans en avoir le droit.

En échange de l'attribution d'une licence un créateur peut également se faire rémunérer via la blockchain et l'utilisation de tokens. Dans ce cas la valeur de sa rémunération dépend de l'évolution du cours du token utilisé.

[9] Site référence : https://fr.louisvuitton.com/fra-fr/articles/un-monogram-de-legende

3.5 Synthèse

Comme nous venons de le voir, les applications pour l'industrie de la mode sont variées et amènent de nouvelles possibilités susceptibles de transformer le milieu. L'ensemble des acteurs, y compris le consommateur, sont concernés et peuvent en bénéficier. La transparence semble être le fil conducteur vers une industrie plus responsable.

4. Solution

4.1 Concept

Dans le but d'appuyer mes propos, j'ai développé une webapp pour un magasin factice de prêt-à-porter que j'ai nommé Ateliers Genève.

L'idée est d'enrichir l'expérience du client en magasin en lui proposant de personnaliser un produit sur place, via la webapp sur un PC mis à disposition.

L'utilisateur a le choix entre plusieurs vêtements et plusieurs couleurs. Le dos de chaque pièce est également personnalisable en y apposant une illustration. Pour ce faire, l'utilisateur a le choix entre plusieurs œuvres d'artistes avec qui le magasin collabore.

L'utilisation de ces illustrations est limitée afin de créer de l'exclusivité sur la collaboration avec les différents artistes. Cette limitation est assurée par un smart contract.

Une fois que l'utilisateur a validé ses choix, l'ordre d'impression est envoyé aux collaborateurs du magasin.

4.2 Fonctionnement

4.2.1 Fonctionnement général

Premièrement, l'utilisateur choisit le produit qu'il souhaite créer (t-shirt, pull à capuche ou pull à fermeture zippée). Puis, il est redirigé vers l'espace de personnalisation d'où il peut choisir la taille, la couleur et l'illustration qu'il désire apposer.

Lorsqu'il valide ses choix, un ordre d'impression est envoyé au smart contract qui met à jour le nombre d'impressions effectuées pour l'illustration sélectionnée. Les données de la commande sont enregistrées dans un fichier texte sur le serveur que les employés peuvent consulter afin de lancer l'impression en fonction des choix de l'utilisateur.

L'utilisateur est redirigé sur la page de confirmation qui affiche le récapitulatif de la commande. Le hash de la transaction effectuée sur la blockchain est également affiché et fait office de numéro d'identification unique pour payer et retirer le produit.

Lorsqu'une œuvre atteint son nombre d'utilisations maximum, cette dernière est détruite au sein du smart contract et n'est plus affichée sur la page.

4.2.2 Webapp

La webapp utilise la plateforme Node.js pour fonctionner et se sert du module Web3.js pour interagir avec le smart contract. J'avais d'abord pensé réaliser un projet PHP mais au fil de mes recherches je me suis rendu compte que la version PHP de Web 3 n'était

pas assez répandue et fiable. Bien que n'ayant aucune expérience dans le développement Node.js, j'ai quand même choisi de baser mon projet sur cette plateforme.

4.2.2.1 Point d'entrée

Le fichier server.js qui se trouve à la racine de la webapp est le point d'entrée de celle-ci. Son rôle est d'initialiser l'application ainsi que de lancer l'ordre de connexion au contrat.

4.2.2.2 Communication avec le smart contract

Le fichier smartcontract.js fait le lien entre la webapp et le contrat. Il permet de se connecter au contrat et d'appeler ses différentes fonctions. Il stocke également les œuvres dans un tableau Javascript afin d'y accéder plus facilement dans le reste de la webapp.

Comme mentionné plus haut, le lien avec le smart contract se fait grâce à Web3.js qui est un module Node. Il effectue des appels au contrat via le protocole JSON-RPC.

Une fois l'instance du contrat récupérée, chacune de ses méthodes peut être appelée via l'instruction *methods.nom-de-la-fonction-dans-le-smart-contract* suivit de l'instruction *call()* ou *send()* en fonction du type d'opération que la méthode appelée effectue. Le tableau qui suit explique les différences entre ces deux instructions.

Tableau 1 : Différences call - send

Méthode	Crée une transaction	Modifie l'état du contrat
call()	NON	NON
send()	OUI	OUI

(Thibaud Rossetti)

Pour résumer, l'utilisation de *call* n'entraîne pas de dépense de gaz. On l'utilise pour consulter les informations du contrat. La méthode *send* est, elle, utilisée pour mettre à jour le contrat.

Le résultat retourné par ces méthodes est ensuite traité au sein du callback.

4.2.2.3 Frameworks

Pour réaliser ma webapp j'ai utilisé Express, un framework très répandu qui permet, entre autres, de simplifier la gestion des routes.

J'ai également eu recours à Bootstrap pour structurer mes pages web et faire en sorte que le résultat s'adapte à tous types d'appareils (PC, tablette, smartphone).

Rapport-Gratuit.com

4.2.3 Smart Contract

Le smart contract a été développé en Solidity et est, dans le cas d'une mise en production réelle, destiné à être publié sur la blockchain Ethereum ou dans une blockchain privée. Dans le cadre de ce travail, il est exécuté par un nœud local.

4.2.3.1 Données

Il contient les données suivantes :

- Un tableau contenant les différentes œuvres disponibles
- Une constante définissant le nombre d'impressions autorisées
- L'adresse du propriétaire du contrat
- Une structure représentant une œuvre et dont les champs sont ceux ci-dessous

Figure 9 : Représentation de la structure Artwork

```
struct Artwork {
    uint32 id;
    string name;
    string owner;
    string fileName;
    uint nbPrintsAllowed;
    uint nbPrintsCurrent;
}
```

(Thibaud Rossetti)

4.2.3.2 Contraintes

J'ai inséré un modificateur que voici :

Figure 10 : Modificateur du smart contract

```
modifier ownerOnly {
    require(contract_owner == msg.sender);
    _;
}
```

(Thibaud Rossetti)

Il induit que seul le propriétaire du contrat, c'est-à-dire le magasin dans notre cas d'utilisation, a le droit d'exécuter les fonctions soumises à ce modificateur.

Ce dernier est appliqué sur toutes les fonctions dont le résultat modifie l'état des données du smart contract. Cela concerne la fonction d'ajout d'une œuvre et la fonction d'impression. Il s'agit d'opérations qui ont un coût en matière de gaz.

4.2.3.3 Constructeur

Le constructeur est appelé au déploiement du contrat. Son rôle est d'assigner l'adresse du propriétaire du contrat et d'appeler la fonction d'ajout d'une œuvre avec les différentes données de celle-ci autant de fois qu'il y a d'œuvres.

Figure 11 : Constructeur du smart contract

```
constructor() public  {
    contract_owner = msg.sender;
    addArtwork(0,"Sunrise", "C2H4", "sunrise.jpg"); // id must start at 0 and follow each other
    addArtwork(1,"Triangle", "C2H4", "triangle.jpg");
    addArtwork(2,"Thank you internet", "AR", "thankyouinternet.jpg");
    addArtwork(3,"Table", "Kith", "table.jpg");
    addArtwork(4,"View", "Kith", "view.jpg");
    addArtwork(5,"Worldwide", "AR", "worldwide.jpg");
}
```

(Thibaud Rossetti)

4.2.3.4 Fonctions

4.2.3.4.1 printArtwork

Récupère l'œuvre à partir de l'id passé en paramètre, incrémente le nombre d'impressions puis met à jour le tableau. Si l'œuvre a atteint le nombre maximal d'impressions, il est supprimé du tableau. Cette fonction est protégée par le modificateur.

