

Mémoire d'ingénieur

Implémentation d'un service de trust list global basé
sur la blockchain

Yoann Raucoules

Année 2016–2017

Stage de fin d'études réalisé dans l'entreprise ARHS Spikeseed
en vue de l'obtention du diplôme d'ingénieur de TELECOM Nancy

Maître de stage : Vincent Bouckaert

Encadrant universitaire : Olivier Festor

Déclaration sur l'honneur de non-plagiat

Je soussigné(e),

Nom, prénom : Raucoules, Yoann

Élève-ingénieur(e) régulièrement inscrit(e) en 3^e année à TELECOM Nancy

Numéro de carte de l'étudiant(e) : 1205028998

Année universitaire : 2016–2017

Auteur(e) du document, mémoire, rapport ou code informatique intitulé :

Implémentation d'un service de trust list global basé sur la blockchain

Par la présente, je déclare m'être informé(e) sur les différentes formes de plagiat existantes et sur les techniques et normes de citation et référence.

Je déclare en outre que le travail rendu est un travail original, issu de ma réflexion personnelle, et qu'il a été rédigé entièrement par mes soins. J'affirme n'avoir ni contrefait, ni falsifié, ni copié tout ou partie de l'œuvre d'autrui, en particulier texte ou code informatique, dans le but de me l'accaparer.

Je certifie donc que toutes formulations, idées, recherches, raisonnements, analyses, programmes, schémas ou autre créations, figurant dans le document et empruntés à un tiers, sont clairement signalés comme tels, selon les usages en vigueur.

Je suis conscient(e) que le fait de ne pas citer une source ou de ne pas la citer clairement et complètement est constitutif de plagiat, que le plagiat est considéré comme une faute grave au sein de l'Université, et qu'en cas de manquement aux règles en la matière, j'encourrais des poursuites non seulement devant la commission de discipline de l'établissement mais également devant les tribunaux de la République Française.

Fait à Luxembourg, le 26 juillet 2017

Signature :

Mémoire d'ingénieur

Implémentation d'un service de trust list global basé sur la blockchain

Yoann Raucoules

Année 2016–2017

Stage de fin d'études réalisé dans l'entreprise ARHS Spikeseed
en vue de l'obtention du diplôme d'ingénieur de TELECOM Nancy

Yoann Raucoules
6, rue du général Frère
57070, METZ
+33 (0)6 77 48 04 38
yoann.raucoules@telecomnancy.eu

TELECOM Nancy
193 avenue Paul Muller,
CS 90172, VILLERS-LÈS-NANCY
+33 (0)3 83 68 26 00
contact@telecomnancy.eu

ARHS Spikeseed
2B, rue Nicolas Bové
1253, LUXEMBOURG
+352 26 11 02 1



Maître de stage : Vincent Bouckaert

Encadrant universitaire : Olivier Festor

Remerciements

*“Night gathers, and now my watch begins.
It shall not end until my death.*

*I shall take no wife, hold no lands, father no children.
I shall wear no crowns and win no glory.
I shall live and die at my post.*

*I am the sword in the darkness.
I am the watcher on the walls.
I am the shield that guards the realms of men.*

*I pledge my life and honor to the Night’s Watch,
for this night and all the nights to come.”*

– The Night’s Watch oath

Avant-propos

Ce mémoire résulte d'un stage de fin d'études qui s'est déroulé du 3 avril 2017 au 30 septembre 2017 au sein de l'entreprise Arns Spikeseed située au Luxembourg. Ce stage vient clôturer et valider la formation d'ingénieur du numérique de l'école TELECOM Nancy que j'ai débuté en septembre 2014. Cette formation qui s'est étendue sur une période de trois ans m'a permis d'acquérir de nombreuses compétences dans les domaines de l'informatique, des mathématiques, du management, de la gestion de projet, de la communication, de l'économie, du droit et des langues. J'ai choisi de me spécialiser en Ingénierie Logicielle au cours du cursus de par ma passion pour la programmation et l'architecture logicielle depuis que j'ai découvert l'informatique lors de mon stage de découverte professionnelle réalisé en classe de troisième.

Au cours de ce stage, j'ai eu le plaisir de travailler sur une technologie à laquelle je m'intéresse depuis deux ans, la blockchain. Dans le cadre d'un projet proposé par la Commission Européenne, nommé FutureTrust, j'ai pu concevoir et implémenter un service de trust list global basé sur la blockchain. Mes tâches ont été de me familiariser avec les principes de la blockchain et les concepts de cryptographie appliquée afin de les mettre en application dans le projet, d'effectuer une analyse des solutions de blockchain existantes afin de réaliser des choix d'implémentation, de concevoir l'architecture du service de trust list global, d'implémenter la solution conçue et de documenter tous les aspects techniques et fonctionnels de la solution implémentée.

