

Entreprise : QualyTrust

Contact : Jorge TELLEZ

Encadrant : Sophie CHABRIDON

Jordan TROESCH – Imane EL BAGDOURI

Rapport du Projet de fin d’Études

Sujet : Maquette d’une solution Blockchain pour l’assurance

# Sommaire

Introduction

I/Contexte et objectifs

Contexte

Objectifs du projet

Expression du besoin

II/Démarche du projet

Etape 1 : Etude préliminaire

Etape 2 : Réalisation du Proof Of Concept

Etape 3 : Réalisation du service

III/Bilan du projet

Résultats obtenus

Difficultés rencontrées

Conclusion

Introduction

Dans le cadre de notre projet de fin d’étude, nous avons choisi de travailler sur le sujet de la Blockchain. Il s’agit de la nouvelle lubie numérique de cette année qui suscite beaucoup d’intérêt pour ses applications dans des domaines variés tel que la banque ou l’assurance. Nous avons donc traité du sujet de la mise en place d’une maquette d’une solution Blockchain pour l’assurance. Le but est d’utiliser cette technologie de stockage et de transmission de l’information pour la gestion sécurisée des dossiers d’assurance. Notre client pour ce projet a été l’entreprise QualyTrust, une jeune entreprise qui met en œuvre une plateforme d’échange dans le domaine de l’assurance.

Le rapport qui suit présente le contexte et les objectifs de notre projet, son déroulement ainsi que les résultats obtenus et les difficultés que nous avons rencontrés.

I/Contexte et objectifs

# Contexte

QualyTrust est une jeune entreprise innovante qui développe une plateforme sécurisée de gestion des échanges dans le domaine de l'assurance. QualyTrust se pose en tiers de confiance entre tous les acteurs de l'assurance (clients, courtiers, assureurs, médecins conventionnés, ...) et propose des services de gestion de dossiers partagés et de gestion de workflow multi-acteurs.

L'objectif est de permettre de simplifier les échanges entre partenaires, garantir la confidentialité et la préservation de la vie privée, optimiser les processus afin de réduire les délais de traitement, offrir la traçabilité complète.

La plateforme est construite autour d'une solution de stockage sécurisée (basée sur un moteur NoSQL) et sur un moteur de workflow. Elle est complètement programmable et intégrable dans des systèmes d'informations existants grâce à un ensemble riche et complet d'API REST. QualyTrust a été primé au concours de l'innovation numérique 2016 de BPIFrance.

Pour assurer la gestion sécurisée de données partagées, QualyTrust veut évaluer les technologies de type Blockchain. Ces technologies sont surtout connues pour être la base de crypto-monnaie comme bitcoin mais peuvent être également utilisées comme répertoire partagé et sécurisé de stockage d'informations.

# Objectifs du projet

Dans ce projet, il s'agira d'une part de comprendre en détail ces technologies et ensuite de mettre en place un démonstrateur adapté à des cas d'usage de QualyTrust. Ce démonstrateur s'appuiera sur l'environnement développé par la startup rennaise [Woleet](https://woleet.io/).

Le projet se décompose donc en deux parties. La première consistera à tester et à effectuer un Proof Of Concept de la solution proposée par Woleet. La deuxième partie du projet consistera à développer une API permettant d’accéder à la solution de Woleet pour la création et la recherche d’ancres.

# Expression du besoin

Phase 1: Proof of Concept

Développement d’une solution simple s’appuyant sur la technologie de Woleet qui permet d’inscrire des données dans la Blockchain Bitcoin. Vérifier l’accessibilité des données dans cette Blockchain sans l’utilisation de Woleet.

Livrables :

* Code source
* POC et démonstration

### Phase 2 : Cas d’usage 1 : Signature électronique

Développement d’une API permettant d’accéder à la solution de Woleet pour ancrer des fichiers dans la Blockchain, ou rechercher les fichiers encrés.

Livrables :

* Code Source

I/Démarche du projet

# Notre projet s’est déroulé en trois étapes. Dans un premier temps, nous avons fait des recherches pour mieux comprendre la technologie Blockchain et ses applications, ainsi que l’usage qui en ai fait par Woleet. Nous avons ensuite testé la plateforme de la startup en réalisant un Proof Of Concept. Enfin, nous avons mis en place une API REST qui communique avec l’API de Woleet et qui permet de générer des ancres pour des fichiers, ou de rechercher les ancres déjà créées.