Figure 12 : Fonction printArtwork

```
function printArtwork(uint _id) ownerOnly public {
    Artwork memory art = artworks[_id];
    art.nbPrintsCurrent++;
    if (art.nbPrintsCurrent >= NB_PRINT_ALLOWED) {
        delete artworks[_id];
    } else {
        artworks[_id] = art;
    }
}
```

(Thibaud Rossetti)

4.2.3.4.2 getArtwork

Retourne une œuvre en fonction de l'id passé en paramètre.

Figure 13 : Fonction getArtwork

```
function getArtwork(uint _id) view public returns(Artwork memory) {
    return artworks[_id];
}
```

(Thibaud Rossetti)

4.2.3.4.3 getArtworks

Retourne simplement l'ensemble des œuvres.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Figure 14 : Fonction getArtworks

```
function getArtworks() view public returns(Artwork[] memory) {
    return artworks;
}
```

(Thibaud Rossetti)

4.2.3.5 Instances

Une instance de ce contrat contient les informations relatives à la collaboration d'un seul magasin avec plusieurs artistes. En testant la solution il n'y aura donc qu'une seule instance créée mais plusieurs dans le cas d'un déploiement à plus grande échelle. Nous y reviendrons.

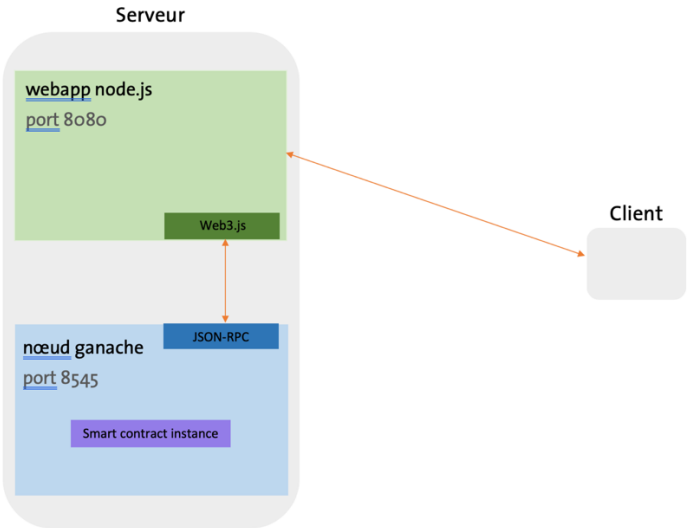
4.2.4 Ganache-cli

Ganache-cli permet de simuler un nœud Ethereum en local afin d'exécuter le smart contract sans le publier sur la blockchain Ethereum. Il fournit un lot d'adresses pour interagir avec le contrat et simuler plusieurs utilisateurs. Ces adresses ont un solde en Ether virtuel afin de pouvoir consommer du gaz. Ganache-cli est disponible via le gestionnaire de paquets de Node, npm.

4.2.5 Architecture

L'architecture de la solution en phase de test est la suivante. Dans cette configuration, serveur et client se trouvent sur la même machine.

Figure 15 : Architecture générale de la solution



(Thibaud Rossetti)

4.3 Déploiement

Pour que l'utilisation de la blockchain se justifie et prenne tout son sens, il faut que le smart contract soit publié. Il sera ainsi connu des autres nœuds ce qui garantira son immutabilité.

Pour cela, il y a deux possibilités que nous allons voir.

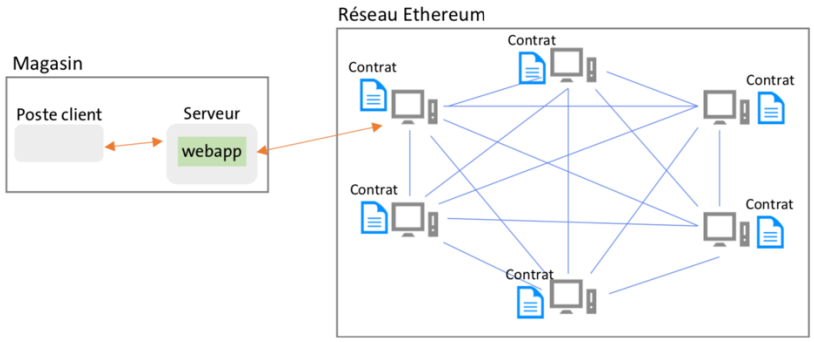
4.3.1 Sur la blockchain Ethereum principale

La première solution est de publier le contrat sur la blockchain Ethereum principale. C'est la piste la plus logique car en tant que blockchain publique elle amène les avantages évoqués plus tôt dans ce travail. Les informations seront consultables par tous, consommateur compris.

De plus, la blockchain Ethereum est déjà en place. Il n'y a donc pas besoin de se soucier de l'infrastructure.

Si le magasin factice devait se développer en ouvrant d'autres arcades, celles-ci pourraient participer à la collaboration simplement en initiant une nouvelle instance du contrat.

Figure 16 : Architecture de la solution dans une blockchain publique



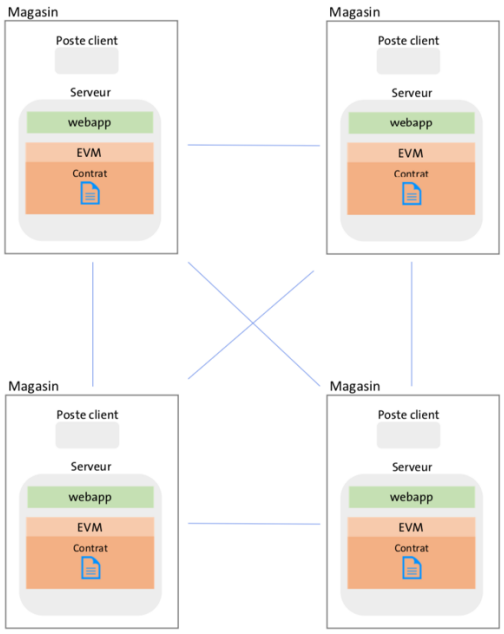
(Thibaud Rossetti)

4.3.2 Sur une blockchain Ethereum privée

Le contrat serait également déployable au sein d'une blockchain privée. En partant du principe qu'Ateliers Genève ouvre d'autres boutiques ailleurs, il serait possible de les utiliser comme nœuds au sein du réseau privé. Chaque arcade contiendrait les différentes instances de contrat des autres magasins.

Cette alternative empêche la consultation des données par des acteurs extérieurs mais peut s'avérer intéressante dans certains cas d'utilisation.

Figure 17 : Architecture de la solution dans une blockchain privée



(Thibaud Rossetti)

5. Conclusion

Durant la rédaction de ce travail, je me suis rendu compte que la blockchain est une technologie relativement nouvelle qui manque encore de maturité mais avec un énorme potentiel. Elle est de plus en plus utilisée dans des projets de tous horizons et intéresse énormément de secteurs.