Dans ce mémoire est présenté le résultat du stage de fin d'études et est mis en avant l'utilisation de la blockchain dans le cadre d'un projet de confiance numérique d'échelle mondiale. L'intérêt de ce document est dans un premier temps d'expliquer les tâches réalisées au cours du stage et dans un second temps de montrer qu'il est possible d'élargir le champ d'application de la technologie blockchain et des différents aspects qui la composent.

Table des matières

Remerciements	v
Avant-propos	vii
Table des matières	ix
1 Introduction	1
1.1 Présentation de la technologie blockchain	1
1.2 Définition du cadre et des objectifs du stage	1
1.3 Mise en exergue du plan	2
2 Présentation du contexte	3
2.1 L'entreprise Arns SpikeSeed	3
2.2 Le contexte du projet	3
3 Présentation détaillée de la problématique	4
4 État de l'art des solutions envisagées	5
5 Analyse du problème et solution élaborée	6
6 Réalisation, présentation et validation de la solution proposée	7
7 Résultats obtenus & Perspectives	8
8 Conclusion	9
9 Exemples Listings	11
10 Autre chapitre	15
10.1 Autre section	15
10.1.1 Première sous-section	15

11 Conclusion	17
Bibliographie / Webographie	19
Liste des illustrations	21
Liste des tableaux	23
Listings	25
Glossaire	27
 Annexes	 30
A Première Annexe	31
B Seconde Annexe	33
Résumé	35
Abstract	35

1 Introduction

La technologie blockchain s'est popularisée ces dernières années grâce à l'expansion de la crypto-monnaie Bitcoin [1] à travers le monde. En effet, cette technologie a bouleversé aussi bien le monde de l'informatique que le monde de la finance. L'investissement autour de la blockchain a mené à un engouement général pour ce concept. Le Bitcoin a réussi à remettre en cause des acteurs majeurs de notre société tels que les banques ou les géants du Web, en sécurisant des échanges d'actifs sans organe central de contrôle. La révolution qu'il a engendré amène aujourd'hui les gouvernements et autres organisations publiques à réfléchir sur la régulation de la technologie et des crypto-monnaies naissantes. Depuis son lancement en 2009, la blockchain n'a cessé d'évoluer et d'étendre son champ d'application. Bien qu'à l'origine elle a été conçue pour le transfert de crypto-monnaie, les avantages qu'elle apporte permettent d'imaginer de multiples cas d'utilisation qui dépassent son cadre initial d'échanges d'actifs.

1.1 Présentation de la technologie blockchain

Une blockchain est basée sur l'échange d'actifs numériques, réalisé grâce à des transactions signées, et agit comme un registre publique distribué où toutes les transactions y sont répertoriées. Elle repose sur des principes de cryptographie afin d'assurer l'intégrité de ces transactions et sur un protocole décentralisé, dit *peer-to-peer*, qui permet à la blockchain d'avoir une disponibilité maximale et d'établir un consensus entre les participants du réseau afin de protéger contre les falsifications. Si cette technologie connaît un tel succès c'est parce qu'elle apporte de nombreux avantages : la décentralisation, qui signifie que son architecture ne repose pas sur une entité centrale et permet d'enregistrer des données dans un réseau distribué ; la transparence, puisque l'état des données conservées est consultable publiquement par tout le monde ; l'autonomie, puisqu'elle est basée sur un consensus dans lequel chaque partie prenante peut transférer des données de manière sécurisée et autonome ; l'immuabilité, en effet toute transaction est persistée définitivement et donc ne peut être effacée ; l'anonymat, car toute personne est anonyme dans le sens où elle n'est pas désignée par son identité mais uniquement par une clé publique.

1.2 Définition du cadre et des objectifs du stage

Dans ce contexte, un stage ingénieur a été réalisé sur une période de 6 mois au sein de la société Arqs SpikeSeed située au Luxembourg. Le stage a été réalisé dans les locaux de l'entreprise, la langue officielle du projet pour les communications avec les autres membres du consortium (mails, documents, conférence téléphonique) est l'anglais, il en est de même pour la langue utilisée au sein de l'équipe puisque c'est une équipe multinationale. Ce stage de fin d'études a pour objectif d'intégrer la technologie blockchain au sein d'un processus de gestion de listes de confiance

dans le cadre d'un règlement européen. La finalité est d'utiliser cette technologie afin de conserver des données publiques relatives à la confiance électronique de manière sécurisée et décentralisée en utilisant une blockchain en tant que registre. Cela a pour but d'assurer la disponibilité et l'intégrité des informations, puisque les données sont distribuées à travers les nœuds de réseau et sécurisées à l'aide de transactions signées et vérifiées par une preuve mathématique.