# 

Données de l’entreprise



Hash du fichier à encrer

Ancrage dans la Blockchain

JAVA CLIENT

# Étape 1 : Étude préliminaire

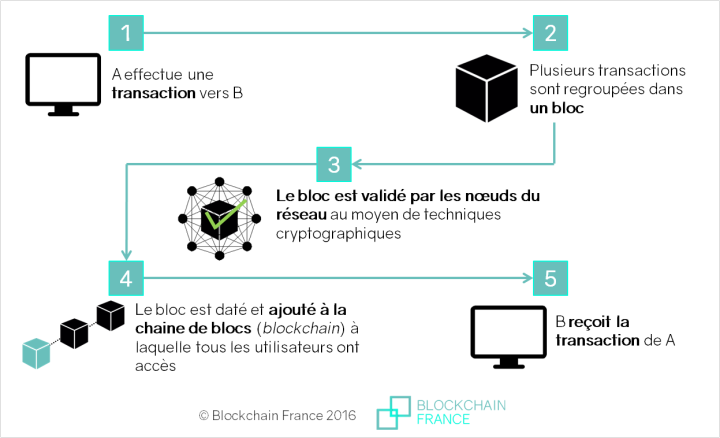
En premier lieu, nous devions comprendre comment fonctionne la technologie Blockchain et quels usages peuvent en être fait. Pour cela, nous avons consulté différentes sources, dont certaines fournies par notre encadrant entreprise.

Ce travail a permis d’étoffer nos connaissances sur le sujet étudié afin de répondre au mieux à la demande de l’entreprise.

Pour réaliser ce projet, il a également fallu comprendre la solution mise en place par Woleet. Il s’agit d’une startup rennaise qui met à disposition des utilisateurs une API REST permettant d’ancrer des fichiers dans la Blockchain de Bitcoin.

La technologie Blockchain

La Blockchain est une technologie de stockage et de transmission d’informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (*définition de Blockchain France*).

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.

La plateforme de Woleet

La solution mise en place par Woleet permet de créer des preuves d’existence de fichier. Il faut dans un premier temps générer le hash d’un fichier et lui associer un nom pour l’identifier. Le fichier réel n’est donc pas envoyé à la plateforme. Il n’y a donc pas de limitation pour la taille du fichier. Une ancre, qui est une preuve d’existence du fichier, est alors créée.

Les ancres sont enregistrées dans la Blockchain de Bitcoin. Une fois cette étape passée, il est possible de récupérer la preuve associée à l’ancre conforme au standard chainpoint. Cette preuve est l’unique donnée nécessaire pour prouver l’existence du fichier. Par la suite, l’utilisateur a uniquement besoin de vérifier que le hash du fichier correspond au hashproperty de la preuve d’existence.



# Étape 2 : Réalisation du Proof Of Concept

Une fois nos connaissances du sujet consolidées, nous avons réalisé un Proof of Concept (POC) basé sur l’API de Woleet. Ce POC permet de tester la plateforme pour ancrer un fichier et le rechercher. Il se compose de deux parties :

* Le java client AnchorGenerator permet de créer une ancre en prenant pour paramètre le chemin vers le fichier. Il retourne le contenu de l’ancre.

* Le java client AnchorSearch permet de rechercher une ancre dans la Blockchain Bitcoin à partir de son identifiant. Il retourne l’identifiant et le nom de l’ancre si elle existe.

Nous avons réalisé ce projet en Java sous Eclipse à l’aide de Maven. Ces technologies sont des standards sur le marché.

# Étape 3 : Réalisation de l’API

Pour s’intégrer au SI de QualyTrust, nous avons décidé de mettre en place une API Rest qui communique avec l’API de Woleet pour créer des ancres ou rechercher des fichiers.

Notre webservice nous permet donc d’ancrer des fichiers dans le bitcoin, de rechercher nos ancres, et de générer le hash d’un fichier avant son ancrage.

Nous nous sommes appuyés sur la librairie Dropwizard pour créer nos services REST car cette librairie est un standard dans le monde Java et possède une communauté active de développeurs.