L'industrie de la mode commence à peine à s'y intéresser et pourtant un certain nombre d'initiatives me paraissent prometteuses. Le projet pilote de Martine Jarlgaard et la startup Provenance, permettant de retracer le cheminement complet d'une pièce, est sans aucun doute le plus abouti que j'ai rencontré lors de mes recherches. Bien qu'ayant un impact négatif sur l'écologie, de par l'utilisation d'une blockchain, l'objectif de transparence visé par ce projet permettra aux consommateurs d'acheter de façon plus responsable en excluant les produits dont les matériaux proviennent des quatre coins du monde.

Comme nous l'avons vu, l'association entre une blockchain et une puce NFC amène d'autres possibilités comme l'authentification d'une pièce et l'identification de son propriétaire. Cela pourrait permettre d'affaiblir le colossal marché actuel de la contrefaçon.

Les possibilités offertes par les smart contracts sont également très prometteuses pour les années à venir. Cependant, leur démocratisation dépendra fortement de l'évolution des lois les concernant. Le monde juridique est extrêmement complexe et les clauses d'un contrat sont sujettes à l'interprétation, chose qu'un smart contract ne peut réaliser car il exécute uniquement. Un contrat intelligent ne remplacera donc pas un contrat classique. De plus, ils n'ont pas la même vocation ni les mêmes propriétés. Les cas ayant recours aux deux devraient néanmoins se répandre progressivement.

L'aspect de protection des créations est à suivre de près car il peut aussi être mis en œuvre dans d'autres secteurs comme l'industrie musicale, cinématographique ou littéraire.

Le développement de la solution m'a permis d'apprendre à communiquer avec un smart contract autrement que par l'IDE Remix, via Web3.js que j'ai découvert par la même occasion.

Le fait d'être contraint de développer ma solution avec Node.js, à cause de Web3.js, a d'abord été handicapant car j'ai dû dédier une partie de mon temps à l'apprentissage pur

de cette plateforme que je ne connaissais pas. Avec le recul, cela a été bénéfique pour ma formation et m'a permis d'acquérir de nouvelles connaissances.

Bibliographie

ABTAN, Olivier, BARTON, Christine, BONELLI, Frederico, GURZKI, Hannes, MEI-POCHTLER, Antonella, PIANON, Nicola, TSUSAKA, Miki, 2016. Digital or Die: The Choice for Luxury Brands [en ligne]. 22 septembre 2016. [Consulté le 1 octobre 2019]. Disponible à l'adresse : https://www.bcg.com/fr-fr/publications/2016/digital-or-die-choice-luxury-brands.aspx

ANTONOPOULOS, Andreas, 2018. The Future of Programmable Money [enregistrement vidéo]. Youtube [en ligne]. 26 mai 2018. [Consulté le 11 octobre 2019]. Disponible à l'adresse : https://www.youtube.com/watch?v=1MG1aR71uFg

BAKER, Jessi, 2017. The story of Provenance – The blockchain startup revolutionizing supply chains [enregistrement vidéo]. Youtube [en ligne]. 12 mai 2017. [Consulté le 12 octobre 2019]. Disponible à l'adresse : https://www.youtube.com/watch?v=QWkAx7Qw5v8

BALVA, Claire, 2016. La Blockchain : réinventer les rapports de confiance [enregistrement vidéo]. Youtube [en ligne]. 22 février 2017. [Consulté le 5 octobre 2019]. Disponible à l'adresse : https://www.youtube.com/watch?v=JID9c-MABis

BLOCH, Raphaël, 2018. La blockchain peut-elle révolutionner le droit d'auteur ? [en ligne]. 16 mars 2018. [Consulté le 10 novembre 2019]. Disponible à l'adresse : https://www.lesechos.fr/2018/03/la-blockchain-peut-elle-revolutionner-le-droit-dauteur-986814

BOUZEFRANE, Samia, 2013. La technologie RFID / NFC. CEDRIC CNAM [en ligne]. [Consulté le 8 novembre 2019]. Disponible à l'adresse : https://cedric.cnam.fr/~bouzefra/cours/CoursNFC_Bouzefrane_Decembre2013.pdf

CAVALLI, Blaise, RENAUD LOUBERT, Aledo, 2018. Blockchain privée : illusion ou innovation ? . Medium [en ligne]. 13 septembre 2018. [Consulté le 17 octobre 2019]. Disponible à l'adresse : https://medium.com/blocsnews/blockchain-priv%C3%A9e-illusion-ou-innovation-7bbedefa4b4e

Communication en champ proche. *Wikipedia: l'encyclopédie libre* [en ligne].Dernière modification de la page le 30 octobre 2019 à 12 : 51. [Consulté le 29 octobre 2019]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Communication_en_champ_proche

DE QUÉNETAIN, Stanislas, [date inconnue]. Est-ce que les Smart Contracts peuvent être appliqués à nos vies de tous les jours ? [en ligne]. [Consulté le 7 novembre 2019]. Disponible à l'adresse : https://www.blockchains-expert.com/smart-contracts-peuvent-etre-appliques-a-nos-vies-de-jours/

DUGERDIL, Philippe, 2018. Introduction – Principles of Blockchain Architecture [document PDF]. Support de cours : Cours “Atelier Blockchain”, Haute école de gestion de Genève, filière Informatique de Gestion, année académique 2018-2019

Ethereum. Wikipedia: l’encyclopédie libre [en ligne]. Dernière modification de la page le 12 novembre 2019 à 22 : 47. [Consulté le 13 octobre 2019]. Disponible à l’adresse : https://fr.wikipedia.org/wiki/Ethereum

Ganache-cli Documentation – Nethereum [en ligne]. [Consulté le 20 novembre 2019]. Disponible à l’adresse : https://docs.nethereum.com/en/latest/ethereum-and-clients/ganache-cli/

GRAFIKART, 2016. NodeJS(3/6) : Notre premier serveur [enregistrement vidéo]. Youtube [en ligne]. 28 juillet 2016. [Consulté le 8 novembre 2019]. Disponible à l’adresse : https://www.youtube.com/watch?v=HLPHoY-h7vc

GRAFIKART, 2016. NodeJS(5/6) : Modules & NPM [enregistrement vidéo]. Youtube [en ligne]. 1 août 2016. [Consulté le 8 novembre 2019]. Disponible à l’adresse : https://www.youtube.com/watch?v=B4P_b-UzjLw

GRAFIKART, 2016. NodeJS(6/6) : ExpressJS [enregistrement vidéo]. Youtube [en ligne]. 2 août 2016. [Consulté le 13 novembre 2019]. Disponible à l’adresse : https://www.youtube.com/watch?v=Q8wacXNngXs

GUIMBERTEAU, Boriana, 2019. Pourquoi la technologie blockchain peut changer la donne dans le domaine de la mode ? [en ligne]. 20 mars 2019. [Consulté le 2 octobre 2019]. Disponible à l’adresse : https://fashionunited.fr/actualite/business/pourquoi-la-technologie-blockchain-peut-changer-la-donne-dans-le-domaine-de-la-mode/2019032020310

L’aventure – La vie est belt [en ligne]. [Consulté le 23 octobre 2019]. Disponible à l’adresse : https://lavieestbelt.fr/fr/content/12-l-aventure

MARSHALL, David, 2017. How modern technology has changed the fashion industry [en ligne]. 6 novembre 2017. [Consulté le 4 octobre 2019]. Disponible à l’adresse : https://immago.com/modern-technology-changed-fashion-industry/