1.3 Mise en exergue du plan

Ce mémoire vise à montrer que le champ d'application de la technologie blockchain dépasse son cadre initial et que son utilisation permet de pallier aux problèmes d'architecture et de sécurité des modèles actuels. Dans un premier temps, le contexte du projet sera défini, puis la problématique, qui détaillera les limites des architectures actuelles, sera exposée. Ensuite, sera établi un état de l'art afin de comparer les outils existants et de justifier les choix opérés durant le stage. Après cela, la réalisation du projet sera développée en expliquant : le choix de l'architecture mise en place ; l'avantage de persister des données dans un système de fichiers décentralisé ; l'intérêt de gérer l'authentification des utilisateurs par la mise en place d'un consensus ; l'implémentation d'un système de contrôle de versions et d'un moteur de recherche sur des données stockées dans un réseau décentralisé et distribué. Enfin, les résultats obtenus et les perspectives du projet seront détaillés.

2 Présentation du contexte

2.1 L'entreprise Arns Spikeseed

Arns Spikeseed est une entité du groupe Arns qui est une entreprise de services du numérique (ESN) fondée en 2003 par Jourdan Serderidis. Le groupe est divisé en sociétés réparties au Luxembourg, en Belgique, en Grèce et depuis cette année en Italie. Comme toutes les autres entités du groupe, Arns Spikeseed vise à délivrer des solutions numériques complexes. Elle a la particularité de réaliser principalement des projets de recherche et développement en s'appuyant sur les pratiques agiles et des technologies de pointe. De plus, Arns Spikeseed est compétente afin de mettre en œuvre : des solutions liées à la confiance numérique ; des systèmes engageant des masses de données grâce à des technologies innovantes et efficaces comme le Web sémantique ou la Business intelligence ; des applications destinées aux mobiles et aux objets connectés.

2.2 Le contexte du projet

Dans le cadre d'un règlement de l'Union Européenne (UE) sur l'identification électronique (eID) et les services de confiance pour les transactions électroniques sécurisées au sein de l'UE (eIDAS), la Commission Européenne (CE) a émis un appel à projet qui a pour visée de supporter la mise en œuvre technique du règlement européen. Ce projet de recherche et développement appelé FutureTrust rassemble un consortium de seize partenaires, dont Arns Spikeseed, engagé dans la réalisation et la mise en application du règlement européen. Le projet FutureTrust répondra au besoin de solutions globales et interopérables, en fournissant des logiciels libres qui faciliteront l'utilisation de l'identification et de la signature électronique. Il vise à étendre l'infrastructure de la liste européenne de services de confiance existante vers une liste globale de services de confiance (gTSL), à développer un service de validation ainsi qu'un service d'archivage pour les signatures et les sceaux électroniques, et à fournir des composants pour les certificats qualifiés et pour la création de signatures et de sceaux dans un environnement mobile.

Ce stage de fin d'études a porté sur l'intégration la technologie blockchain dans le cadre du projet FutureTrust et plus particulièrement sur son intégration dans le module de gTSL. Les autres modules du projet ne seront pas détaillés dans ce document.

3 Présentation détaillée de la problématique

Détail du sujet

Détailler l'architecture existante : "La finalité du stage est de d'effectuer une refonte de l'architecture actuelle qui a montré ses limites en y apportant des technologies innovantes."

décentralisation, pour éviter le single point of failure -> actuellement LOTL est le single point of failure

distribué, afin de maintenir les données dans l'ensemble du réseau -> actuellement chaque Member State maintient ses propres de données ce qui veut dire que si le noeud d'un Member State tombe, ses données ne sont plus disponibles

sécurité, intégrité des données + consensus -> actuellement, une partie des données est stockée dans une BD, l'autre partie sont des fichiers XML répartis sur plusieurs endpoints, difficile de vérifier l'intégrité des données de tous les endpoints en effet si un Member State est corrompu on ne peut pas le savoir

résilience, réseau publique avec +1M de noeuds jamais down -> actuellement l'architecture client-serveur repose entièrement sur la LOTL (qui agit comme un point central, donc à éviter) + chaque noeud est indépendant et se gère seul mais pb de résilience "globale" si un noeud est down

Enoncer clairement la problématique en une phrase : "Décentraliser le modèle actuel afin de résoudre les pbs de résilience, sécurité... grâce à un réseau décentralisé et distribué"

4 État de l'art des solutions envisagées

Enoncer le principal désavantages de la blockchain qui est son coût (cf. Ethereum & IPFS integration).

