République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UniversitéAMO de Bouira

Faculté des Sciences et des Sciences Appliquées

Département d'Informatique

Mémoire de Master

En Informatique

Spécialité *: GSI*

Thème

Sécurisation des communications dans les réseaux sociaux décentralisée

Encadré par

- Monsieur BADIS Lyes

Réalisé par

- DAHMANI Said
- HAMMADI Sofiane

2017/2018

Remerciements

Tout d'abord, nous tenons à remercier Allah, le clément et le miséricordieux de nous avoir donné la force et le courage de mener à bien ce travail

*Nous voudrions exprimer nos vifs remerciements à notre encadreur**Mr.Badis Lyes et Dr. Amad Mourad**, pour ses orientations, ses encouragements, sa disponibilité et ses précieux conseils qui nous ont permis de mener àbien ce travail.*

Nous tenons à remercier les membres du jury qui ont bien voulu accepter de juger notre modeste travail.

Nos remerciements s'adressent également à tous les enseignantsdudépartementinformatique ayant participé d'une manière ou d'une autre à notre formation master et licence.

A la fin nos remerciements les plus sincères à toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année Universitaire...

Dédicaces

Ce modeste travail est dédié à :

A celle qui a été toujours la source de grande affection...ma MEREque dieu paix à son âme.

A celui quia été toujours la source d'inscription, de courage a tout le long de mes études...mon PERE.

A tous mes frères et ma sœur.

A toutes ma famille (DAHMANI) et mes proches.

A tous mes amis sons exception.

A toute la promotion informatique 2017/2018 que je leurs souhaite un bon avenir.

A tous mes collègues au travail (CEM djohri ali –la gare aomar-).

A tous ceux qui m'ont aidé de près ou de loin à la réalisation de ce modeste travail.

DAHMANI SAID.

Dédicaces

Louange à Dieu, le miséricordieux, sans Lui rien de tout cela n'aurait pu être.

À mes chers parents qui m'ont aidé à accomplir ce travail

À la petit fille de mon frère « Meryoma »

À mon cher frère et mes chères sœurs.

A toute ma grande famille.

A tous mes amis..

HAMMADI Sofiane.

Resumé

Les reseaux sociaux centralisés telque Facebook, Twiter, Instagram.. .ont fait du monde un petit village, malgré leurs performances, il menace la vie privée des utilisateurs, Les chercheurs proposent les réseaux sociaux décentralisés comme solution. Dans notre travail on va participer dans l'amélioration des RSD on proposants des techniques pour sécuriser l'authentification à l'aide de la technologie Blockchain et la fonction de hachage SHA-256.

Mots clés : Réseau sociaux décentralisés (RSD), Authentification, Blockchain, SHA-256

Abstract

Centralized social networks as Facebook, Twiter, Instagram ... have made the world a small village, despite their performances, it menaces the users privacy, So Researchers propose decentralized social networks as a solution. In our work we will participate in the improvement of RSD by proposing techniques to secure authentication using Blockchain technology and SHA-256 hash function.

Keywords: Decentralized Social Networks (RSD), Authentication, Blockchain, SHA-256

Table des matières

Table des matières v

Liste des figures ix

Liste des tableaux xi

Liste des algorithmes xii

Liste des abréviations xiii

Introduction générale 1

1. Généralité sur les réseaux sociaux 2

.1.1 Introduction 2

.1.2 Historique 2

1.3. Définition 4

1.4. Fonctionnalités 6

1.5. Application des réseaux sociaux 9

1.6. Types de réseaux sociaux 10

1.6.1. Réseaux généraliste/ Réseaux spécialisé 11

1.6.2. Réseaux de relations /réseaux de contenu 12

1.6.3. Classiffication a base des objectifs 12

1.6.4. Classiffication basée sur l'usage 13

1.6.5. Classification de Delcroix 15

1.7. Avantages et Inconvénients 15

1.8. Exemples de réseaux sociaux 17

1.9. Les statistiques 19

1.10. Conclusion 25

2. Réseaux Sociaux Décentralisé 26

2.1. Introduction 26

2.2. Définition 27

2.3. Raisons d'utilisation de réseaux sociaux décentralisés 29

2.4. Décentralisation, réseaux sociaux et protection des données personnelles 32

2.5. Vers des réseaux sociaux décentralisés 33

2.6. Composants DOSN 34

2.7. Les Exemples de DOSN [31] 35

2.8. Architecture DOSN 36

2.9. Conclusion 41

3. La technologie des chaines du bloc « Blockchain » 42

3.1. Introduction 42

3.2. Historique 43

.3.3 Principe de fonctionnement 44

3.3.1. Un bloc 44

3.3.2. Blockchain 45

3.4. Mécanisme du blockchain 45

3.5. Avantages et inconvénients du blockchain 48

3.5.1. Avantages de la blockchain 48

3.5.2. Les inconvénients du blockchain 50

3.6. Autre application des blockchaine 51

3.6.1. Médicaments tracés et dossiers médicaux certifiés 51

3.6.2. Officialiser et sécuriser les cadastres 51

3.6.3. Assurance 52

3.6.4. Reseaux sociaux 53

3.7. Conclusion 53

4. Gérer l'authentification dans un réseau social décentralisé à l'aide de blockchaine 55

4.1. Introduction 55

4.2. Authentification dans un réseau social centralisé 55

4.2.1. Définition 55

4.3. Motivation 56

4.4. Contribution 56

4.4.1. Présentation 56

4.4.2. Principe de fonctionnement 56

A. Le contenu du bloc 57

B. Création d'un bloc 58

C. Processus d'authentification 59

4.4.3. Blockchain dans tous les nœuds « broadcast » 60

A. Les limites 62

B. Constat 62

4.4.4. Blockchain chez les amis « Clusturing » 63

A. Limites 64

B. Constat 65

4.4.5. Tout la Blockchain dans des supers nœuds « Nœud de sauvetage » 65

A. Le contenu du bloc 65

B. La création de bloc 66

C. Authentification d'un nœud par l'entité de confiance 67

D. Le cas des liens d'amitiés 67

E. Les limites 71

F. Constat 71

4.4.6. Gestion de mot de passe 71
4.5. Conclusion 72
5. Implémentation **74**
5.1. Introduction 74
5.2. Outils de développement 74
5.2.1. Langage JAVA 74
5.2.2. IDE NetBeans 74
5.2.3. Bibliothéque gson-2.6.2 75
5.3. Fonctionnement d'application 75
5.3.1. Inscription 76
5.3.2. L'authentification 79
5.3.3. Les fonctions 81
5.3.4. Conclusion 85
Conclusion générale et perspectives **86**
Bibliographie **87**

Liste des figures

Figure 1 : Panorama des médias sociaux [18] 13

Figure 2 : Des statistiques sur l'utilisation de télephone portable [29] 20

Figure 3 : Des statistiques sur les appareils les plus connecteé a l'internet [29] 20

Figure 4: Des statistiques sur l'utilisation de facebook par différantes appareils [29] 21

Figure 5 : Des statistiques sur la croissance annuelle des utilisateurs des réseaux sociaux dans les pays [29] 22

Figure 6 : Des statistiques sur l'age et sexe des utilisateurs de Facebook [29] 22

Figure 7 : Classement de la parité hommes-femmes sur Facebook par pays [29] 23

Figure 8 : Des statistiques sur les utilisateurs actifs dans les plateformes sociales mondiales [29] 24

Figure 9 : Top applications de messagerie par pays [29] 24

Figure 10 : Des statistiques sur l'age et sexe des utilisateurs d'Instagram [29] 25

Figure 11 : Illustration de la décentralisation 27

Figure 12 : différence entre la centralisation et la décentralisation [44] 28

Figure 13 : L'application connectée avec Facebook peut accéder à la donnée privée des utilisateurs facebook [49] 32

Figure 14 : Architectuer pour DOSN [31] 34

Figure 15 : Un bloc contient des transaction [42] 44

Figure 16 : Réalisation de la preuve de travail trouvée en N essais[43] 47

Figure 17 : Processus exécution d'une transaction avec la technologie Blockchain 48

Figure 18 : Blockchain de deux blocs 57

Figure 19 : Structure d'un simple bloc 58

Figure 20 : Processus de création d'un bloc 58

Figure 21 : L'authentification par Blockchain d'appareil 59

Figure 22 : Processus d'authentification broadcast 61

Figure 23 : Processus d'authentification par les liens d'amitié 63

Figure 24 : Structure de bloc dans la Blockchain de super noeud 65

Figure 25 : Authentification par les trois possibilités... 70

Figure 26 : Le bloc complet 71

Figure 27 : L'interface Login... 75

Figure 28 : Interface d’inscription.. 76

Figure 29 : message d'erreur.. 76

Figure 30 : Enregistrement des ifnoramtions 77

Figure 31 : interface d'authentification.. 79

Figure 32 : vérification d'existence de deux champs.. 79

Figure 33 : vérification d'existence d'empreinte... 80

Figure 34 : La réussite d’authentification 81

Figure 35 : L'utilisateur accéde à son compte. 81

Liste des tableaux

Tableau 1: La différance entre la centralisation et la décentralisation [43] 28

Tableau 2 : Caractéristiques des RSD 39

Liste des algorithmes

Algorithme 1 : Création de bloc 59

Algorithme 2 : Authentification à partir d'appareil 60

Algorithme 3 : Authentification par la technique broadcast 61

Algorithme 4 : l'authentification par amis 64

Algorithme 5 : Création d’un bloc dans Blockchain de l’entité de confiance 66

Algorithme 6 : Authentification par l’entité de confiance 68

Algorithme 7 : Changement de mot de passe 72

Liste des abréviations

ABE (Attribute-based encryption) Algorithme de chiffrement

API (Application Programming Interface)

DHT (Distributed Hash Table)

DOSN (Decentralized Online Social Networks)

OpenDHT (Open Distributed Hash Table)

OSN (Online Social Networks)

P2P (Per To Per)

PDG (Président Directeur Général)

POD: point of delivery

SIR (social information retrieval)

SMS (Short Message Service)

SNP (Social Network Provider)

RSD (Réseaux Sociaux Décentraliser)

TIS (Trusted Identity Service)

Introduction générale

L'émergence de l'Internet et le développement des moyens de communication sont apparus sur plusieurs sites de messagerie et de chat entre les gens, ainsi que sur l'émergence du concept de réseau social sur le Web. Les sites suivants sont spécialisés dans la communication entre les gens, le premier Myspace et le plus célèbre Facebook, et se répandent terriblement lorsque l'émergence des smartphones et des applications mobiles : ils ont fait du monde un petit village.

Bien qu'ils présentent des avantages, ils ont un côté dangereux que les entreprises ont exploité d'une manière ou d'une autre la vie privé des utilisateurs. La plupart des sociétés des réseaux sociaux vendent les données des utilisateurs sauvegardées dans ces serveurs à des agences de publicité ou à des entreprises commerciales.

C'est la principale raison de l'émergence de l'autre type de média social décentralisé, ou y'a pas un serveur qui gère tous, mais chaque utilisateur jeu le rôle d'un client et d'un serveur ou même temps. Une architecture décentralisée d'un réseau social doit définir clairement les aspects : stockage, sécurité et communication. Notre travail est une contribution dans les performances de la sécurité des réseaux sociaux décentralisés.

Ce mémoire est structuré en cinq chapitres :

Dans le premier chapitre, on va étudier les réseaux sociaux d'où on va présenter l'efficacité et la puissance et les relations humaines de ces plateformes de communication.

Dans le second chapitre, on va présenter les raisons d'utilisations des réseaux sociaux décentralisés, comme on va étudier ces composants puis on va terminer le chapitre par quelques exemples sur des réseaux sociaux décentralisés.

Dans le troisième chapitre, on va présenter le fonctionnement de la technologie Blockchain, après on va indiquer ces avantages et inconvénients, puis on va terminer le chapitre par quelques applications de cette technologie.

Dans le quatrième chapitre, on va proposer les techniques d'authentification dans un réseau social décentralisé à l'aide de Blockchain.

Dans le cinquième chapitre, on va essayer d'implémenter les techniques proposées.

Chapitre 1

1. Généralité sur les réseaux sociaux

1.1. Introduction

Les sites des réseaux sociaux sont des plateformes de communication mais leur efficacité due à la puissance de relations humaine transitives à leur affecter d'autre fonction : marketing, recherche d'information, collaboration en ligne, recrutement et affaire, jeux… . On va présenter dans ce chapitre une vue général sur ces systèmes.

1.2. Historique

Le phénomène des sites web de réseautage social est très récent et il date au début du troisième millénaire mais la notion du réseau social est plus ancienne. Il faut donc, faire la différence entre « réseau social » dans le domaine de la sociologie et les sites web qui offrent le service de réseautage social qui sont connus sous le nom de « réseaux sociaux numériques » ou « médias sociaux ».

La notion du « réseau social » (social network) a été inventé par John A. Barnes pour décrire des ensembles d'individus et les relations qu'ils entretiennent les uns avec les autres, ce qui était jusque-là connu sous divers noms : structures, systèmes, cercles, groupes [2]. Le travail de Barnes a étudié la relation entre chaque individu et la société dans une petite île Norvégienne et il a montré que tous les individus étaient indirectement liés entre eux par une chaîne de relations de quatre maillons au maximum. Il a proposé que ce principe relie chaque individu avec le reste du pays et du monde entier grâces aux liens de parenté ou d'amitié.

Milgram, en 1967 qui a testé cette théorie dans le cadre de l'expérience dite « le phénomène du petit monde », a cherché à évaluer le nombre moyen d'intermédiaire entre un individu et un autre au sein de la société américaine ; aboutissant au chiffre de 5,2 voire 6 degrés de séparation.