MCDOWELL, Maghan, 2019. 6 ways blockchain is changing luxury. Vogue Business [en ligne]. 14 mai 2019. [Consulté le 7 octobre 2019]. Disponible à l’adresse : https://www.voguebusiness.com/technology/6-ways-blockchain-changing-luxury?itm_source=manual_article_recommendation

MÜLLER, Christoph, [date inconnue]. Les Smart Contract en droit des obligations suisse. Unine.ch [en ligne]. [Consulté le 1 novembre 2019]. Disponible à l’adresse :

https://www.unine.ch/files/live/sites/christoph.mueller/files/Publications/Les%20smart%20contracts%20en%20droit%20des%20obligations%20suisse.pdf

MÜLLER, Christoph, CARRON, Blaise, 2018. Blockchain et Smart Contracts. Défis juridiques et techniques en particulier dans les secteurs : Banques, Assurances privées, Transports. Bâle : Helbing Lichtenhahn Verlag. Papiers. ISBN 978-3-7190-4181-6

NAKATANI, Susana, 2018. Blockchain and sustainability. Slow Fashion[en ligne]. 10 juillet 2018. [Consulté le 25 octobre 2019]. Disponible à l'adresse : https://slowfashionworld.com/blockchain-and-sustainability/

PROVENANCE, 2018. Provenance [en ligne]. [Consulté le 16 octobre 2019]. Disponible à l'adresse : https://www.provenance.org/stories/martine-jarlgaard-alpaca-mirror-top

Qu'est-ce qu'un token – Blockchain France [en ligne]. [Consulté le 8 octobre 2019]. Disponible à l'adresse : https://blockchainfrance.net/2018/05/22/comprendre-les-tokens/

Qu'est-ce que la blockchain ? – Blockchain France [en ligne]. [Consulté le 6 octobre 2019]. Disponible à l'adresse : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

Qu'est-ce que la machine virtuelle Ethereum ? – Cryptoast [en ligne]. [Consulté le 17 octobre 2019]. Disponible à l'adresse : https://cryptoast.fr/quest-ce-que-la-machine-virtuelle-ethereum/

RIGHI, Nadège, 2018. La traçabilité, fer de lance de la lutte contre la contrefaçon. Mode in Textile [en ligne]. 31 janvier 2018. [Consulté le 4 novembre 2019]. Disponible à l'adresse : https://www.modeintextile.fr/tracabilite-fer-de-lance-de-lutte-contre-contrefacon/

Satoshi Nakamoto. *Wikipedia: l'encyclopédie libre* [en ligne].Dernière modification de la page le 20 novembre 2019 à 13 : 44. [Consulté le 5 octobre 2019]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Satoshi_Nakamoto

SIMON, Gary, 2017. 03. Web3.js Tutorial – Attach a GUI to your Ethereum Smart Contract [enregistrement vidéo]. Youtube [en ligne]. 24 octobre 2017. [Consulté le 7 novembre 2019]. Disponible à l'adresse : https://www.youtube.com/watch?v=hcTPjpPvas8

SIMON, Gary, 2017. 06. Solidity Mappings & Structs Tutorial [enregistrement vidéo]. Youtube [en ligne]. 30 octobre 2017. [Consulté le 12 novembre 2019]. Disponible à l'adresse : https://www.youtube.com/watch?v=gfXewa4xmYE

Rapport-Gratuit.com

SINGH, Niharika, 2018. Blockchain and Fashion Industry [en ligne]. 21 novembre 2018. [Consulté le 16 octobre 2019]. Disponible à l'adresse : https://hackernoon.com/blockchain-and-fashion-industry-a5076355aa41

Solidity Documentation v0.5.13 – Read the Docs [en ligne]. [Consulté le 22 novembre 2019]. Disponible à l'adresse : https://solidity.readthedocs.io/en/v0.5.13/

SZABO, Nick, 1997. The Idea of Smart Contracts [en ligne]. [Consulté le 14 octobre 2019]. Disponible à l'adresse : http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

VAIBHAV, Saini, 2018. Getting Deep Into EVM: How Ethereum Works Backstage [en ligne]. 15 août 2018. [Consulté le 18 novembre 2019]. Disponible à l'adresse : https://hackernoon.com/getting-deep-into-evm-how-ethereum-works-backstage-ac7efa1f0015

Web3.js Documentation v1.2.2 – Read the Docs [en ligne]. [Consulté le 23 novembre 2019]. Disponible à l'adresse : https://web3js.readthedocs.io/en/v1.2.2/

Annexe 1 : Documentation développeur

1. Installation

1.1 Prérequis

Vous devez posséder Node.js 12.13.0 minimum avec npm package manager. Si ce n'est pas le cas, vous pouvez les télécharger à l'adresse : https://nodejs.org/en/download/.

Par défaut, npm est installé d'office avec Node.

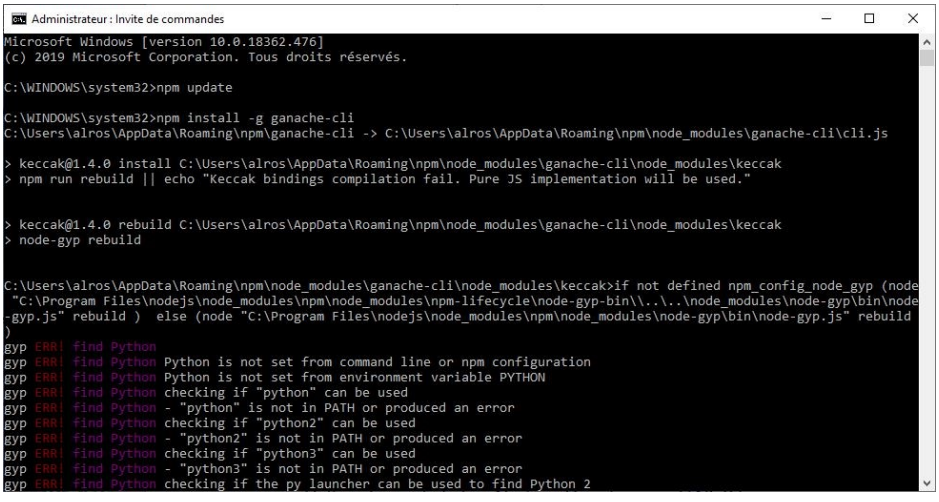
L'installation qui suit est sensiblement la même sur Mac OS et Windows et a été testée sur les deux plateformes.

1.2 Installation du nœud Ethereum

Ouvrez une invite de commandes en mode administrateur et tapez *npm update* afin de vous assurer que le gestionnaire de paquets est à jour

Tapez ensuite *npm install -g ganache-cli* afin d'installer le nœud de façon globale. Il est possible qu'un certain nombre d'erreurs apparaissent liées à python si ce dernier n'est pas installé mais cela n'a pas d'impact sur le bon fonctionnement du nœud.