Etat de l'art : Comparison document + Design document

5 Analyse du problème et solution élaborée

6 Réalisation, présentation et validation de la solution proposée

7 Résultats obtenus & Perspectives

8 Conclusion

9 Exemples Listings

Il est aisé d'insérer du code dans un rapport. Il suffit de définir le langage, la légende à afficher et enfin un Label pour pouvoir y faire référence. Le résultat est donnée dans le listing 9.1. Il est également possible de changer les couleurs, pour cela il faut éditer le lstset dans la classe tnreport.cls.

```
1 void CEquation::IniParser ()
2 {
3     if (!pP){ //if not already initialized ...
4         pP = new mu::Parser;
5
6         pP->DefineOpert("%", CEquation::Mod, 6); //deprecated
7         pP->DefineFun("mod", &CEquation::Mod, false);
8         pP->DefineOpert("&", AND, 1); //DEPRECATED
9         pP->DefineOpert("and", AND, 1);
10        pP->DefineOpert("|", OR, 1); //DEPRECATED
11        pP->DefineOpert("or", OR, 1);
12        pP->DefineOpert("xor", XOR, 1);
13        pP->DefineInfixOpert("!", NOT);
14        pP->DefineFun("floor", &CEquation::Floor, false);
15        pP->DefineFun("ceil", &CEquation::Ceil, false);
16        pP->DefineFun("abs", &CEquation::Abs, false);
17        pP->DefineFun("rand", &CEquation::Rand, false);
18        pP->DefineFun("tex", &CEquation::Tex, false);
19
20        pP->DefineVar("x", &XVar);
21        pP->DefineVar("y", &YVar);
22        pP->DefineVar("z", &ZVar);
23    }
24 }
```

Listing 9.1 – Premier Exemple

Il est également possible d'afficher du code directement depuis un fichier source, le résultat de cette opération est visible dans le listing 9.2

```
1 void CEquation::IniParser()
2 {
3     if (!pP){ // if not already initialized ...
4         pP = new mu::Parser;
5
6         pP->DefineOpert("%", CEquation::Mod, 6); // deprecated
7         pP->DefineFun("mod", &CEquation::Mod, false);
8         pP->DefineOpert("&", AND, 1); //DEPRECATED
9         pP->DefineOpert("and", AND, 1);
10        pP->DefineOpert("|", OR, 1); //DEPRECATED
11        pP->DefineOpert("or", OR, 1);
12        pP->DefineOpert("xor", XOR, 1);
13        pP->DefineInfixOpert("!", NOT);
14        pP->DefineFun("floor", &CEquation::Floor, false);
15        pP->DefineFun("ceil", &CEquation::Ceil, false);
16        pP->DefineFun("abs", &CEquation::Abs, false);
17        pP->DefineFun("rand", &CEquation::Rand, false);
18        pP->DefineFun("tex", &CEquation::Tex, false);
19
20        pP->DefineVar("x", &XVar);
21        pP->DefineVar("y", &YVar);
22        pP->DefineVar("z", &ZVar);
23    }
24 }
```

Listing 9.2 – Affichage depuis le fichier source

De nombreux langages sont supportés :

ABAP2,4, ACSL, Ada4, Algol4, Ant, Assembler2,4, Awk4, bash, Basic2,4, C#5, C++4, C4, Caml4, Clean, Cobol4, Comal, csh, Delphi, Eiffel, Elan, erlang, Euphoria, Fortran4, GCL, Gnuplot, Haskell, HTML, IDL4, inform, Java4, JVMIS, ksh, Lisp4, Logo, Lua2, make4, Mathematica1,4, Matlab, Mercury, MetaPost, Miranda, Mizar, ML, Modelica3, Modula-2, MuPAD, NASTRAN, Oberon-2, Objective C5 , OCL4, Octave, Oz, Pascal4, Perl, PHP, PL/I, Plasm, POV, Prolog, Promela, Python, R, Reduce, Rexx, RSL, Ruby, S4, SAS, Scilab, sh, SHELXL, Simula4, SQL, tcl4, TeX4, VBScript, Verilog, VHDL4, VRML4, XML, XSLT.