I/Bilan du projet

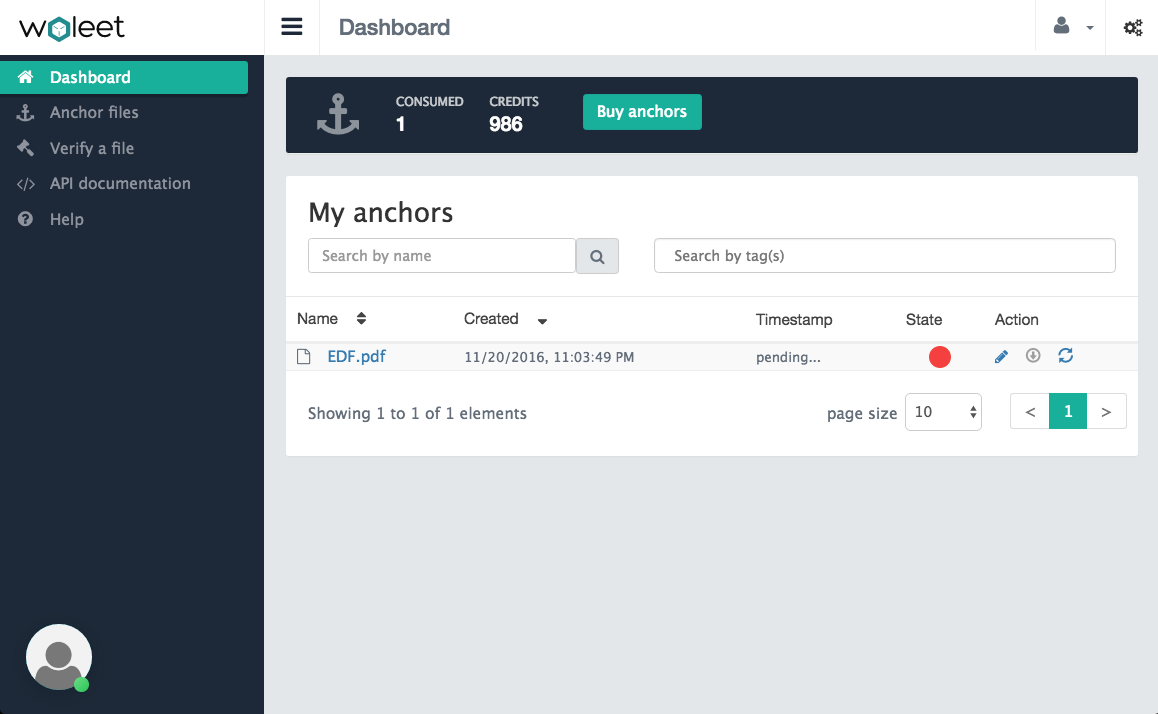
# Résultats obtenus

1. Proof Of Concept

La réalisation du POC a permis de montrer comment utiliser l’API de Woleet en Java pour ancrer des fichiers dans la Blockchain Bitcoin ou rechercher des fichiers ancrés.

Le code source est disponible sur GitHub : https://github.com/JorTro/Proof-Of-Concept-Blockchain-Qualytrus

Nous avons réussi à ancrer un fichier dans la Blockchain. Les fichiers ancrés sont visibles sur le site web de Woleet à travers le tableau de bord suivant :



1. API Rest

Le service que nous avons mis en place permet à Qualytrust de communiquer directement avec l’API de Woolet pour ancrer et rechercher des fichiers.

Le service est fonctionnel et le code source se trouve sur GitHub : <https://github.com/JorTro/PFE_Blockchain>. Le service ne répond pas à 100% aux attentes de Qualytrust, il représente néanmoins une bonne base pour un développement futur à partir du code que nous avons fourni.

# Difficultés rencontrées

La première difficulté que nous avons rencontrée est la difficulté technique. Nous étions en phase d’apprentissage et donc pas forcément à l’aise avec les technologies que nous utilisions au début du projet : Java, Maven, Blockchain ect…

Nous nous sommes donc formés sur ces technologies.

De plus, nous avons découvert et appris à travailler avec des services REST en cours de projet grâce à notre formation. Nous nous sommes donc appuyés sur cette expérience pour coder nos propres services à l’aide de la libraire Dropwizard qui nous a été présentée en conférence.

La deuxième difficulté que nous avons rencontrée est la communication avec l’entreprise.

L’une des difficultés du projet de fin d’études est de concilier la vision d’étudiant avec le monde professionnel, nous n’avions pas les mêmes objectifs, les mêmes horaires, ni les mêmes disponibilités.

Nous avons donc perdu beaucoup de temps entre chaque prise de contact et rendez-vous, ce qui a probablement nuit à la qualité du projet.

Bien que nous sommes satisfaits du travail que nous avons fournis, nous pensons que nous aurions pu aller beaucoup plus loin et fournir un service totalement opérationnel et correspondant mieux aux attentes de Qualytrust si nous avions amélioré nos méthodes de communication et de travail avec l’entreprise.