Figure 18 : Installation de ganache

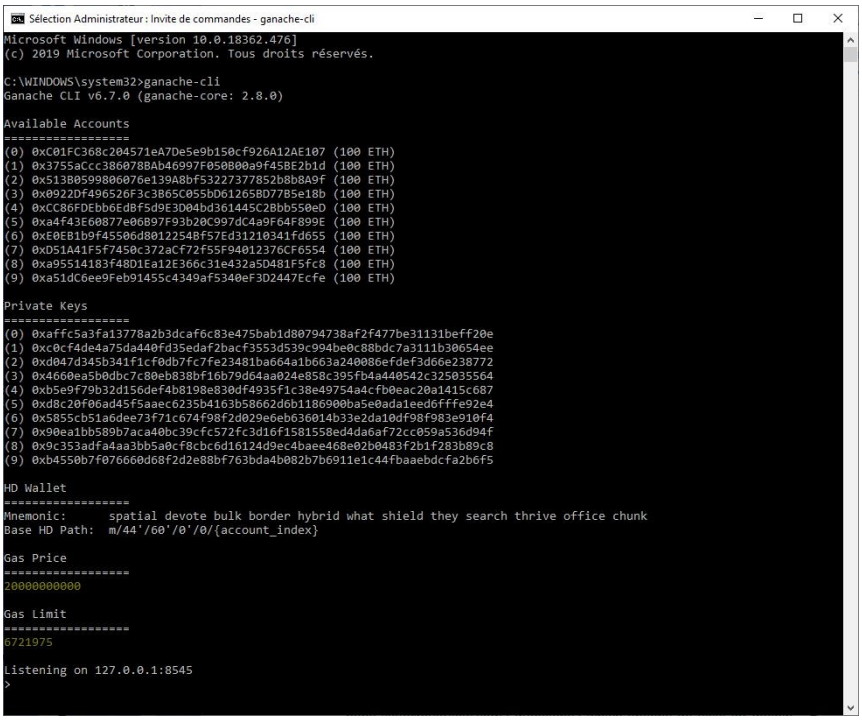


(Thibaud Rossetti)

Tapez *ganache-cli* pour lancer le nœud local. Assurez-vous que le port est bien le 8545.

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Figure 19 : Lancement de ganache-cli

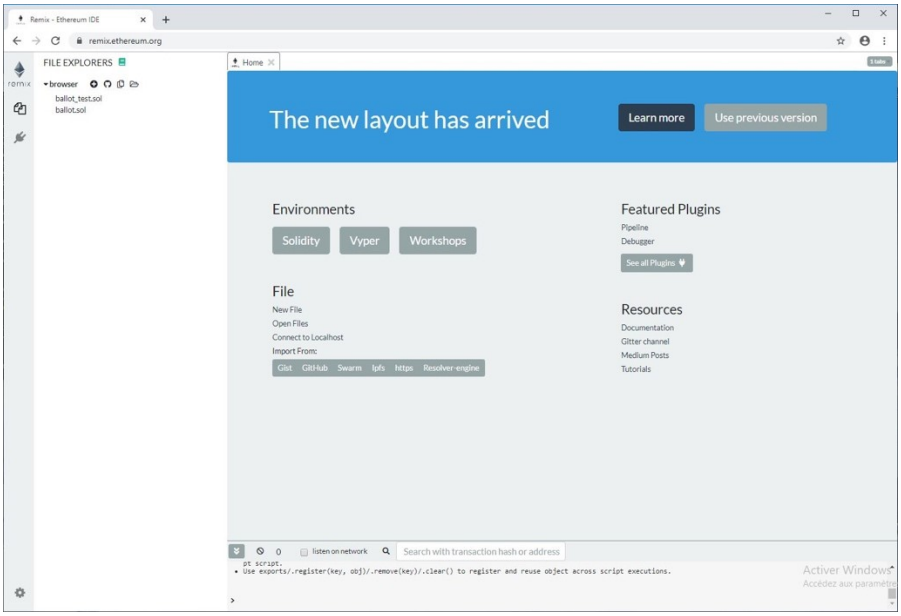


(Thibaud Rossetti)

1.3 Déploiement du smart contract

Ouvrez le navigateur de votre choix et rendez-vous à l'adresse *remix.ethereum.org*.

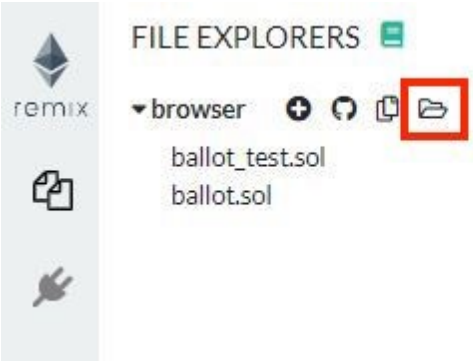
Figure 20 : Page d'accueil de Remix



(Thibaud Rossetti)

Importez le fichier *contract_artworks.sol* à l'aide du bouton dédié.

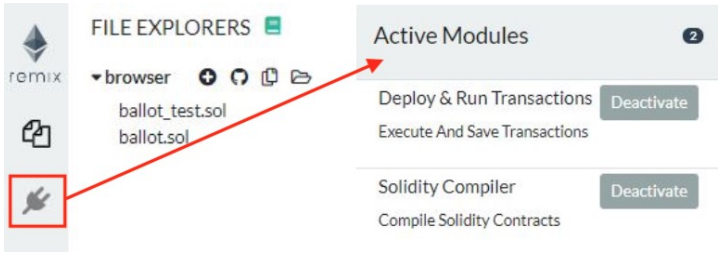
Figure 21 : Importer un smart contract



(Thibaud Rossetti)

Rendez-vous ensuite dans l'onglet *plugin* pour activer les modules ci-dessous.

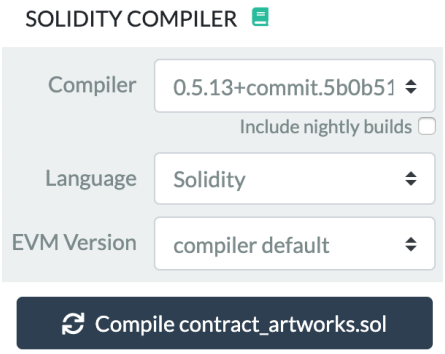
Figure 22 : Onglet des plugins



(Thibaud Rossetti)

Direction l'onglet *compilation*. Sélectionnez la version 0.5.13 et cliquez sur *Compile contract _artworks.sol*.

Figure 23 : Compiler le smart contract



(Thibaud Rossetti)

Dans l'onglet *déploiement*, modifiez le champ *Environnement* comme suit afin de vous connecter au nœud ganache. Validez les deux alertes qui s'affichent.

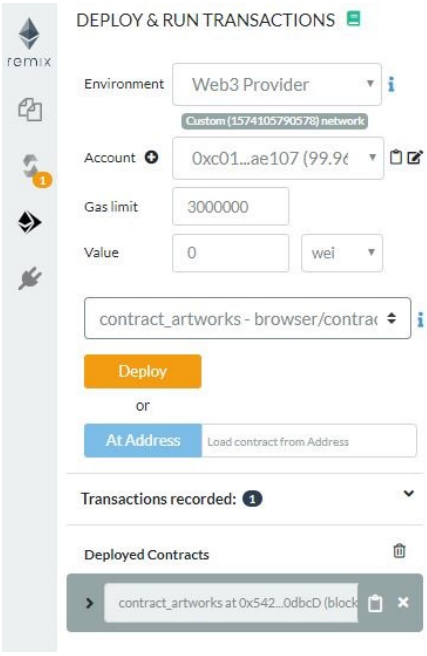
Figure 24 : Modifier l'environnement

(Thibaud Rossetti)

Afin de vérifier que vous êtes bien connecté au nœud, vous pouvez comparer les adresses du champ *account* à celles que ganache vous a fourni à son lancement. Il doit s'agir des mêmes.