Cette théorie a inspiré l'acteur américain Kevin Bacon pour concevoir un jeu qui se base sur la relation entre lui et les différents acteurs de Hollywood. Le principe de ce jeux et que Bacon est relié avec un degré de 1 avec tous les acteurs qui ont joué avec lui ; les acteurs avec un degré 2 n'ont jamais travaillé avec lui mais ils ont joué avec un acteur d'ordre 1. Le défi du jeu est de trouver un chemin inferieur a 6 entre Kevin Bacon est n'importe quel autre acteur de cinéma. Le succès de ce jeu a conduit à la création d'une organisation de charité nommée **SixDegrees.org**.

Cette théorie a ouvert la voie d'une longue série de travaux empiriques cherchant à valider ou invalider les hypothèses de Barnes et Milgram, travaux qui, dans les années suivantes, ont fait d'Internet leurs terrains d'expériences [1].

L'implémentation de ce concept était difficile avec les anciennes technologies web qui comportent des pages statiques rarement modifiées. Dans ce contexte (web 0.1), l'utilisateur est plus consommateur que producteur d'information avec la difficulté de gestion qui demandait l'intervention des experts (programmeurs ou administrateurs). Le web ensuite a évolué en introduisant la notion des sites dynamiques dont les pages sont chargées à la demande à partir des bases de données.

Arrivant au web 2.0 qui a permet de transformer les utilisateurs a des acteurs actifs .Philippe Torloting résume ainsi : « dans le web1.0 l'internaute était seulement passif ; à partir du web2.0 l'internaute c'est-à-dire l'utilisateur devient actif : il crée son propre contenu, partage des informations, se crée un réseau, etc. ; en particulier via les médias sociaux dont les réseaux sociaux » [3].

Dans le web 2.0, les applications sont plus accessibles et disposent des interfaces interactives permettant aux utilisateurs de produire, modifier et partager des informations qui sont par la suite enrichies par d'autres utilisateurs [4]. Dans ce contexte d'interaction et collaboration, les réseaux sociaux numériques sont nés. On peut dire que les forums de discussion, les plateformes de blogs et les sites collaboratifs tel que Wikipédia constituent un premier pas dans cette tendance.

On peut considérer « **friendster** » lancé en 2002 comme le premier réseau social aux sens actuel du mot. C'était un site destiné aux jeux qui utilisait pour la première fois la notion de cercles et réseaux d'amis. Ensuite, d'autres plateformes ont été mises en service. On peut citer **« MySpace »** lancé en 2003 qui dépassa **« friendster »** en avril 2004 en termes de nombre de pages affichées. Les réseaux sociaux professionnels tels que « **LinkedIn »** et « **XING »** ont vu le jour en 2003. En 2004, **« facebook »** a été lancé pour servir à la communication entres les étudiants de l'université de Harvard mais son succès fait de lui le réseau social le plus populaire jusqu'à nos jours. Plusieurs réseaux de partage de contenu sont ensuite apparus : « **Flickr »** en 2003, « **Youtube »** en 2005 et « **Slide Share** »en 2006. Google a essayé de joindre ce monde en offrant 30 millions dollars pour acheter **« friendster »** et on achetant **« youtube »** en 2006 et en lançant son propre réseaux « **Google** + » en juin 2011.

L'invention des smartphones et le développement des applications mobile a permet aussi de créer des réseaux sociaux pour cette environnement. On peut citer : **« WhatsApp »** en 2009, « **Instagram** » en 2010.

1.3.Définition

Un réseau social est un ensemble d'entités (individus ou organisations) connectés via plusieurs types de relations (familiale, amitié ou professionnelles...). Les définitions proposées aux réseaux sociaux d'une manière générale sont concentrés sur ces deux caractéristiques : les entités et les liens qui leur connectent.

Les relations sont de plusieurs types (collaboration, soutien, amitié, contrôle, conseil, échange d'informations) et les acteurs peuvent être des individus, des groupes ou des organisations [5] [6].

Lemieux Vincent précise que le réseau social est un ensemble qui peut être organisé (une entreprise par exemple) ou non (comme un réseau d'amis) et ces relations peuvent être de nature fort diverse (pouvoir, échanges de cadeaux, etc.), spécialisées ou non, symétriques ou non [7].

Une autre définition s'intéresse à l'utilité de ces structures : « C'est un moyen efficace pour les individus de bénéficier d'avantages et d'opportunités au travers des liens établis au sein du réseau social » [8].

Même si Les définitions citées ci-dessus parlent du concept sociologique, elles sont cohérentes dans le contexte des réseaux sociaux numériques qui peuvent être définies comme une implémentation de la théorie des réseaux sociaux.
Boyd et Ellison décrit les sites des réseaux sociaux : On définit les sites des réseaux sociaux comme des services web qui permettent aux individus de :

1. construire un profile publique ou semi-publique au sein d'un système délimité.
2. articule ce profil avec une liste des autres utilisateurs avec qui ils partagent une connexion.
3. afficher et naviguer leur liste de connexions et ceux des autres au sein du système » [9]

La définition suivante éclaire aussi bien le fonctionnement des relations dans les médiassociaux : « Un réseau social représente des entités et des connexions entre eux. Les entités sont généralement des individus connectés par des relations personnelles, des interactions et le suivi des activités de leurs contacts sur le réseau » [10].

D'autres essayent d'aller plus loin pour mettre en évidence la différence entre les réseaux sociaux avant et après internet. Ils essayent de définir les médias sociaux non seulement comme un ensemble d'entités reliées par des relations sociales mais en mettant la lumière sur les services échangées et les centres d'intérêts qui regroupent les utilisateurs.
On peut donner par exemple la définition de Yahoo qui appartient aux propriétaires des réseaux sociaux grâce à son service Yahoo !360. Selon Yahoo, un réseau social est « un terme assez large qui désigne des sites Internet qui aident leurs utilisateurs à créer leur propre profil Internet et à partager une partie de leurs contenus préférés, y compris des photos et de la musique » [11].
Dupin [12] différencie les réseaux et medias sociaux de la façon suivante :

- Les réseaux sociaux reposent sur un lien social,
- Les medias sociaux reposent sur l'ensemble des sites proposant une interaction sociale.

« Dans le premier cas, c'est donc l'individu qui est au centre des échange alors que pour le second, c'est l'ensemble des objets présents qui favorise l'interaction. Dans cette logique, les réseaux sociaux sont une partie des medias sociaux. Ils sont la plus pure représentation du terme « social », qui connote la relation entre différents individus et dont l'expression se centralise par un profil utilisateur ».

On peut dire que les médias sociaux on permet de construire des réseaux sociaux plus larges, plus diversifiés et souvent plus concentré autour des thèmes ou des centres d'intérêts bien définis. En plus, ces technologie ont permet aux utilisateurs de mieux bénéficier de la puissance des relations.

1.4.Fonctionnalités

Les réseaux sociaux se partagent les fonctionnalités de base mais chaque réseau développe une ou plusieurs services comme il peut bloquer définitivement une fonctionnalité donnée. On résume dans ce paragraphe les différentes fonctionnalités des réseaux sociaux.

Création de profil

C'est une étape indispensable que chaque utilisateur doit faire pour pouvoir participer dans les réseaux. Il s'agit de remplir une fiche d'identité contenant essentiellement :

- Un identifiant qui est en général une adresse mail ou un numéro téléphone.
- Le mot de passe qui sécurise l'accès au compte.
- Un pseudo nom qui représente l'utilisateur dans le réseau et qui peut être changé par la suite.
- Les informations personnelles tel que le nom, le prénom, la date de naissance. La vérification de la fiabilité n'est pas exigée dans la plupart des médias sociaux.

On peut ajouter d'autres informations telles que la photo d'identité du profil, une citation introductive.

Publication

Une fois le profil créé, l'utilisateur peut contribuer dans les réseaux en publiant différent types d'information. Certain réseaux limitent la taille de la publication comme Twitter qui limite la publication a 140 caractères. D'autre n'acceptent qu'un seul type de données, c'est le cas des plateformes de partages : YouTube pour les vidéos, SlideShare pour les présentations… . Les réseaux généralistes tel que Facebook et google + ne mettent aucune restriction sur le contenu publié. Les publications peuvent être organisées sous différente formes (album de photo, playlist de vidéos, collection…).

Navigation

L'utilisateur peut consulter le contenu présent dans le réseau suivant différente manière :

-il peut visualiser sa page personnelle qui ne contient que l'information qu'il a publié auparavant.

-il peut visualiser les pages des autres utilisateurs.

-Souvent les réseaux proposent ce qu'on appelle un fil d'actualité qui contient un contenu varié extrait des pages des différents utilisateurs. Le choix de cet extrait est en général basé sur des algorithmes intelligents dont la notion d'apprentissage est nettement présente. Le système repose sur le comportement de l'utilisateur pour lui propose un contenu approprié.

Interactions avec les autres utilisateurs

L'interactivité est une propriété de base dans les médias sociaux et dans les applications du web 2.0. L'utilisateur peut réagir aux publications des utilisateurs par :

L'appréciation : il s'agit de donner un avis positive ou négative sur un contenu. Ceci est réalisé par les boutons de type « like /dislike »(le cas de YouTube ou Yahoo question/réponse) ou pour une vote (+1) comme le cas de Google+. Ces mentions d'appréciation ont un effet important sur la propagation du contenu dans le réseau.

Commentaire : L'avis sur un contenu peut être exprimé par un commentaire textuel ou image (fonctionnalité ajouté par Facebook en juin 2013).

Partage : Le partage signifie que l'utilisateur souhaite de sa part publier le contenu provenant d'un autre membre. La publication partagée aura la même propriété d'une nouvelle publication : elle apparait dans la page personnelle de l'utilisateur et elle peut être appréciée, commentée ou même partagée une nouvelle fois.

Connexion aux autres utilisateurs

Les liaisons entre les membres d'un réseau social peuvent prendre plusieurs formes

Liens symétrique (amitié) [21] : Dans ce type de liens les deux parts ont le même rôle. C'est le membre ALI en voie une demande au membre Mohamed et que Mohamed accepte cette invitation, Ali est l'ami de Mohamed et de même Mohamed et l'ami de Ali.

Lien asymétrique (abonnement) [21] : Cette liaison a un seul sens. Il s'agit de la fonctionnalité d' « abonner » ou « suivre » qui représente la relation éditeur/lecteur. Si par exemple Ali s'abonne pour suivre les publications de Mohamed, Mohamed n'est pas forcement abonné au compte d'Ali.

Groupes d'utilisateurs : Plusieurs utilisateurs regroupés autour d'une thématique ou d'un centre d'intérêt bien définit. Les membres ne sont pas forcément des amis mais ils peuvent publier librement dans l'espace réservé au groupe. En peut différentier une sous-catégorie de membres dans le groupe : les administrateurs ou les modérateurs, ils disposent de quelques privilèges par rapport aux autres membres. Il intervient pour modifier le contenu et le paramètre du groupe comme ils peuvent décider l'ajout ou la suppression des membres.

Administration

L'utilisateur est le maitre de son espace personnelle. Il dispose de quelque autorisation pour la gestion de son contenu. En plus de la publication, l'utilisateur peut :

-Supprimer une publication ou un commentaire.

-Définir le public qui peut visualiser une publication donnée.

-Autoriser ou interdire un autre membre à interagir avec lui.

-Autoriser ou interdire les invitations d'amitié

Discussion

La position de cette fonctionnalité diffère d'un réseau social à un autre. Il existe des réseaux qui ignorent ce service. D'autres mettent en place un service de messagerie entre les membres. La messagerie peut être « statique » ou instantané, elle supporte ou non la communication audiovisuelle. Il est a noté aussi qu'il existe des médias sociaux dont la messagerie constitue la fonctionnalité de base.

Jeux

Les jeux en ligne est l'un des fonctionnalités les plus anciennes dans les réseaux sociaux avec « **Friendster** ». Aujourd'hui, il existe des réseaux dédiés uniquement aux jeux. Certain réseaux généralistes -tel que Facebook-intègrent des applications de jeux en ligne.

Diffusion en direct du contenu multimédia

En plus du partage des vidéos, Il existe des réseaux sociaux qui offrent une fonctionnalité plus avancé. Il s'agit de la diffusion des vidéos en direct. On cite par exemple : **Meerkat, Periscope, Blab.** « **Facebook** » a intégré ce service an mars 2016.

1.5.Application des réseaux sociaux

Diffusion d'information

Les réseaux sociaux offrent au grand public un outil facile et puissant de diffusion d'information. Sont avoir besoin d'un grands budget ou un contact avec les medias classiques (journaux, chaines télévisés, sites web informatif), les internautes peuvent publier leur avis ou leur talents en toute liberté et leurs publications se propagent ensuite dans les pages des amis et ceux des amis des amis. Cette efficacité à créer un nouveau type de presse électronique. Ce sont les pages et les comptes des réseaux sociaux qui sont devenu un concurrent important aux anciens médias. Ces derniers n'ont pas tardé de constaté la puissance des médias sociaux et il est devenu indispensable pour les institutions des médias d'avoir des comptes dans les réseaux sociaux populaires.

Communication

Les réseaux sociaux ont permet aux utilisateurs de rester en contact avec leurs proches ou amis éloignés. En plus, ils ont permet de communiquer avec des personnes célèbres qui sont difficile à contacter a la vie réelle.

Réseautage d'affaires

Grâce aux liaisons qui existent entre les utilisateurs et la propagation rapide des informations. Les réseaux sociaux permettent de conduire des affaires avec succès, que ça soit la promotion d'un produit ou d'un service ou même la recherche d'un emploi.