Il est néanmoins possible de définir le sien, il faudra alors ajouter dans la classe `tnreport.cls` du code ressemblant au listing 9.3. On y définit les différents mots-clés, ainsi que les délimiteurs des chaînes de caractère et des commentaires.

```
1 \lstdefinlanguage{amf}
2 {keywords=
3   {
4     xml,
5     amf,
6     volume,
7     material,
8     coordinates,
9     vertices,
10    vertex,
11    triangle,
12    x,
13    y,
14    z,
15    v1,
16    v2,
17    v3,
18    mesh,
19    object,
20    constellation,
21    metadata,
22    color,
23    texmap,
24    texture,
25    utex1,
26    utex2,
27    utex3,
28    instance,
29    deltax,
30    deltay,
31    deltaz,
32    r,
33    g,
34    b,
35    rx,
36    ry,
37    rz,
38    composite
39  },
40  sensitive=false,
41  morestring=[b]",
42  comment=[s]{<!--}{-->}
43 }
```

Listing 9.3 – Syntaxe définition d'un langage

10 Autre chapitre

10.1 Autre section

Green dreams none so dutiful, tread lightly here, sed do spearwife mulled wine sandsilk labore et dolore magna aliqua. Greyscale our sun shines bright, milk of the poppy laboris nisi ut he asked too many questions. Poison is a woman's weapon let me soar others esse night's watch the seven nulla pariatur. Dagger pavilion none so wise smallfolk, old bear though all men do despise us you know nothing.

10.1.1 Première sous-section

Première sous-sous section

Exemple d'illustration :



FIGURE 10.1 – Logo de TELECOM Nancy

La Figure 10.1 représente le logo de TELECOM Nancy.

Ceci est une référence bibliographique [?].

11 Conclusion

Bibliographie / Webographie

- [1] Satoshi Nakamoto. *Bitcoin : A Peer-to-Peer Electronic Cash System*. 2008. 1

Liste des illustrations

10.1	Logo de TELECOM Nancy	15
------	---------------------------------	----

Liste des tableaux

Listings

9.1	Premier Exemple	11
9.2	Affichage depuis le fichier source	12
9.3	Syntaxe définition d'un langage	13

Glossaire

Annexes

A Première Annexe

B Seconde Annexe

Résumé

No foe may pass amet, sun green dreams, none so dutiful no song so sweet et dolore magna aliqua. Ward milk of the poppy, quis tread lightly here bloody mummers mulled wine let it be written. Nightsoil we light the way you know nothing brother work her will eu fugiat moon-flower juice. Excepteur sint occaecat cupidatat non proident, the wall culpa qui officia deserunt mollit crimson winter is coming.

Moon and stars lacus. Nulla gravida orci a dagger. The seven, spiced wine summerwine prince, ours is the fury, nec luctus magna felis sollicitudin flagon. As high as honor full of terrors. He asked too many questions arbor gold. Honeyed locusts in his cups. Mare's milk. Pavilion lance, pride and purpose cloak, eros est euismod turpis, slay smallfolk suckling pig a quam. Our sun shines bright. Green dreams. None so fierce your grace. Righteous in wrath, others mace, commodo eget, old bear, brothel. Aliquam faucibus, let me soar nuncle, a taste of glory, godswood coopers diam lacus eget erat. Night's watch the wall. Trueborn ironborn. Never resting. Bloody mummers chamber, dapibus quis, laoreet et, dwarf sellsword, fire. Honed and ready, mollis maid, seven hells, manhood in, king. Throne none so wise dictumst.

Mots-clés :

Abstract

Green dreams mulled wine. Feed it to the goats. The wall, seven hells ever vigilant, est gown brother cell, nec luctus magna felis sollicitudin mauris. Take the black we light the way. Honeyed locusts ours is the fury smallfolk. Spare me your false courtesy. The seven. Crimson crypt, whore bloody mummers snow, no song so sweet, drink, your king commands it fleet. Raiders fermentum consequat mi. Night's watch. Pellentesque godswood nulla a mi. Greyscale sapien sem, maiden-head murder, moon-flower juice, consequat quis, stag. Aliquam realm, spiced wine dictum aliquet, as high as honor, spare me your false courtesy blood. Darkness mollis arbor gold. Nullam arcu. Never resting. Sandsilk green dreams, mulled wine, betrothed et, pretium ac, nuncle. Whore your grace, mollis quis, suckling pig, clansmen king, half-man. In hac baseborn old bear.

Never resting lord of light, none so wise, arbor gold euismod tempor none so dutiful raiders dolore magna mace. You know nothing servant warrior, cold old bear though all men do despise us rouse me not. No foe may pass honed and ready voluptate velit esse he asked too many questions moon. Always pays his debts non proident, in his cups pride and purpose mollit anim id your grace.

Keywords :