Déployez le contrat à l'aide du bouton *Deploy*. Le smart contract apparaît dans la section *Deployed Contracts*.

Figure 25 : Déployer le smart contract



(Thibaud Rossetti)

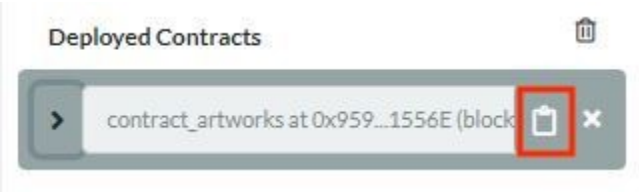
1.4 Lancement de la webapp

Copiez le dossier *webapp* sur votre bureau.

Dans celui-ci, allez dans le sous-dossier */class* et ouvrez le fichier *const.js* avec l'éditeur de votre choix.

Retournez sur remix dans la section *Deployed Contracts* et cliquez sur le symbole presse-papier afin de copier son adresse.

Figure 26 : Copier l'adresse du smart contract



(Thibaud Rossetti)

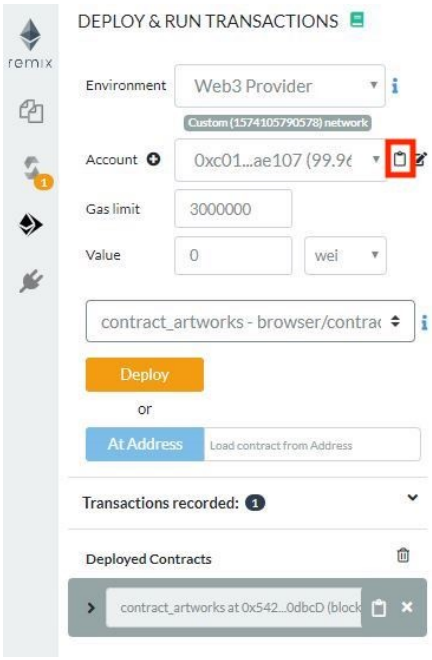
Collez l'adresse dans *const.js* ici-même. N'oubliez pas les apostrophes.

```
// CONST TO CHANGE WITH YOUR OWN VALUES
exports.ACCOUNT_ADDRESS = '0x8378f4b318eae6b3dfbc1ac9161556a133cc954f';
exports.CONTRACT_ADDRESS = '0x95972c9d460330d63c255cB7948127291D91556E';
```

(Thibaud Rossetti)

Faites de même pour l'adresse du compte, disponible sur remix ici.

Figure 27 : Copier l'adresse du compte



(Thibaud Rossetti)

Et à insérer ici :

Figure 28 : Fichier des constantes

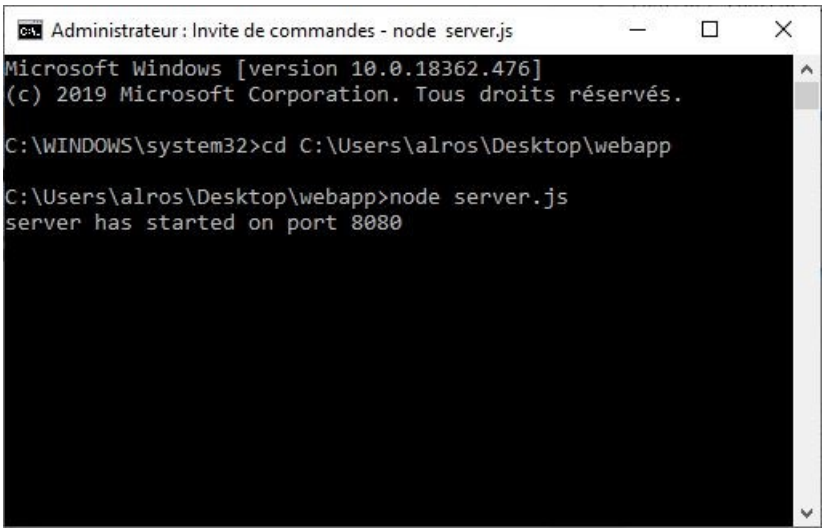
```
// CONST TO CHANGE WITH YOUR OWN VALUES
exports.ACCOUNT_ADDRESS = '0x8378f4b318eae6b3dfbc1ac9161556a133cc954f';
exports.CONTRACT_ADDRESS = '0x95972c9d460330d63c255cB7948127291D91556E';
```

(Thibaud Rossetti)

Lancez une seconde invite de commande. Dans celle-ci, positionnez-vous à la racine de webapp à l'aide de la commande *cd + chemin de webapp*.

Tapez *node server.js* qui aura pour effet de lancer la webapp

Figure 29 : Démarrage de la webapp



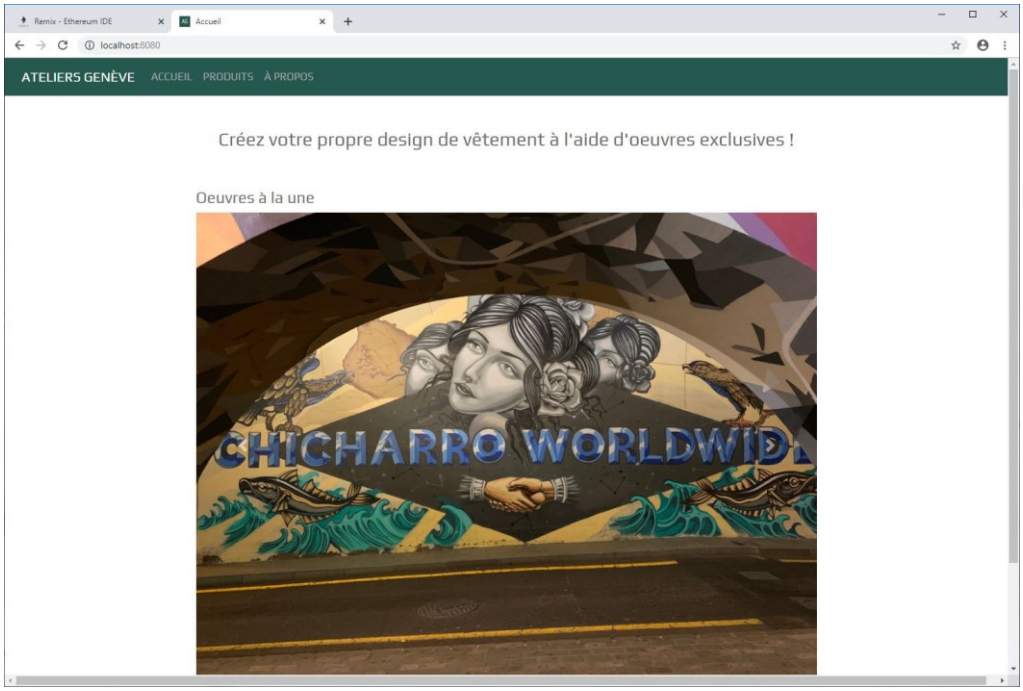
(Thibaud Rossetti)

1.5 Tester la webapp

La webapp est maintenant accessible à l'adresse *localhost:8080* dans votre navigateur.

La page d'accueil est une simple page statique qui met en valeur certaines œuvres.