Recherche d'information

En plus des moteurs de recherche, l'utilisateur repose sur les médias sociaux pour rechercher un contenu ou une personne. Cette tendance a conduit vers l'apparition d'une nouvelle classe de systèmes de recherche d'information : Les systèmes de recherche d'information sociale (SIR social information retrieval) [21]. Ces systèmes se basent sur la fonctionnalité d'indexation personnelle (dit **folksonomie**). Les utilisateurs jointent à leurs publications des marques « Tag ». Ces marques proposées par les utilisateurs constituent un index collaboratif qui peut servir aux outils de recherche de relier une requête avec un contenu adéquat. Cette technique a rendu la recherche plus efficace par rapport aux différents algorithmes d'indexation utilisés dans les systèmes de recherche d'information classiques. Les résultats de la recherche d'information sociale sont basés sur des propositions des utilisateurs. Cette collaboration des utilisateurs pour répondre une requête d'un autre utilisateur peut être observée dans les réseaux sociaux basés sur les questions et les réponses. Les utilisateurs proposent des réponses et votes les réponses des autres qui permettent au chercheur de l'information d'avoir les réponses les plus pertinentes.

Marketing

Pour promouvoir leurs produits et services, les entreprises donnent plus d'importance à la publicité dans les réseaux sociaux. Selon une étude emarketer, marketingland et recode, « 70% des annonceurs ont augmenté leur budget publicitaire sur les médias sociaux en 2015 » [20].

1.6.Types de réseaux sociaux

Même si chaque réseau social possède ces propres caractéristiques, il existe une intersection entre plusieurs réseaux ce qui a poussé les chercheurs à définir des classes des réseaux sociaux. Ces travaux ont résulté plusieurs approches basées sur différents critères (usage, objectifs,…). On résume ci- dessous les classifications les plus rencontrés dans la littérature.

1.6.1. Réseaux généraliste/ Réseaux spécialisé

La classification la plus présente dans la littérature considère deux grandes catégories des réseaux sociaux. Les réseaux généralistes et les réseaux spécialisés.

Les réseaux généralistes

Ils sont les réseaux populaires dont on peut trouver la plupart à savoir toutes les fonctionnalités des réseaux sociaux. On peut citer par exemple : Facebook et MySpace qui sont basés sur plusieurs utilisateurs connectés par des liaisons d'amitié et échangeant plusieurs types de données.

Les réseaux spécialisés

Ils sont des réseaux concentrés sur une thématique bien définie. D'où on trouve plusieurs sous-catégories :

-Les réseaux communautaires : Ils regroupent des utilisateurs partageant un même centre d'intérêt autour d'une thématique bien définie comme c'est le cas des ventes aux enchères sur eBay ou encore la mise à disposition des internautes de différents et divers registres musicaux sur Boompa

-Les réseaux professionnels : Ce sont des réseaux permettant à leurs membres de se valoriser sur le marché de l'emploi en créant leurs curriculum vitae en ligne, de chercher des opportunités d'emploi ou des opportunités de partenariat comme c'est le cas par exemple de Viadeo, Linkedin ou 6nergies.

-Les réseaux de partage de contenus : des réseaux sociaux tournés vers le partage d'un certain type de contenu multimédia (vidéos, son…) tels que YouTube, Dailymotion ou Sound Cloud. Ces réseaux permettent la publication et le partage des contenus, l'échange autour de ces contenus sous forme de commentaires mais ne proposent pas une fonctionnalité de mise en relation.

1.6.2. Réseaux de relations /réseaux de contenu

Dans cette classification ([13], [14]), les réseaux sociaux sont observés selon la fonctionnalité la plus importante : Les relations entre individu ou le partage de contenu.
Les réseaux structurés autour des individus et les relations qui les connectent. Ces relations peuvent êtres de plusieurs type mais l'essentiel est que le plus important dans ces réseaux est les liens d'amitié ou d'abonnement. On peut citer par exemple : **Facebook** ou **Linkedin**.
L'autre classe contient des réseaux centrés autour des contenus partagés. La navigation des profils est réalisée beaucoup plus suivant les données qu'il partage même s'ils permettent de visualiser une page ou une chaine d'un utilisateur bien déterminé.
Ziryeb Marouf [16] opte pour cette classification (ils nomment les deux classes : « profil centric » et « content centric ») en ajoutant une troisième catégorie : « Collaborative Centric » qui regroupe les plateformes collaboratives qui proposent les mêmes fonctionnalités qu'un groupware d'entreprise tel que le partage des documents, les agendas partagés, les forums de discussions. Il s'agit ici d'un groupware grand public accessible par un grand nombre d'internautes tel que Google Agenda.

1.6.3. Classiffication a base des objectifs

Thelwall [15] catégorise les réseaux sociaux selon leurs trois objectifs : socialisation, réseautage et navigation (sociale) :

-Les réseaux sociaux de socialisation : L'objectif de ces réseaux est la communication sociale entre les utilisateurs. Il permet de rechercher et afficher des amis et de se connecter a des nouveaux amis. MySpace et Facebook sont à la tête de cette catégorie.

-Les réseaux sociaux de réseautage : il permet de naviguer pour trouver de nouveaux contacts et entrer en connexions avec des personnes inconnues auparavant comme c'est le cas de LinkedIn ou Viadeo.

-Les réseaux sociaux de navigation : ce sont des sites de partage de liens Internet (connu sous le social bookmarking). Leur objectif est de faciliter la recherche et l'accès à l'information. Les membres partagent des liens ou des informations. Chaque utilisateur reçoit une page principale contenant un extrait des partages des membres avec les mentions d'appréciations des utilisateurs qui peuevent service comme indice d'aimportance. L'utilisateur peut également consulter les contributions d'un membre données. C'est le cas de Digg ou Del.icio.us.

Thelwall différencie également les sites pour lesquels les fonctionnalités de réseaux sociaux sont principales (de type Facebook et LinkedIn) ou secondaires (Youtube, FlickR, Deezer).

1.6.4. Classiffication basée sur l'usage

En février 2018, Frédéric Cavazza propose le graphique suivant qui résume ça vision à la typologie des médias sociaux basée sur l'usage :

Figure 1 : Panorama des médias sociaux [17]

D'après Cavazza [16], les médias sociaux peuvent être répartis en dix catégories :

-Forum : Un espace de discussion public où les messages sont affichés par ordre chronologique. La consultation est libre, mais l'inscription est obligatoire pour pouvoir répondre. La modération des discussions se fait à priori ou a posteriori. Exemples de gros forums français : Doctissimo, Forum-auto, Cyberbricoleur, MagicMaman, Comment ça marche, etc. Exemples de plateformes de forum : PHPbb, Phorum, bbPress, etc.

-Blogue : Un outil de publication simplifié où les articles sont affichés par ordre chronologique et triés dans des catégories. Les lecteurs peuvent déposer des commentaires qui sont modérés à postériori. Le flux RSS permet de facilement exporter le contenu vers des agrégateurs et lecteurs. Exemples de plateformes de blogues : Blogger, WordPress, Typepad, etc.

-Wiki : Une base de connaissance en ligne où les internautes rédigent et corrigent eux-mêmes le contenu. Les wikis sont constitués d'un ensemble de pages sans système de navigation cohérent. Chaque page dispose d'un historique des modifications et peut être commentée. La modération est assurée par des équipes organisées de façon pyramidale. Exemple de wikis célèbres : Wikipedia, Wookipedia, Brickipedia, etc. Exemples de plateformes de wiki : MediaWiki, Wikia, Wetpaint, etc.

-Service de partage : Service en ligne où les internautes peuvent publier des photos, vidéos, liens… Chaque élément publié est rattaché à un membre et peut être commenté et noté. La communauté ou les annonceurs peuvent créer des chaines et des groupes pour fédérer des micro-communautés. Exemples : YouTube, FlickR, Delicious, Deezer, Slideshare, etc.

-Réseau social : Site à l'accès restreint où chaque utilisateur possède un profil. Les membres sont liés de façon bilatérale ou au travers de groupes. Certains réseaux proposent également des fonctionnalités plus sophistiquées (messagerie, publication et partage de contenus, etc.) ainsi que la possibilité d'héberger des applications tierces (plateforme). Exemples : Facebook, Orkut, Friendster, Tagged, etc.

-Microblogue : Service de publication, de partage et de discussion reposant sur des messages très courts. La consultation des messages et profils ne requiert pas d'inscription et peut se faire sur le web, les terminaux mobiles ou au travers d'applications. Chaque membre possède un profil public où sont listés les derniers messages. Les membres peuvent s'abonner aux profils des autres pour recevoir leurs messages dans un flux unique. Exemples : Twitter, Google Buzz, etc.

-Agrégateur : Service en ligne permettant de regrouper l'ensemble des publications d'un utilisateur des médias sociaux (social stream). De très nombreuses formes de contributions sont acceptées (RSS, photos, vidéos, liens, email, etc.). Les utilisateurs peuvent s'abonner aux flux des autres membres. Exemples : Posterous, FriendFeed, etc.

-FAQ collaborative : Service en ligne d'entraide où les questions et les réponses sont publiées par les utilisateurs. Les réponses sont commentées et notées, le membre qui a publié la question sélectionne la réponse la plus satisfaisante afin de clôturer les échanges et récompenser l'auteur avec un système de points. Exemples : Quora, StackOverflow, etc.

-Jeux sociaux : Jeux en ligne reposant sur une plateforme sociale exploitant les profils des membres pour proposer différentes interactions sociales entre les joueurs (tableau publics des meilleurs scores, système d'invitation et de défis, objectifs ne pouvant être réalisés en solo, etc.). Exemples : Farmville, Mafia Wars, Texas HoldEm Poker…

-Service de géolocalisation : Applications permettant de publier, partager et discuter sur des terminaux mobiles. Les articles ou photos publiés sont rattachés à un lieu afin de leur donner un contexte géographique. Chaque membre dispose d'un profil où sont listées ses dernières publications ainsi que les lieux qu'il a visités. Chaque lieu dispose également d'une page où sont listés les membres qui s'y sont signalés (check-in). Exemples : Foursquare, Facebook Places, Gowalla, etc.

1.6.5. Classification de Delcroix

Une autre classification proposée par Eric Delcroix [19], consultant, spécialiste et expert en communication web, web2.0, réseaux sociaux. Il détermine 07 catégories.

-Réseau d'Affaires et d'Emplois : Viadeo, Linkedin.

-Réseau Communautaire et Thématique : Wikkio, Scoopeo.

-Réseau de Jeunes, « bloglike » : MySpace, Skyrock.

-Réseau « Identité Numérique » : Ziki, MyBlogLog.

-Réseau « Micro » (micro-blogging, micro-vidéo, etc.) : Twitter, Tumblr.

-Réseau « Privé » : sur invitation.

-Réseau Spécialisé (vidéo, images…) : Dailymotion, YouTube, Flickr.

1.7.Avantages et Inconvénients

On peut résumer les aspects qui font que les réseaux sociaux numériques sont plus performent que les sites web classiques dans les points suivant :

-Omniprésence : grâce à la notion des notifications l'utilisateur est informé en temps réel de ce qui se passe dans son réseau.

-accès l'information : grâce aux réseaux sociaux, l'information circule d'une manière très rapide et très souple. Il suffit d'être abonné a une page ou dans un groupe de discussion ou tout simplement suivre un amis pour recevoir les informations qui vous intéressent dans un temps très réduit.

-facilité d'administration : les réseaux sociaux ont permet aux grands publiques de publier différents format d'information sans avoir besoin de payer un hébergeur ou faire appel à un spécialiste en informatique.

-liberté d'expression : Les réseaux sociaux présentent un milieu idéal des échanges de pensées loin de tout type de contrôle ou de censure. Ils ont permet aux internautes de s'exprimer et de discuter leurs problèmes et proposant des solutions qui ont été souvent mise en action. A titre d'illustration les révolutions arabes connus sous le nom de « printemps arabe » est un résultat de plusieurs débats et compagnes dans les réseaux sociaux notamment Facebook et Twiter.

Par contre, l'expansion des médis sociaux a déclenché plusieurs études socioéconomique ou même psychologiques pour mettre le point sur les effets de l'utilisation des médias sociaux. On cite quelques inconvénients dus à la mauvaise utilisation des médias sociaux :

-Une vie virtuelle : Les soupers entre amis ou les rencontres familiales sont souvent altérés par les gens qui sont connectés à leurs comptes des médias sociaux. Il est donc très facile de vivre dans le virtuel et de ne pas vivre tout à fait le moment présent.

-Crédibilité des informations : il est facile de publier et l'information se propage rapidement mais rien n'empêche de publier des informations erronées ou des avis dans des domaines dont le rédacteur n'est plus expert. Il se peut alors que l'information que nous trouvons sur les réseaux sociaux ne soit pas exacte.

- Diminution de productivité : Les médias sociaux nous incitent à être de plus en plus multitâches. Nous regardons souvent notre compte Facebook alors que nous sommes en train de travailler sur autre chose. On pourrait croire que cela nous permettrait d'accomplir deux choses en même temps, mais au contraire, notre concentration diminue et notre rythme de productivité baisse.

-Réputation professionnelle : Employeurs et chasseurs de têtes utilisent de plus en plus les réseaux sociaux pour dénicher des candidats. Mais aussi pour vérifier leur profil avant un entretien. Un sondage publié sur le site de recrutement en ligne CareerBuilder révélait que des employeurs qui consultent Facebook et compagnie ont déjà écarté des candidats à cause du contenu de leurs pages personnelles [22].

-Sécurité et protection de la vie privée : Nos contributions et comportements dans les réseaux sociaux appartient totalement aux propriétaires de ces sites. Il est clair que ces informations sont analysées pour nous proposer des services des amis ou des publicités mais rien n'assure que nous somme protégés contre une utilisation illégitime de ces données.

-Intimidation et harcèlement en ligne : Le cyber harcèlement sur les réseaux sociaux est un problème qu'il ne faut pas prendre à la légère, il peut avoir de graves conséquences.

En effet, le cyber harcèlement peut revêtir plusieurs formes comme : la création de faux profils, l'usurpation d'identité, la diffusion de rumeurs infondées ou encore l'envoi de messages d'insultes. Ces agressions répétées sur le long terme peuvent prendre des proportions importantes et impacter directement la vie des victimes. De plus, ces messages, photos et vidéos publiées et échangées via les canaux numériques à grande échelle, laissent des traces même après que le harcèlement cesse. Les adolescents sont tout particulièrement touchés par ce phénomène.

1.8.Exemples de réseaux sociaux

On expose dans ces paragraphes des réseaux sociaux très populaires de différentes catégories :

Facebook

Facebook est un réseau social généraliste. Ils supportent toutes les fonctionnalités citées ci-dessus. Facebook est né en 2004 à l'université Harvard ; d'abord réservé aux étudiants de cette université, il s'est ensuite ouvert à d'autres universités américaines avant de devenir accessible à tous en septembre 2006.

Facebook est le troisième site web le plus visité au monde après Google et YouTube selon Alexa, il compte, en décembre 2015, 1,04 milliard d'utilisateurs actifs quotidiens sur un total de 1,59 milliard d'utilisateurs actifs mensuels [24].

Linkedin

Un réseau social professionnel en ligne créé en 2003 à Mountain View (Californie). LinkedIn est principalement utilisé par ses membres pour trouver du travail, des clients, des fournisseurs et développer ses affaires.

Il fonctionne sur le principe de la connexion, ce qui signifie que pour entrer en contact avec un professionnel, vous ne pouvez le faire que par l'entremise de votre réseau. Si ce professionnel n'est connu par aucun membre de votre réseau, il vous sera impossible de le rejoindre, ou de lui envoyer un message. LinkedIn divise les connexions en trois niveaux distincts :

- Les contacts directs (le premier degré)
- Les contacts de notre réseau (le 2e degré)
- Les contacts de nos contacts de 2e degré (le 3e degré)

Twitter

Twitter est un outil de **micro-blogging** géré par l'entreprise Twitter Inc. Il permet à un utilisateur d'envoyer gratuitement de brefs messages, appelés tweets, sur internet, par messagerie instantanée ou par SMS. Ces messages sont limités à 140caractères. Les utilisateurs peuvent apprécie, commenter ou partager (retweet) les publications. Les liaisons entre les utilisateurs sont basé sur le principe d'abonnent.

Twitter a été créé le 21 mars 2006 par Jack Dorsey, Evan Williams, Biz Stone et Noah Glass[25], et lancé en juillet de la même année. Le service est rapidement devenu populaire, jusqu'à réunir plus de 500 millions d'utilisateurs dans le monde fin février 2012 [26]. Twitter compte 320 millions d'utilisateurs actifs par mois en avril 2016[27].

YouTube

YouTube est un site web d'hébergement de vidéos sur lequel les utilisateurs peuvent **envoyer**, é**valuer**, **regarder, commenter**et **partager** des vidéos. Il a été créé en février 2005 par Steve Chen, Chad Hurley et Jawed Karim, trois anciens employés de PayPal et racheté par Google en octobre 2006 pour la somme de 1,54 milliard de dollars. En Avril 2016, YouTube est classé en deuxième position dans la liste des sites les plus visité [23].

1.9.Les statistiques

Le nouveau rapport digital 2018 publié par We Are Social et Hootsuite révèle que désormais, ce sont plus de 4 milliards de personnes dans le monde qui utilisent internet.Plus de la moitié de la population mondiale est maintenant connectée à internet, avec plus d'un quart de milliard de nouveaux utilisateurs en 2017.L'Afrique est le continent qui a connu la croissance d'internautes la plus rapide : plus de 20 % en un an[28].

a. Internet et mobile :

Plus des deux tiers de la population mondiale possèdent aujourd'hui un téléphone portable, avec une majorité d'utilisateurs de smartphones.

Le nombre d'utilisateurs uniques de portables dans le monde a augmenté de 4% cette année, bien que le taux de pénétration dans la plupart des pays d'Afrique Centrale reste en dessous des 50%.

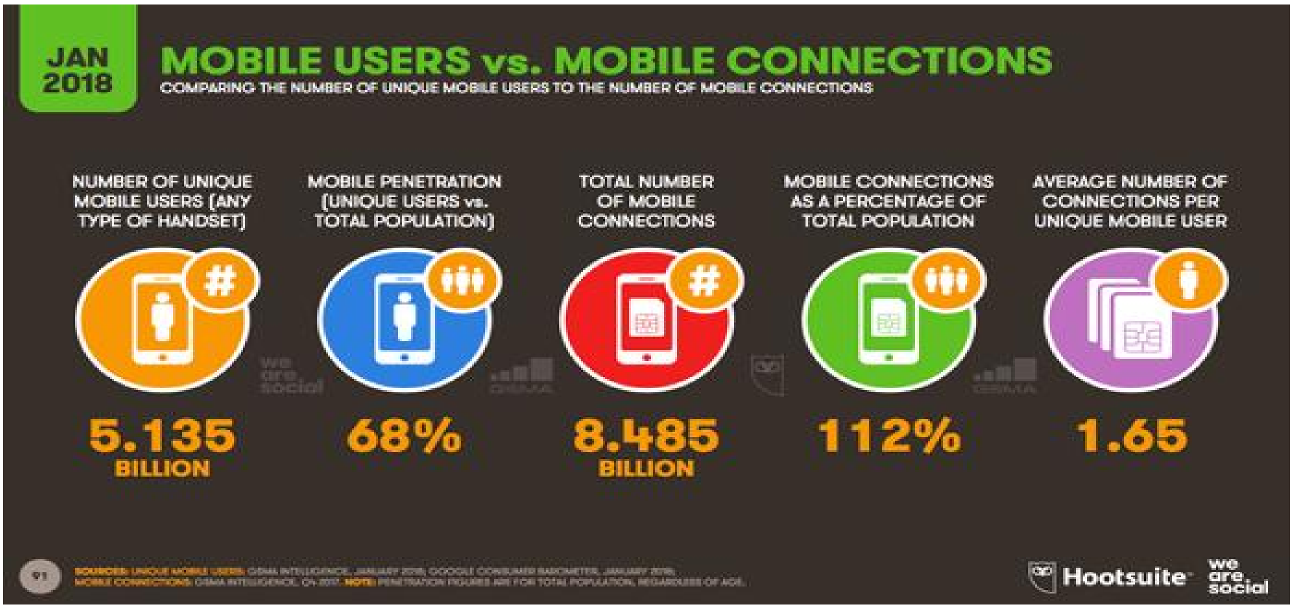


Figure 2 : Des statistiques sur l'utilisation de téléphone portable [28]

Le Smartphone est également le device préféré dans le monde pour se connecter à internet et représente une part de trafic web supérieure à celle de tous les autres devices réunis.

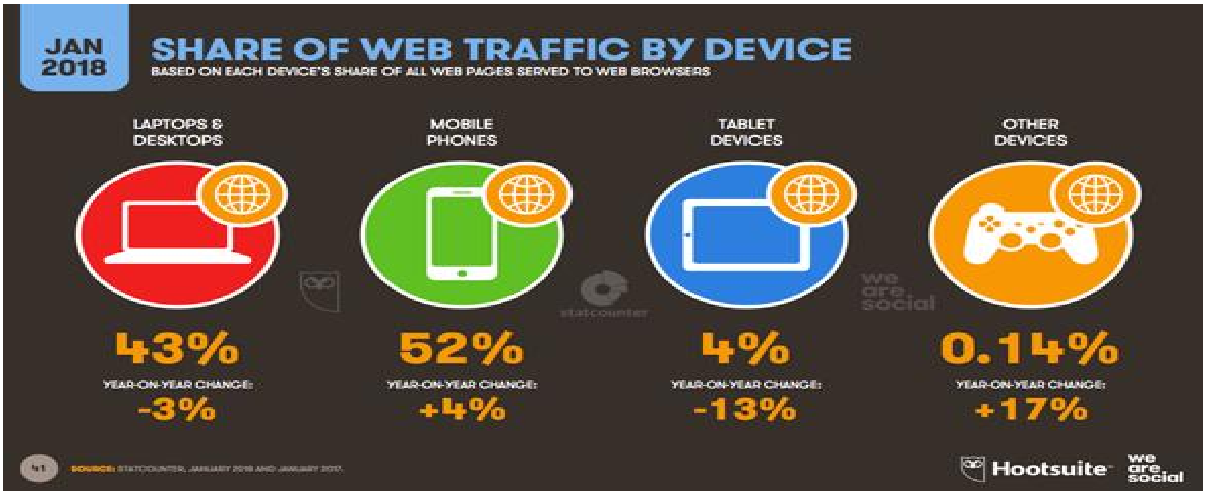


Figure 3 : Des statistiques sur les appareils les plus connecteé a l'internet [28]

Soulignons que cette donnée ne concerne que l'utilisation du web... La dernière étude d'App Annie montre qu'en outre, les utilisateurs passent aujourd'hui 7 fois plus de temps sur les applications mobiles que sur les navigateurs internet mobiles. Donc en fait, la part du mobile dans la consommation d'internet est encore plus importante que ce que les chiffres nous suggèrent ici.

Les dernières données de Facebook sont en ligne avec ce ce constat : aujourd'hui, seulement 5% de ses utilisateurs n'accèdent pas à la plateforme via le mobile.

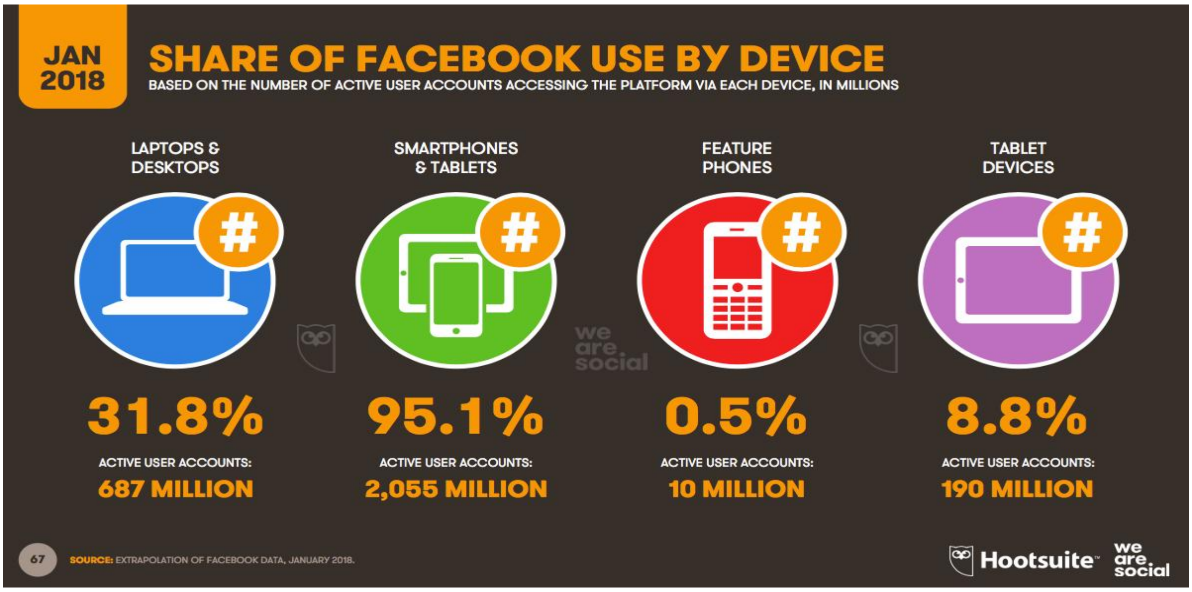


Figure 4: Des statistiques sur l'utilisation de facebook par différantes appareils [28]

b. nouveaux utilisateurs de réseaux sociaux chaque seconde :

Quasiment 1 million de personnes par jour a fait ses premiers pas sur les réseauxsociaux en 2017, ce qui équivaut à plus de 11 nouveaux utilisateurs chaque seconde.De plus, le nombre total d'utilisateurs des réseaux sociaux a augmenté de 13% ces12 dernier mois.

Et ce sont les régions d'Asie centrale et d'Asie du Sud qui enregistrent lesaugmentations les plus rapides, avec respectivement + 90% et + 33% de croissanceannuelle.

L'Arabie Saoudite est le pays qui connait la croissance la plus rapide parmi 40économies étudiées, avec 32% de nouveaux utilisateurs de réseaux sociaux en 2017et juste derrière se trouve l'Inde avec 31% de croissance.