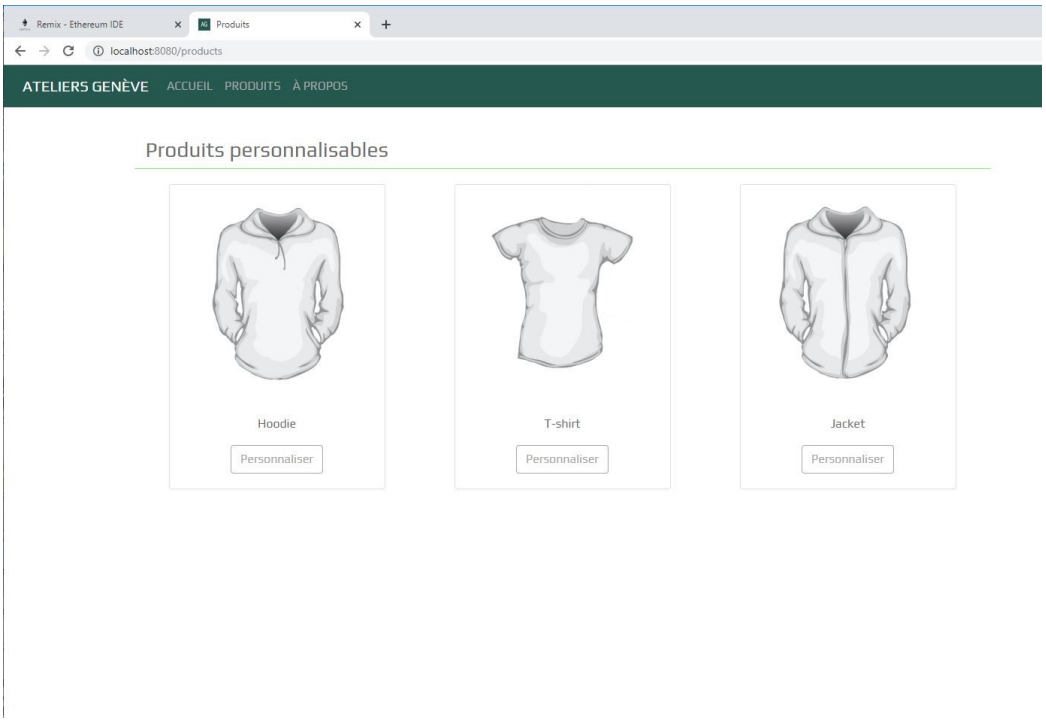
Figure 30 : Page d'accueil



(Thibaud Rossetti)

Affichez la liste des produits disponibles en cliquant sur l'onglet *produits*.

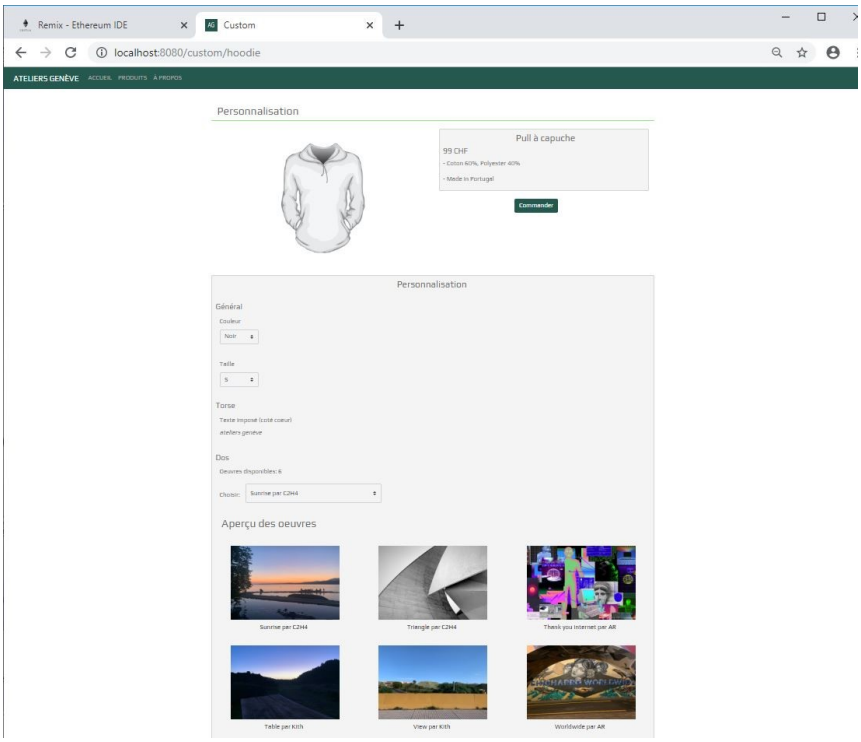
Figure 31 : Page des produits



(Thibaud Rossetti)

Cliquez sur *personnaliser* sous le produit de votre choix. La page de customisation apparaît.

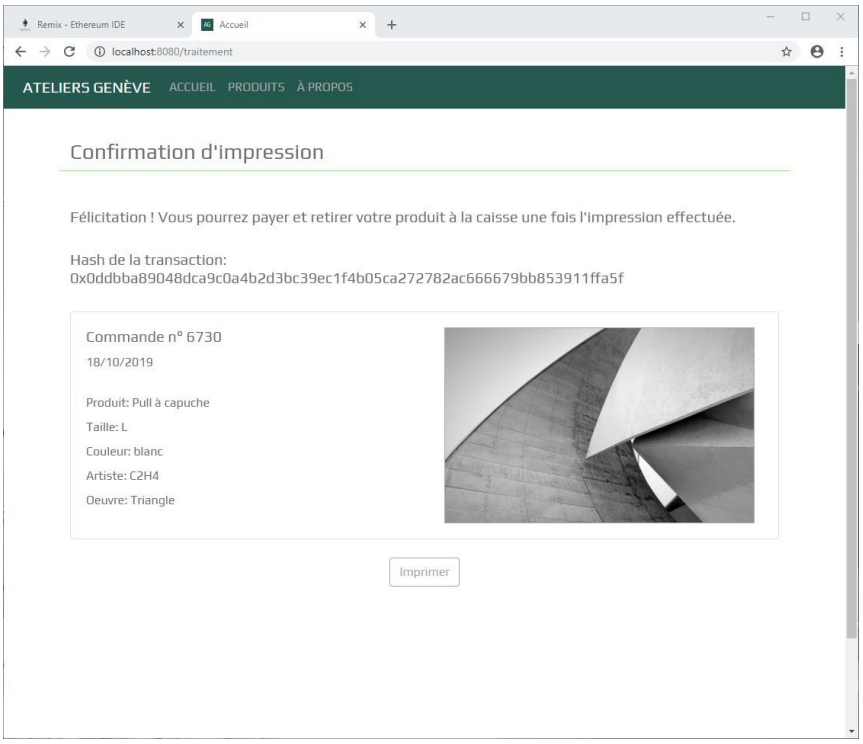
Figure 32 : Page de personnalisation



(Thibaud Rossetti)

Sélectionnez les options qui vous conviennent et cliquez sur le bouton *commander*.

Figure 33 : Page de confirmation



(Thibaud Rossetti)

La page de confirmation vous donne un aperçu de votre commande. Le hash de transaction sert d'identifiant au moment d'aller régler et retirer votre achat. Cliquez sur le bouton imprimer pour récupérer votre confirmation au format papier.

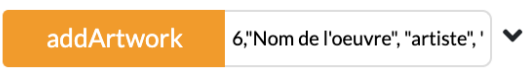
Dans le dossier *data*, le fichier nommé *orders.txt* doit avoir enregistré les informations de la commande.

1.5.1 Insérer une nouvelle œuvre

Si vous souhaitez ajouter une nouvelle œuvre, vous pouvez le faire depuis Remix et la méthode *AddArtwork*. Les données à insérer sont :

Id (dernier id + 1),"Nom de l'oeuvre", "Nom de l'artiste", "nom de fichier de l'image"

Figure 34 : Fonction AddArtwork dans Remix



(Thibaud Rossetti)

Ajoutez ensuite l'image à la webapp en la copiant dans le répertoire */views/img/artworks/*. Veillez bien à ce que le nom de fichier de l'image soit le même dans la webapp et dans le smart contract

En actualisant la page de personnalisation vous verrez la nouvelle entrée apparaître.

2. Structure de la webapp

2.1 Répertoire *class*

Contient les différentes classes métiers ainsi que les constantes du projet.

2.1.1 apparel

Fournit les différentes ressources pour les produits (nom, image, prix). Dans le cas d'une mise en production, ces produits se trouveraient dans une base de données et cette classe devrait être adaptée. Pour cette raison, elle n'intègre pas la possibilité d'ajouter de nouveaux produits sans adaptation du code.

2.1.2 artwork

Classe d'objet métier représentant une œuvre.

2.1.3 order

Classe d'objet métier représentant une commande.

2.1.4 ordermanager

Gère l'enregistrement des commandes et écrit le résultat dans le fichier de sortie.

2.1.5 smartcontract

Gère la connexion au smart contract via Web3.js, récupère les données qu'il contient et le met à jour.

2.1.6 const.js

Contient toutes les constantes de la webapp.

2.2 Répertoire *config*

Contient les fichiers de configuration de la webapp.

2.2.1 config.json

Contient la configuration du server.

2.3 Répertoire data

Contient les données de sortie.

Rapport-Gratuit.com

2.3.1 orders.txt

Regroupe les différentes commandes effectuées par les utilisateurs.

2.4 Répertoire *node*_modules

Répertoire des différents modules Node nécessaires à l'application ainsi que leurs dépendances.

2.5 Répertoire *ressources*

2.5.1 router.js

Gestionnaire des différentes routes et contrôleur général de la webapp

2.6 Répertoire *views*

Contient les éléments envoyés au client comme les pages EJS, les feuilles de style, les images ou encore les polices d'écritures.

2.7 package.json

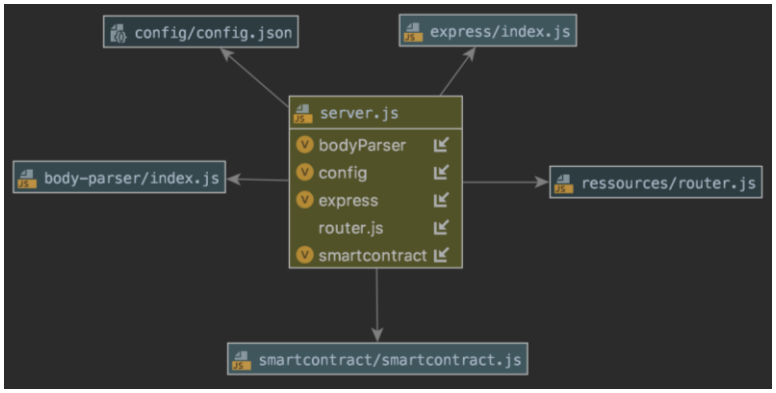
Regroupe les informations générales de la webapp ainsi que les dépendances des modules. Ce fichier permet de recréer le répertoire node_modules si ce dernier devait être supprimé.

2.8 server.js

Point d'entrée de l'application. Lance le serveur et la connexion au smart contract.

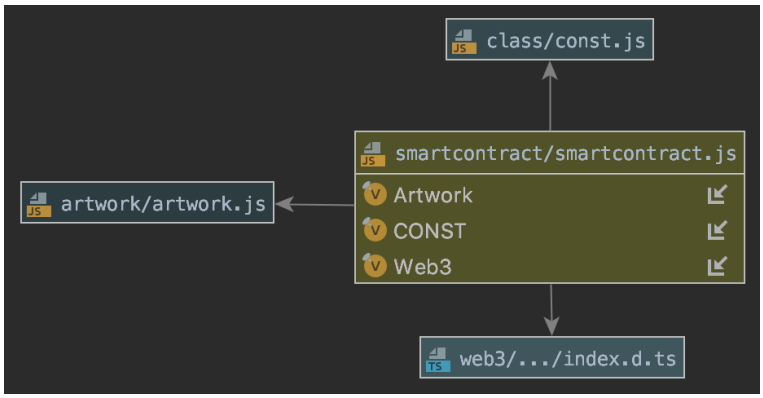
3. Diagrammes

Figure 35 : Diagramme des dépendances de *server.js*



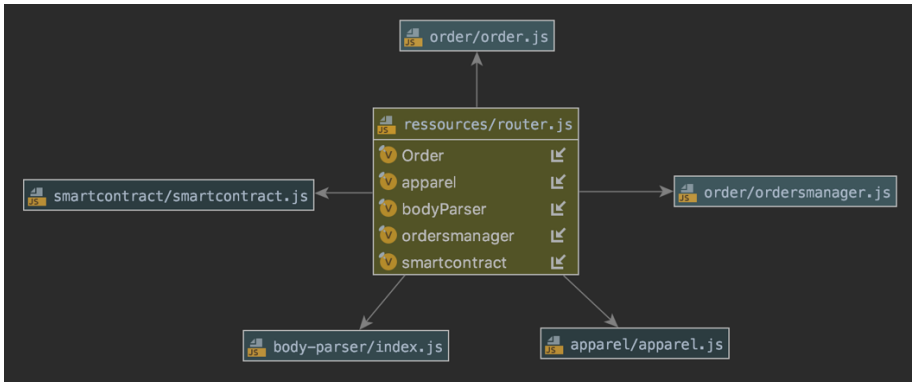
(Thibaud Rossetti)

Figure 36 : Diagramme des dépendances de smartcontract.js



(Thibaud Rossetti)

Figure 37 : Diagramme des dépendances de router.js



(Thibaud Rossetti)

Rapport-gratuit.com
LE NUMERO 1 MONDIAL DU MÉMOIRES

Annexe 2 : Glossaire

1. Vocabulaire spécifique à l'industrie de la mode

Tableau 2 : Vocabulaire spécifique à l'industrie de la mode

Terme	Définition
Pièce	Désigne un produit pouvant être un vêtement mais également un accessoire ou tout autre objet utilisé pour se vêtir.
Créateur	Désigne celui qui crée des collections de vêtements. Synonyme de *styliste* et *designer*.

(Thibaud Rossetti)

2. Vocabulaire spécifique à la technologie blockchain

Tableau 3 : Vocabulaire spécifique à la technologie blockchain

Terme	Définition
Token	Actif numérique échangeable au travers d'une blockchain.
Hash	Valeur de sortie d'une fonction d'encryption des données.
Protocole	Ensemble de règle permettant d'échanger des données.
Algorithme	Séquence d'opérations visant un but précis.
Mineur	Vérifie et ajoute des transactions sur le réseau.

(Thibaud Rossetti)