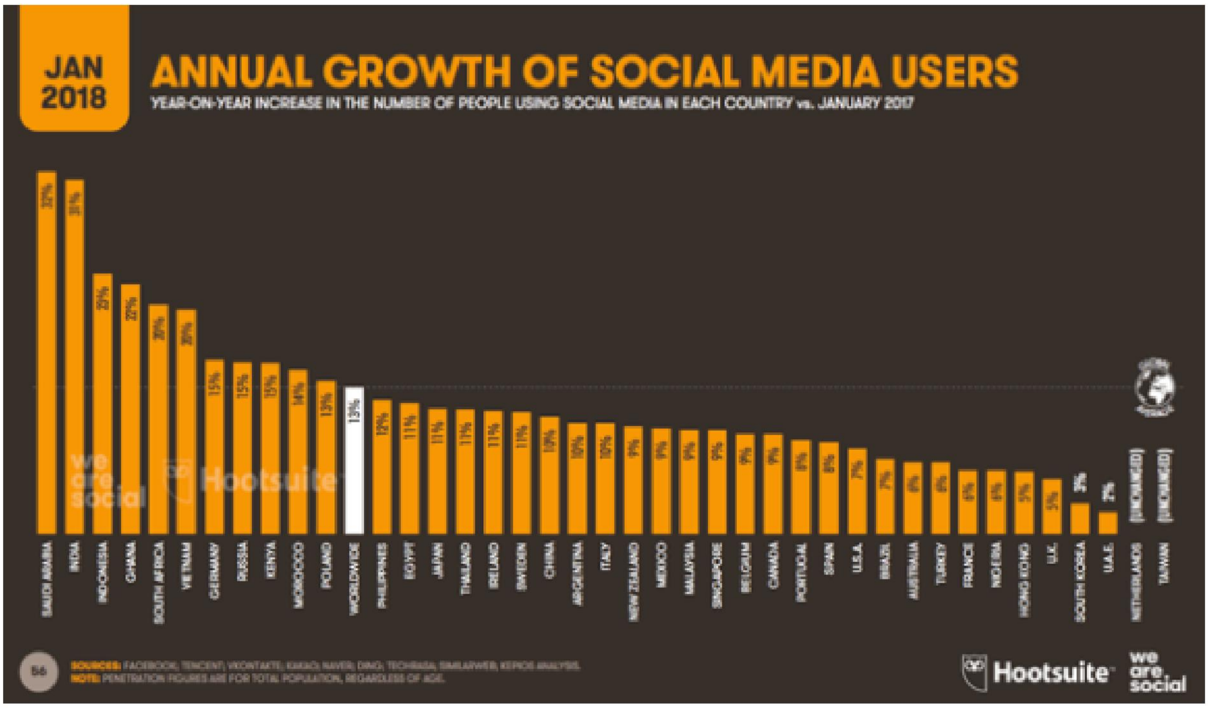


Figure 5 : Des statistiques sur la croissance annuelle des utilisateurs des réseaux sociaux dans les pays [28]

L'un des facteurs de cette croissance est l'augmentation des utilisateurs plus âgésqui ont rejoint les plateformes sociales. Ainsi, uniquement sur Facebook, le nombred'utilisateurs âgés de 65 ans et plus a augmenté de quasiment 20% sur les 12derniers mois.

Le nombre d'adolescents utilisant Facebook a également crû, mais dans uneproportion moindre, avec une croissance de 5% d'utilisateurs âgés de 13 à 17 ans.

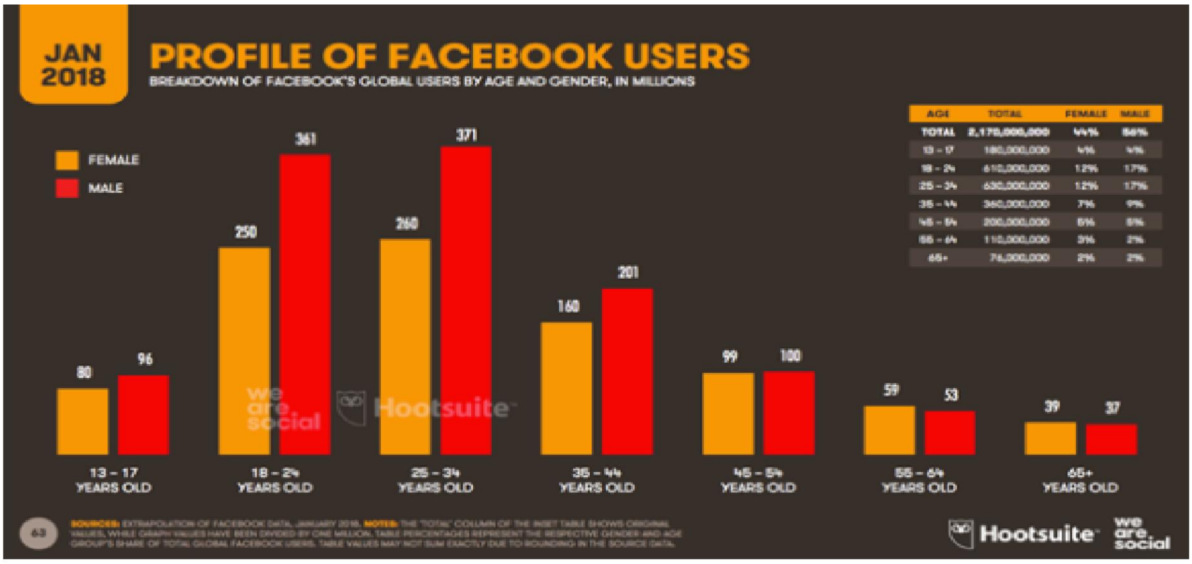
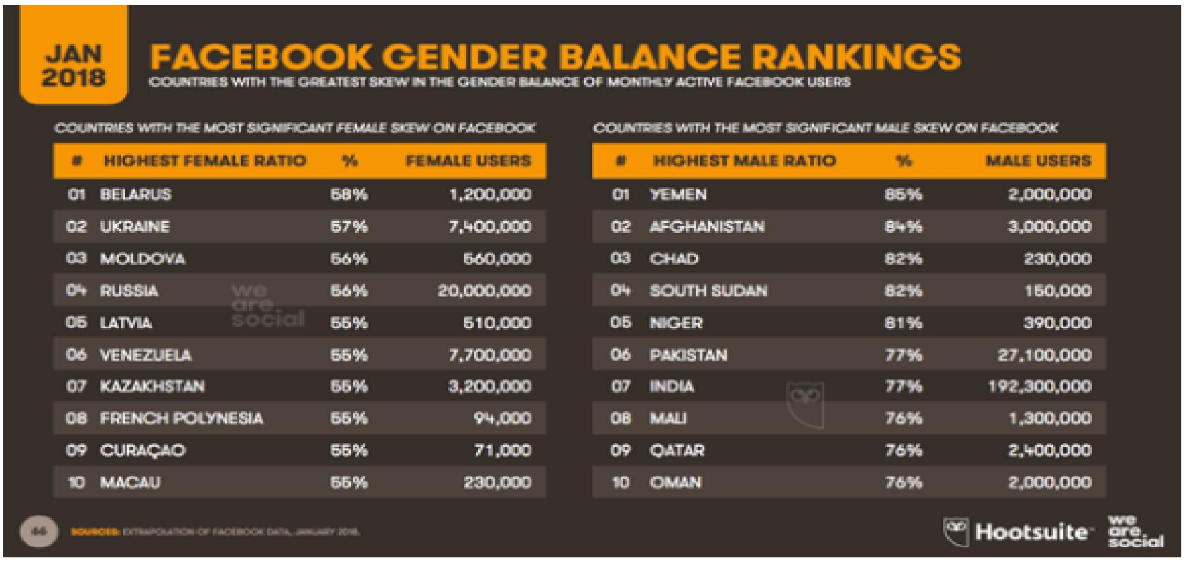


Figure 6 : Des statistiques sur l'age et sexe des utilisateurs de Facebook [28]

La répartition par sexe sur internet reste un sujet préoccupant. Les dernières données de Facebook montrent ainsi que les femmes sont encore significativementsous-représentées en Afrique Centrale, au Moyen-Orient et en Asie du Sud.



#	HIGHEST FEMALE RATIO	%	FEMALE USERS
01	BELARUS	58%	1,200,000
02	UKRAINE	57%	7,400,000
03	MOLDOVA	56%	560,000
04	RUSSIA	56%	20,000,000
05	LATVIA	55%	510,000
06	VENEZUELA	55%	7,700,000
07	KAZAKHSTAN	55%	3,200,000
08	FRENCH POLYNESIA	55%	94,000
09	CURAÇAO	55%	71,000
10	MACAU	55%	230,000

#	HIGHEST MALE RATIO	%	MALE USERS
01	YEMEN	85%	2,000,000
02	AFGHANISTAN	84%	3,000,000
03	CHAD	82%	230,000
04	SOUTH SUDAN	82%	150,000
05	NIGER	81%	390,000
06	PAKISTAN	77%	27,100,000
07	INDIA	77%	192,300,000
08	MALI	76%	1,300,000
09	QATAR	76%	2,400,000
10	OMAN	76%	2,000,000

Figure 7 : Classement de la parité hommes-femmes sur Facebook par pays [28]

c. Facebook poursuit sa domination :

Encore une belle année pour Mark Zuckerberg et ses équipes : l'ensemble des plateformes de Facebook Inc. enregistre une croissance impressionnante en 2017. La plateforme principale de Facebook domine toujours le paysage mondial du social media, avec une croissance de 15% en 1 an, pour atteindre un total de près de2,17 milliards d'utilisateurs début 2018.

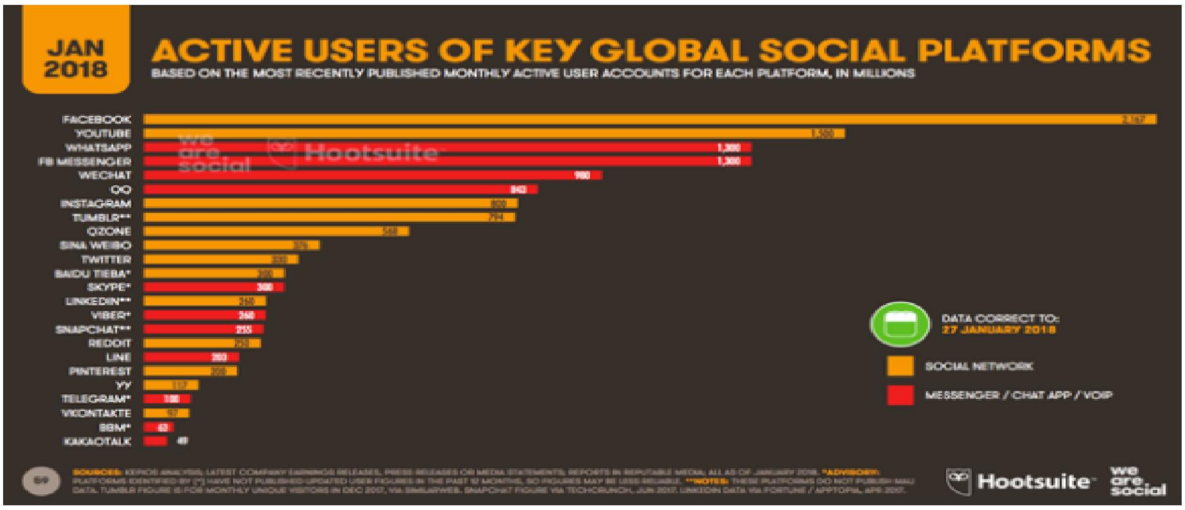


Figure 8 : Des statistiques sur les utilisateurs actifs dans les plateformes sociales mondiales [28]

WhatsApp et Facebook Messenger ont progressé deux fois plus vite que la plateforme principale de Facebook, avec une croissance de 30% sur un an. Les deux applications sont encore à égalité en termes de nombre d'utilisateurs,mais d'après la récente étude de SimilarWeb, WhatsApp est mieux implantégéographiquement : WhatsApp est désormais l'application de messagerie n°1 dans 128 pays à travers le monde, tandis que Facebook Messenger l'est dans 72 pays.Et il n'y a aujourd'hui que 25 pays dans le monde où une application de messagerie appartenant à Facebook n'est pas la plateforme de messagerie n°1.

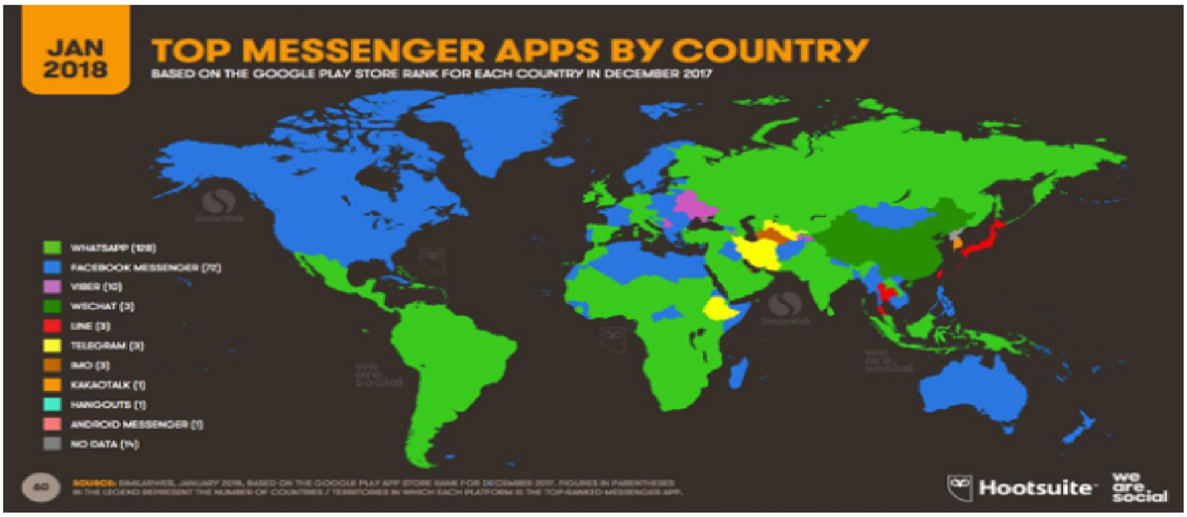


Figure 9 : Top applications de messagerie par pays [28]

Malgré ces chiffres impressionnants sur les messageries de Facebook, avec une hausse de près d'un tiers de son nombre d'utilisateurs en un an, Instagram est également parvenu à revendiquer une partie de la croissance remarquable de Facebook Inc.

Pour aider les entreprises à évaluer l'opportunité que représente Instagram dansleurs pays respectifs, nous avons inclus cette année les données locales sur sonutilisation dans plus de 230 pays dans les rapports régionaux.

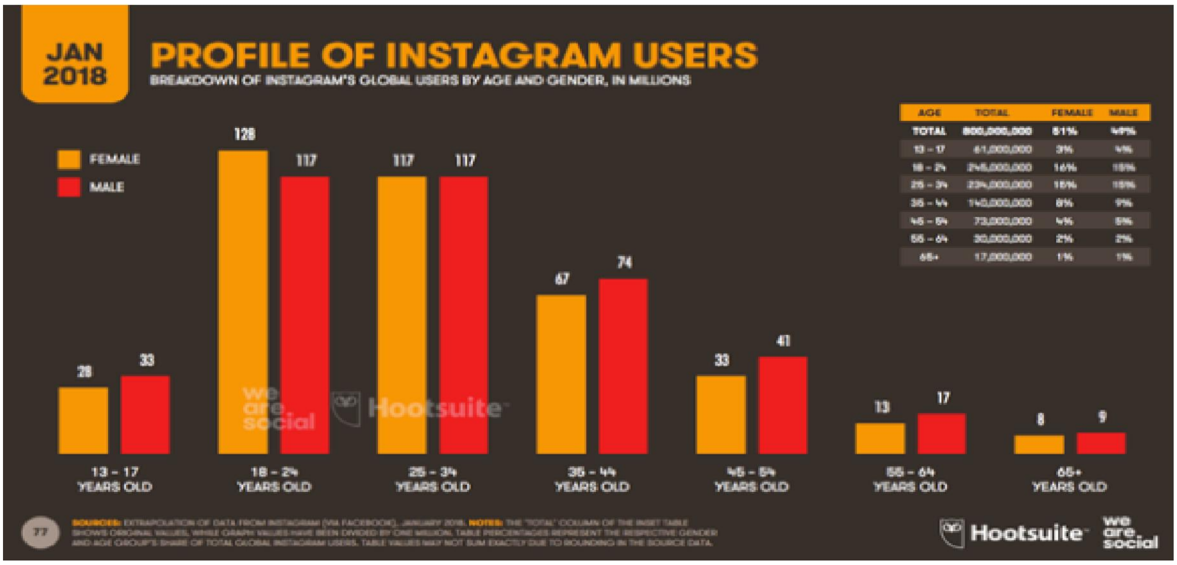


Figure 10 : Des statistiques sur l'age et sexe des utilisateurs d'Instagram [28]

1.10.Conclusion

Les médias sociaux sont de plus en plus présents dans notre quotidien. Leur efficacité a leur permet de remplacer les médias et les outils de communication classiques. Ils se basent sur une théorie sociologique intéressante et ils exploitent l'énorme développement des technologies web. On a présenté brièvement les notions de bases de ces plateformes. Le rapport suivant sera une recherche bibliographique sur les architectures des réseaux sociaux numériques.

Chapitre 2

2. Réseaux Sociaux Décentralisé

2.1. Introduction

En raison de la popularité croissante des réseaux sociaux en ligne (OSN) et de l'énorme quantité de données partagées sensibles, la préservation de la confidentialité devient un problème majeur pour les utilisateurs d'OSN.

Alors que la plupart Les OSN reposent sur une architecture centralisée, avec un fournisseur de service omnipotent, plusieurs Des architectures décentralisées ont récemment été proposées pour les OSN décentralisés (DOSN).

OSN évolué dans le temps, fournissant plusieurs communications et partage d'installations qui amènent les utilisateurs à partager d'énormes quantités de l'information personnelle [29] sur eux.

Maintenant ce que le réseau social décentralisé est pourquoi il est mieux que le réseau social centralisé ?

2.2.Définition

Depuis les débuts d'internet, le principe de décentralisation a été à la base de la circulation des transmissions et télécommunications sur les réseaux des réseaux.

La décentralisation [30] : Concevoir le réseau de manière à ce que les communications et les échanges aient lieu entre des nœuds jouant tous un rôle symétrique dans le système, éliminant ainsi la dualité le fournisseur de service et l'utilisateur, typique du modèle serveur/client, et la remplaçant par une situation ou chaque client devient serveur.

Les plus célèbres (ou les plus sulfureux, selon les points de vue) modèles de réseaux informatiques décentralisés sont ceux qui sont utilisés, depuis quinze ans, dans les systèmes de partage de fichiers basés sur le Peer-To-Peer (p2p).

L'architecture des systèmes p2p est aussi à même d'apporter davantage d'efficacité, de liberté et de stabilité à la distribution de contenu en ligne, grâce aux connections directes entre les utilisateurs devenus des nœuds de systèmes.

Lorsque chaque nœud du réseau décentralisé est autonome, on parle de réseau décentralisé : c'est le modèle de pair-à-pair (P2P) comme Bittorrent, GNUne Tor, I2P, cjdns ou Bitcoin. Ce modèle est le plus robuste face à l'agression d'un pouvoir centralisé (observation, censure, manipulation), car il n'offre pas de prise directe ni de cible particulière - il ne dispose pas de point unique de défaillance, contrairement aux modèles sus-cités. En revanche sa réalisation est bien plus difficile qu'un service centralisé, notamment en raison de l'hétérogénéité et la complexité de l'environnement.

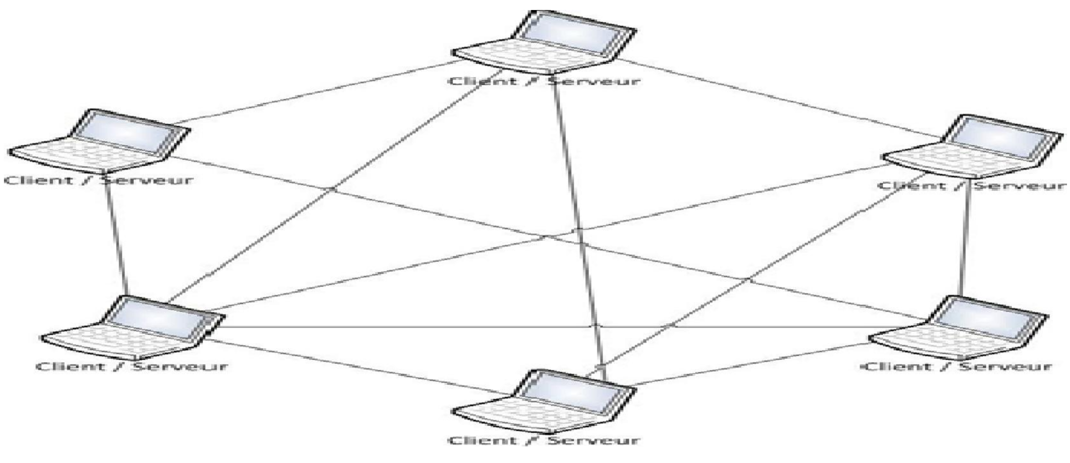


Figure 11 : Illustration de la décentralisation

La différence entre la centralisation et la décentralisation :

BASE DE COMPARAISON	CENTRALISATION	DÉCENTRALISATION
Sens	Le maintien des pouvoirs et de l'autorité en matière de planification et de décisions, avec la direction, est connu sous le nom de centralisation.	La dissémination de l'autorité, de la responsabilité et de la responsabilité aux différents niveaux de gestion est connue sous le nom de décentralisation.
Implique	Réserve d'autorité systématique et cohérente.	Dispersion systématique de l'autorité.
Flux de communication	Verticale	Ouvert et gratuit
La prise de décision	Lent	Comparativement plus rapide
Avantage	Bonne coordination et leadership	Partage du fardeau et de la responsabilité
Pouvoir de la prise de décision	Mensonges avec la direction supérieure.	Plusieurs personnes ont le pouvoir de prendre des décisions.
Les raisons	Contrôle inadéquat de l'organisation	Un contrôle considérable sur l'organisation
Le mieux adapté pour	Organisation de petite taille	Organisation de grande taille

Tableau 1: La différance entre la centralisation et la décentralisation [43]

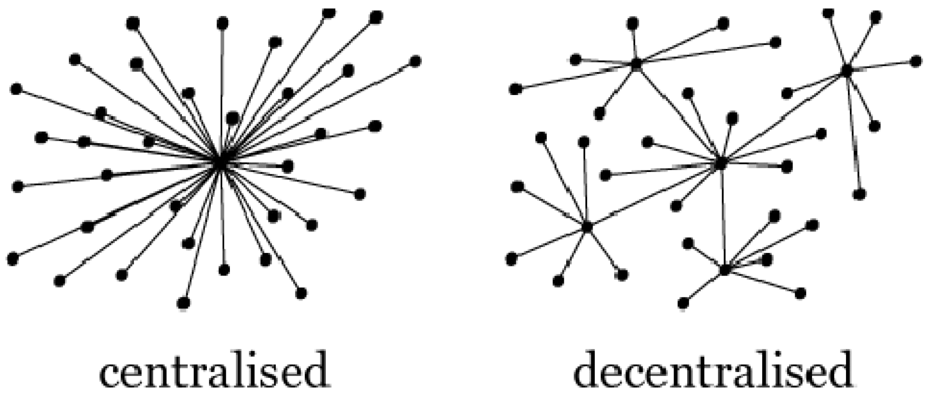


Figure 12 : différence entre la centralisation et la décentralisation [44]

2.3.Raisons d'utilisation de réseaux sociaux décentralisés

Parmi les points les plus controversés des réseaux sociaux se trouvent les utilisations, que font leurs administrateurs des données personnelles et privées des utilisateurs, donnant souvent à des applications externes la permission d'y accéder, suivant parfois une véritable stratégie commerciale. Relativement peu d'utilisateurs sont aujourd'hui conscients qu'en utilisant de telles applications, ils laissent la possibilité à des publics peu ou pas du tout identifiés d'accéder aux informations d'ordre privé stockées sur les serveurs des entreprises, qui fournissent le service- un comportement qualifié récemment de « à risque »par des experts légaux et technique. [30]

Ces effets secondaires comprennent : la nécessité d'un degré élevé de confiance le fournisseur OSN, les problèmes de censure et les problèmes de confidentialité. [29]

Protéger le système contre les deux attaquants de l'extérieur et de l'intérieur même de l'organisation du fournisseur. [29]

Récemment, plusieurs projets de rechercher et applications commerciales ont tenté, dans ce contexte, de proposer une alternative, en offrant des solutions permettant de contourner au moins certaines de ces limites ; Comme l'a résumé Niva Elkin-Koren, des solutions qui préfèreraient « éliminer les intermédiaires>dans les activités de partage et de réseau en ligne.

Ces propositions relèvent pour la plupart d'alternatives décentralisées aux services et aux outils qui occupent aujourd'hui une place importante dans notre vie.

D'autre raisons pour lesquelles nous énumérons un scandale survenu le 10 avril 2018 et que Facebook était la pièce maîtresse de l'affaire :
En mardi 10 avril 2018 Convoqué par le Congrès des États-Unis, Mark Zuckerberg, le Pdg (Président directeur général) du plus grand réseau social au monde, a réitéré ses excuses et va tenter d'expliquer comment les données personnelles de quelque 87 millions d'utilisateurs se sont retrouvées entre les mains de la firme d'analyse de données Cambridge Analytica. Retour sur ce scandale qui impacte la protection de la vie privée de 2,13 milliards d'utilisateurs et qui

remet en cause le cœur du business model de Facebook : la collecte de données à des fins publicitaires, qu'elles soient commerciales ou... politiques.

a. Définition Cambridge Analytica : [48]

Cambridge Analytica, créé en 2013, est une société basée au Royaume-Uni spécialisée dans l'analyse de données et la communication stratégique dont la maison-mère est Strategic Communication Laboratories. Son but est d'aider les équipes de campagnes politiques à s'adresser en ligne à des électeurs potentiels. Pour cela, la firme combine des données de sources multiples, notamment des informations en ligne et des sondages, afin de créer des « profils » d'électeurs.

Cambridge Analytica se sert ensuite de programmes prédictifs pour anticiper le comportement des électeurs, lesquels peuvent ensuite être influencés par des publicités ciblées. Pour cela, l'entreprise travaille avec d'énormes quantités de données utilisateurs. Elle revendique « 5.000 points de données sur 230 millions d'électeurs Américains », ce qui touche presque toute la population en âge de voter aux Etats-Unis qui est estimée à 250 millions de personnes.

b. Histoire de L'Affaire : [48]

Jusqu'à présent, ce dont on avait entendu parler au sujet de Facebook et la présidentielle US de 2016 **concernait l'ingérence d'opérateurs russes**. Ceci fait l'objet d'une enquête du FBI et du Sénat des Etats-Unis.

L'affaire impliquant la société de conseil stratégique **Cambridge Analytica** est un tout autre problème. Cette société britannique aurait acquis les données de millions de membres Facebook en violation des règles du réseau social. Elle a ensuite exploité ces informations pour créer des profils psychographiques de ces utilisateurs, mais aussi leurs amis, qui ont été utilisés pour concevoir des publicités politiques ciblées lors de la campagne sur le référendum du Brexit et l'équipe du candidat Donald Trump en 2016.

Facebook a indiqué avoir demandé à Cambridge Analytica de détruire ces données, ce qui n'a apparemment pas été fait. De son côté Cambridge Analytica assure avoir respecté les règles du réseau social avec des données « obtenues légalement et équitablement ». L'entreprise ajoute qu'elle a effacé les données qui suscitent l'inquiétude de Facebook.

c. Access les Données Facebook par Cambridge Analytica : [49]

C'est le point crucial de l'affaire. Dans un premier temps, les estimations affirmaient que 50 millions de données personnelles d'utilisateurs Facebook s'étaient retrouvées entre les mains du cabinet d'analyse - soit près d'un quart des électeurs américains. Mais le chiffre est grimpé à 87 millions de profils concernés, dont 81% situés aux Etats-Unis, d'après Facebook le 4 avril.

L'entreprise serait passée par un intermédiaire : un certain Aleksandr Kogan. Cet universitaire a développé en 2013 une application baptisée "thisisyourdigitallife", fonctionnant grâce aux identifiants Facebook. Ainsi, lors de son téléchargement, les utilisateurs concédaient un droit d'accès à leurs données personnelles sur la plateforme.

"Environ 270.000 personnes ont téléchargé l'application, chiffre Facebook. En faisant cela, ils donnent leur consentement à Kogan pour avoir accès à des informations comme leur ville d'origine, les contenus "likés" » mais aussi leur nom et prénom. Et ce n'est pas tout. L'application pouvait également avoir accès aux "amis" des utilisateurs l'ayant téléchargée. En 2014, Kogan aurait transmis ces données à Cambridge Analytica. Si l'accès aux données était légal pour le chercheur, leur transmission à un tiers constitue une violation des règles d'utilisation de Facebook.

"En 2015, nous avons appris que le Dr. Aleksandr Kogan nous avait menti", s'est défendus le réseau social. Une façon pour Facebook de se dédouaner sur l'usage détourné des données personnelles de ses utilisateurs. "Les gens ont connaissance de fournir ces informations. Aucun système n'a été infiltré, aucun mot de passe ou données sensibles n'ont été volées ou piratées", poursuit la plateforme. De son côté, Alexsandr Kogan estime servir de « bouc émissaire ».

Figure 13 : L'application connectée avec Facebook peut accéder à la donnée privée des utilisateurs facebook [49]

Le New-York Times par de « l'une des plus grandes fuites de données de l'histoire du réseau social ». Cela s'explique par le fait qu'environ 270.000 membres qui ont utilisé l'application d'Aleksandr Kogan lui en fait donné l'autorisation de collecter les données sur leurs amis. Au total, cela fait plus de 50 millions d'utilisateurs concernés. Le New-York Times s'est concentré sur l'exploitation non consentie de ces données.

Facebook a indiqué que bien qu'il ait mal agi avec des données, Aleksandr Kogan les a obtenues légalement et en conformité avec ses règles de l'époque. Le problème est qu'il n'était pas censé les transmettre à un tiers, en l'occurrence Cambridge Analytica.

Facebook conteste la thèse d'une fuite de données car l'accès aux informations s'est fait par des moyens normaux, via une application demandant aux usagers une autorisation à laquelle ils ont consenti. « Les gens ont fourni leurs informations en connaissance de cause, aucun système n'a été infiltré et aucun mot de passe ou informations sensibles volés ou piratés », a tenu à préciser Facebook.

Les critiques arguent que Kogan a pu faire ce qu'il a fait parce que le réseau social autorisait les développeurs d'applications à récupérer les données des amis d'un membre. Facebook a mis fin à cette pratique en 2015.

2.4.Décentralisation, réseaux sociaux et protection des données personnelles

Depuis les débuts d'internet, le principe de décentralisation a été à la base de la circulation des transmissions et télécommunications sur le réseau des réseaux. Pourtant, l'introduction du Web en 1990 a progressivement conduit à une large diffusion des modèles basés sur l'architecture client-serveur ; les services internet les plus répandus et les plus diffusés (réseaux sociaux, outils de messagerie instantanés, services de stockage de données numériques…) sont conçus à partir de modèles économiques et techniques dans lesquels l'utilisateur final demande une information, une donnée ou un service à de puissants centres de serveurs, qui stockent l'information et gèrent le trafic sur le réseau. Ainsi, même si sur internet le trafic fonctionne sur le principe de la distribution généralisée, il est aujourd'hui concentré autour de serveurs qui délivrent l'accès au contenu. Les observateurs pensent que cette tendance va se développer encore davantage avec la diffusion du modèle de cloud computing dans les marchés où services et plates-formes sont fournis clés en main ; dans ce modèle, le vendeur fournit l'infrastructure physique et le produit logiciel, abritant ainsi à la fois les applications et les données dans un lieu inconnu de l'utilisateur (le fameux « nuage », cloud en anglais), et interagit avec ce dernier grâce à une interface client. Ce choix d'organisation des structures et des services, à l'intérieur et en périphérie du réseau, n'est cependant pas le seul possible – et s'il est le plus répandu, il n'est probablement pas le plus efficace. Comme l'ont souligné des chercheurs comme Barbara Van Schewick, Eben Moglen et Niva Elkin Koren – pour n'en citer que trois –, l'une des alternatives possibles,, et potentiellement la plus prometteuse, est la décentralisation : concevoir le réseau de manière à ce que les communications et les échanges aient lieu entre des nœuds jouant tous un rôle symétrique dans le système, éliminant.Ainsi la dualité entre le fournisseur de service et l'utilisateur, typique du modèle serveur/client, et le remplaçant par une situation où chaque client devient serveur. [50]

2.5.Vers des réseaux sociaux décentralisés

Récemment, plusieurs projets de recherches et applications commerciales ont tenté, dans ce contexte, de proposer une alternative, en offrant des solutions permettant de contourner au moins certaines de ces limites ; comme l'a résumé Niva Elkin-Koren, des solutions qui préfèreraient « éliminer les intermédiaires » dans les activités de partage et de réseau en ligne. Ces propositions relèvent pour la plupart d'alternatives décentralisées aux services et aux outils qui occupent aujourd'hui une place importante dans notre vie quotidienne sous les noms de Google, Facebook, ou encore Picasa. Et si le modèle du réseau décentralisé était appliqué pour les réseaux sociaux du futur ? Les « premiers pas » des réseaux décentralisés marquent-ils l'arrivée de nouveaux paradigmes, de nouvelles possibilités de préserver le droit à la vie privée tout en maintenant, voire en améliorant, l'accès au réseau ? Penchons nous sur quelques exemple pour illustrer les développements en cours dans ce secteur, autour du très médiatique cas Diaspora et au-delà. [50]

2.6.Composants DOSN

Les composants de DOSN sont brièvement définis ci-dessous [30] :

Utilisateur : personne ou organisation possédant un identifiant et un profil d'utilisateur dans l'OSN.

Profil utilisateur : représentation numérique d'un utilisateur dans l'OSN, contenant toutes les données appartenant à l'utilisateur articles.

Poignée de l'utilisateur : identifiant unique pour chaque utilisateur partie du s système OSN.

Contenu : élément de données stocké ou partagé dans l'OSN.

Connexion : affiliation déclarée ou connaissance entre les utilisateurs (par exemple, les amitiés).

Node : périphérique réseau, utilisé par les utilisateurs pour se connecter à l'OSN.

Serveur : périphérique réseau, qui prend en charge de façon fiable la fourniture de services

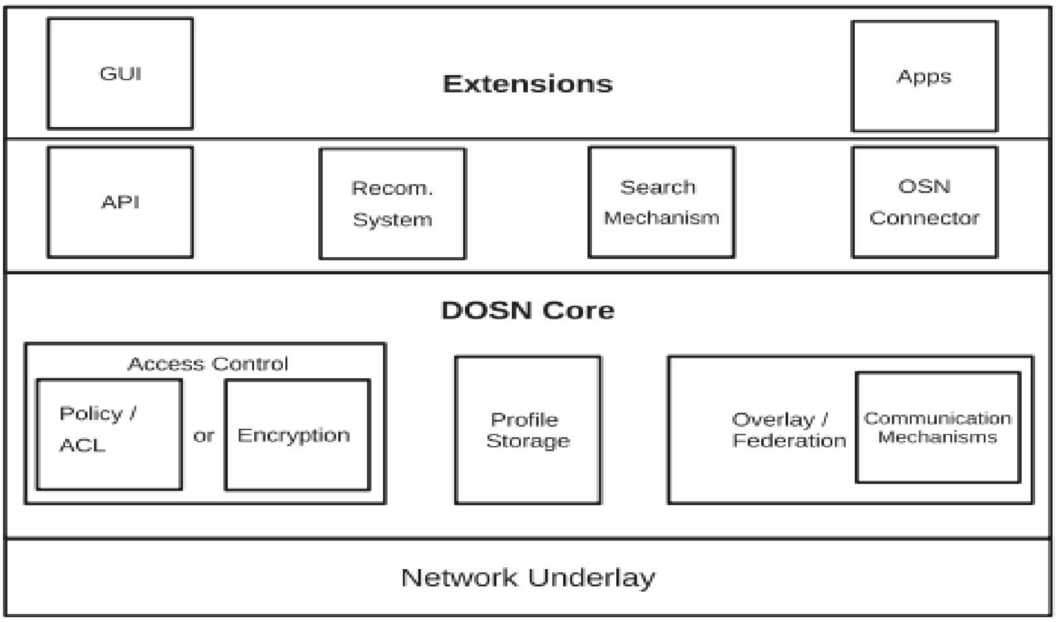


Figure 14 : Architectuer pour DOSN [31]

2.7.Les Exemples de DOSN [30]

1) **LotusNet :**

LotusNet [30] est une plate-forme P2P-OSN modulaire qui permet de réaliser des fonctionnalités de réseaux sociaux dans des widgets. L'infrastructure de communication ainsi que le schéma de chiffrement et la gestion d'identification est réalisée en utilisant la DHT modification Likir [31]. Le contrôle d'accès est réalisé par signé subventions pour la preuve des relations sociales. Le propriétaire des données par conséquent spécifie le type de relation sociale nécessaire pour accéder à l'élément de données.

2) **PeerSoN :**

Les auteurs de PeerSon [32] proposent une architecture à deux niveaux dans laquelle le premier niveau est un hachage distribué La table (DHT) et le deuxième niveau sont constitués des noeuds représentant les utilisateurs. L'idée est d'utiliser la DHT pour trouver les informations nécessaires pour les utilisateurs se connectant directement aux nœuds cibles. Cette approche est sans réplication

Planifie et stocke les messages hors ligne au DHT (OpenDHT dans la mise en œuvre du prototype). Tout le contenu de l'utilisateur est chiffré.

3) **Safebook** :

L'objectif principal dans Safebook [34] est de protéger la confidentialité des utilisateurs dans un environnement DOSN. L'architecture se compose de trois composants principaux, à savoir : Matryoshkas (un ego graphique ressemblant à un anneau reflétant les relations d'amitié), un service de recherche P2P et un Trusted Identity Service (TIS).

Chaque nœud est entouré de ses amis (premier shell) et amis-de-amis deuxième) shell dans sa Matroyschka. Les profils utilisateur sont répliqués pour une meilleure disponibilité des profils à nœuds de l'ami dans la coquille la plus intérieure. Les nœuds de la coque la plus extérieure sont des points d'entrée pour les demandes de routage vers le centre de la Matriochka et peuvent être trouvés en interrogeant le service de recherche. Cette structure de superposition cache les relations d'amitié des étrangers par le routage multihop. TIS vérifie les identités des utilisateurs.

4) **LifeSocial.KOM :**

Graffi et al. [35] présenter une approche où tous les OSNla fonctionnalité est réalisée par des plug-ins. Le stockage et l'échange d'éléments de données sont réalisés à l'aide de FreePastry [36].

PAST [37] est utilisé pour la réplication de données. Cryptographique

Les clés publiques sont utilisées comme ID utilisateur dans le réseau identifié ainsi de manière unique les utilisateurs en plus de chiffrer le contenu et des messages.

5) **DECENT :**

DECENT [38] est une architecture DOSN modulaire et orientée objet. Il exploite une DHT pour stocker l'utilisateur données et utilise la cryptographie pour protéger la confidentialité et l'intégrité du contenu appartenant à l'utilisateur. L'objectif des auteurs est un mur comme un blog plutôt que des messages de discussion. L'architecture est modulaire, c'est-à-dire les objets de données, la cryptographie et DHT sont trois composants distincts interagissant avec chaque

D'autres basés sur une interface. Cette modularité donne la liberté d'utiliser n'importe quel type de cryptographie (ABE basé sur [39] est suggéré dans DECENT) et tout type de DHT.

6) **Diaspora :**

L'objectif principal de la diaspora [51] est de construire un réseau fiable. Un réseau social en ligne décentralisé utilisable. L'architecture est basée (comme PrPL réseaux sociaux décentralisé) sur un modèle client-serveur où chaque utilisateur a sa propre instance de serveur (Pod : point of delivery) qui est utilisé pour le stockage, la communication et le contrôle d'accès.

En l'absence de réplication de données ou de services, les pods doivent toujours être en ligne pour une fourniture de services fiable. Un pod peut être hébergé sur son propre matériel ou par un fournisseur de services (service cloud). Les données sont stockées non chiffrées sur le pod, protégées par un mécanisme de contrôle d'accès.

2.8.Architecture DOSN

D'après nos recherches on a trouvé plusieurs réseaux sociaux qui utilise la décentralisation, chaque un à une architecture spécial.

Le tableau suivantrésume plusieurs exemples des RSD avec ses caractéristiques.

D = distributed.

FD = fully distributed.

BE = broadcast encryption.

OOB = out of band.

Ref = reference.

Arch	Ref	Degree	Storage		AC		Interact Mech.		Comments
			Peers	Server	ACLs	Encr.	Centr.	Dec.	
P2P-OSN	PeerSoN	FD	Previous download	_	_	PKI	_	Direct + DHT	Support for direct interactions (also with no Internet access)
	Safebook	FD	Trusted friends	_	_	PKI	_	DHT	Anonymity of interactions via encryption and recursive hop-by-hop routing
	LifeSocial. KOM	FD	DHT	_	_	BE	_	Plugins	Interactions based on external applications (plugins)
	LotusNet	FD	DHT	_	_	PKI	_	DHT	Based on Likir
	DECENT	FD	Random nodes in a DHT	_	_	ABE	_	DHT	Social network functionality on top of EASIER
	Cachet	FD	Random nodes in a DHT	_	_	ABE	_	DHT	Performance improvement of DECENT
F-OSN	SoNet	FD	_	Active	Servers	OOB or SMP	_	XMPP	XMPP-like architecture/social graph obfuscation
	Mantle	FD	_	Passive	_	OOB	_	Pub/	Group encryption on any storage, pub/sub

								submodel	for interactions
	PrPl	FD	_	Active	Cloud buttler	Undef.	_	Plugins	Cloud buttler either at home or in the cloud/ own language: SocialLite
	Diaspora	FD	_	Active	Hosting nodes	_	_	Hosting nodes	Trusted social hubs, hosting several user pods each
	[Anderson]	D	_	Active	_	PKI	_	Pub/sub	Multi-layer clients with sandbox for external Applications
Hybrid	Vis-a-Vis	FD	_	Passive	User pod	_	_	DHT	P2P substrate, data stored in user pods on personal devices/cloud services
	[Kryczka]	D	Social graph, locality	Active	Hosting node	_	Central Index	_	Centralized OSN extended with P2P content storage
	[Raji]	D	_	Active	_	BE	_	Pub/sub	Private data on personal storage, rest at OSN provider
	Polaris	FD	_	Passive	User home	_	_	Ext. apps + direct	Storage on phones or servers, NAT traversal necessary
	Confidant	D	Trusted Friends	_	_	OOB	Extern. Platform	_	Storage on trusted servers, existing OSN isused for signaling (notification)
	Vegas	D	_	Passive	_	PKI	_	Direct	P2P/reliable storage

Tableau 2 : Caractéristiques des RSD

2.9.Conclusion

La décentralisation d'OSN peut s'attaquer à deux questions :

Premièrement, c'est une possibilité de contourner la nécessité de faire confiance au SNP pour ne pas avoir appris des faits qui ne peuvent être cachés par cryptage. Un fournisseur omnipotent pourrait encore apprendre qui communiquée avec qui et à quelle fréquence. Deuxièmement, les utilisateurs ne font pas besoin d'accepter les transferts de droits d'auteur au SNP et les termes d'usage qui sont désavantageux pour eux.

Le résultat de la sécurité est que les DOSN visent principalement à protéger le contenu du fournisseur curieux et assurer la confidentialité de la communication avec l'utilisateur. Les DOSNs abolissent potentiellement la censure de contenu en tirant parti schémas de chiffrement À côté de Safebook, aucune des approches présentées introduit des mécanismes pour protéger contre l'observateur de la circulation ou le bâtiment des assaillants gouvernementaux graphiques de communication.

Chapitre 3

3. La technologie des chaines du bloc « Blockchain »

3.1. Introduction

Blockchain, la technologie derrière Bitcoin , semble être la technologie de conduite derrière la prochaine génération d'Internet, également appelé le Web décentralisé, ou Web3. Blockchain est une solution innovante au problème de confiance humain séculaire. Il fournit une architecture pour la confiance dite sans confiance. Cela nous permet de faire confiance aux sorties du système sans faire confiance à un acteur.

Un protocole Blockchain fonctionne sur le dessus d'Internet, sur un réseau P2P d'ordinateurs qui exécutent tous le protocole et détiennent une copie identique du ledger (registre) des transactions, permettant des transactions de valeur P2P sans intermédiaire grâce à un consensus machine. Blockchain lui-même un fichier - un registre public et partagé des transactions qui enregistre toutes les transactions du bloc de genèse (premier bloc) jusqu'à aujourd'hui.

3.2.Historique

La blockchain a été créée en 2008 avec la monnaie virtuelle bitcoin. Les deux sont donc historiquement liées : la blockchain est l’infrastructure virtuelle sur laquelle repose le bitcoin.

Le terme Bitcoin (B majuscule) renvoie à la fois à une monnaie numérique utilisant des techniques cryptographiques - le bitcoin (b minuscule) - et au protocole décrivant le fonctionnement du réseau sur lequel cette monnaie circule.

Ce protocole, c’est la blockchain, où la création monétaire et la validation des transactions s’effectuent de manière horizontale et transparente. Ce système fonctionne sans autorité centrale ni tiers de confiance, à l’inverse des monnaies contrôlées par des banques ou des gouvernements.

L’inventeur de Bitcoin (et donc de la blockchain) reste à ce jour inconnu, même si certains ont tenté de revendiquer sa paternité, sans réussir toutefois à présenter les preuves nécessaires. On ne connaît que son pseudonyme, Satoshi Nakamoto, sous lequel il a mis en ligne fin 2008 le *whitepaper* à l’origine de ce qu’il définissait comme un "système de monnaie électronique pair-à-pair". Il pourrait s’agir d’un individu mais aussi d’un groupe et ce mystère entretient une certaine mythologie autour de la figure de Satoshi Nakamoto.

Il propose un système basé sur des preuves cryptographiques, censées remplacer la confiance accordée aux institutions financières. Ce système a pour objectif de répondre à plusieurs enjeux [42] :

- Une transaction entre deux parties sans tiers de confiance
- Des vendeurs protégés contre d’éventuelles fraudes grâce à une impossibilité de supprimer ou modifier une transaction
- Des acheteurs protégés avec un système de comptes séquestres (terme juridique : indisponibilité d’un bien pendant une courte période)
- Pas de double dépense possible grâce à l’horodatage des transactions

3.3.Principe de fonctionnement

L'objet de cette partie est de présenter les blockchains d'une manière conceptuelle dans un premier temps, avant de préciser ensuite les mécanismes techniques liés à cette technologie, en s'appuyant sur la création du premier blockchain : celle du Bitcoin.

3.3.1. Un bloc

Un bloc est un enregistrement dans la blockchain qui contient et confirme plusieurs donneés ou transactions en attente. Toutes les 10 minutes (dans le cas de bitcoin), en moyenne, un nouveau bloc contenant des transactions est ajouté à la chaine de blocs par le minage [39].

Chaque bloc Bitcoin est constitué de :

Block : l'indice de bloc

Nonce : Un nonce ("nombre utilisé seulement une fois") est un nombre ajouté à un bloc haché qui une fois ré-haché répond aux restrictions de niveau de difficulté. Le nonce est le nombre pour lequel les mineurs blockchain résolvent [40].

Tx : la partie centrale qui contient une liste de transactions (les donneés).

Prev : champ contient l'empreinte de bloc précedant (bloc d'indice numero 1 dans notre exemple).

Hash : l'empreinte de bloc actuel.

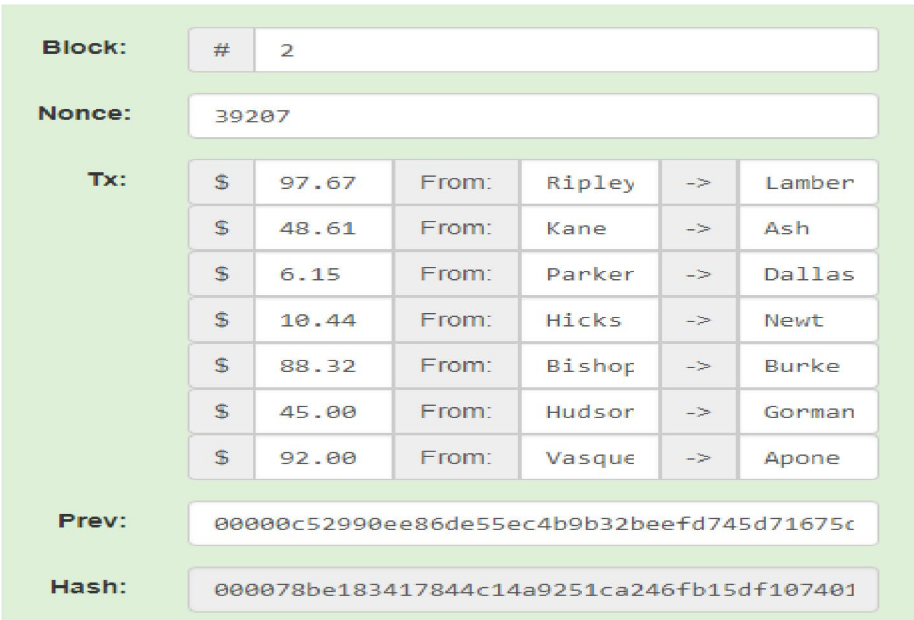


Figure 15 : Un bloc contient des transaction [42]

3.3.2. Blockchain

La Blockchain est une chaine de blocs de codes informatiques. Chaque bloc contient des attributs relatifs à une ou plusieurs transactions (expéditeur, destinataire, montant…), ou autres objets qui seront précisés ultérieurement. Il contient également des informations liées au bloc prédécesseur sur le Blockchain, et il est encrypté, c'est-à-dire qu'il est sécurisé à l'aide de procédés cryptographiques (algorithmes informatiques).

Lorsque les transactions récentes sont enregistrées, elles sont regroupées en bloc, et chaque transaction sera validée par les « mineurs », qui vont analyser la chaîne de blocs entière.

3.4.Mécanisme du blockchain

Pour une première approche du fonctionnement des blockchain, le plus facile est de raisonner avec un blockchain purement monétaire. On peut prendre l'exemple de Bitcoin, ou d'une blockchain avec des jetons "simples", pour laquelle une transaction se résume en fait à trois informations : qui donne quoi à qui [42].

Par exemple, on peut imaginer qu'Alexandre veuille donner deux bitcoins à Camille.

Les transactions effectuées entre les utilisateurs du réseau sont d'abord regroupées par blocs. Cette étape passée, il est nécessaire de vérifier qu'Alexandre a les moyens de réaliser cette transaction, avant qu'elle ne soit inscrite dans la blockchain. Le processus est simple, dans la mesure où la blockchain ne tolère pas le découvert : pour qu'Alexandre puisse envoyer ces bitcoins à Camille, il doit les avoir reçus au préalable.

Ceux qui sont chargés de vérifier la validité des transactions sont des acteurs du réseau que l'on appelle des "mineurs".

Lors de la vérification, l'historique des transactions d'Alexandre est remonté pour vérifier que ces 2 bitcoins qu'il a reçus précédemment n'ont pas été réutilisés depuis. On vérifie en fait tout simplement qu'il n'essaye pas de dépenser deux fois l'argent qu'il a reçu.

Une fois les vérifications effectuées, le bloc dans lequel se trouve la transaction entre Alexandre et Camille est validé par les mineurs, selon des techniques qui dépendent du type de blockchain, et qui permettent d'atteindre le consensus distribué, c'est-à-dire le consensus des noeuds sur l'état du réseau. Dans la blockchain Bitcoin, cette technique est appelée le "Proof-of-Work"2 (preuve de travail) [43] et consiste en la résolution de problèmes algorithmiques très lourds.

Afin d'ajouter un nouveau bloc à la chaîne de blocs, les noeuds participant à la création de la chaîne (les mineurs) doivent lancer un procédé cryptographique : le calcul du hash du bloc. Ce procédé a pour but de convertir des données en une suite pseudo-aléatoire de chiffres. Il est impossible de modifier les données en entrée de l'algorithme pour obtenir un résultat précis. Ceci est dû au caractère aléatoire de l'algorithme.

Voici comment marche un algorithme de Hachage : c'est une fonction mathématique qui, à partir de données (par exemple, un fichier Word), retourne une chaîne de caractères (64 dans le cas du Bitcoin). A un fichier correspond un unique hash, une unique empreinte, et il est impossible de retrouver l'information contenue dans le fichier à partir de son hash. Ainsi, la preuve de travail consiste à demander aux mineurs de calculer le hash des données constituées du bloc en cours de création (contenant l'empreinte / hash du bloc précédent), des données du mineur et d'un nombre aléatoire, afin de trouver un hash qui commence par un nombre de zéros défini [43].

Dans l'exemple suivant, la complexité (nombre de zéros en début de hash requis pour attribuer un hash à un nouveau bloc) est de 10. Le schéma ci-dessous montre l'activité des mineurs pour l'ajout d'un bloc sur la Blockchain [42].

Ainsi l'algorithme proposé est le suivant :

1) Calcul de :

   $fonction\ hash\ (Bloc, infosmineur, hash\ blocprécédent, \boldsymbol{nbrealéatoire1}) < C$

   Avec C : la valeur dépendant de la complexité. Par exemple, si la complexité est de 10, il faudra trouver un h inférieur à 0000000000ffffffffffffffffffffffffffffffffffffffffffffffffffffff. Le calcul s'effectue en hexadécimal (base 16), c'est-à-dire en une base allant de 0 à f.

   La fonction hash est aléatoire, ainsi la seule méthode de résolution de cette inéquation est de recommencer le calcul jusqu'à trouver la solution.

2) Recommencer le calcul de l'inégalité précédente en modifiant uniquement le nombre aléatoire, tant que la condition n'est pas réalisée

3) Lorsqu'une solution est trouvée, le bloc ainsi formé peut être envoyé à tous les noeuds du réseau

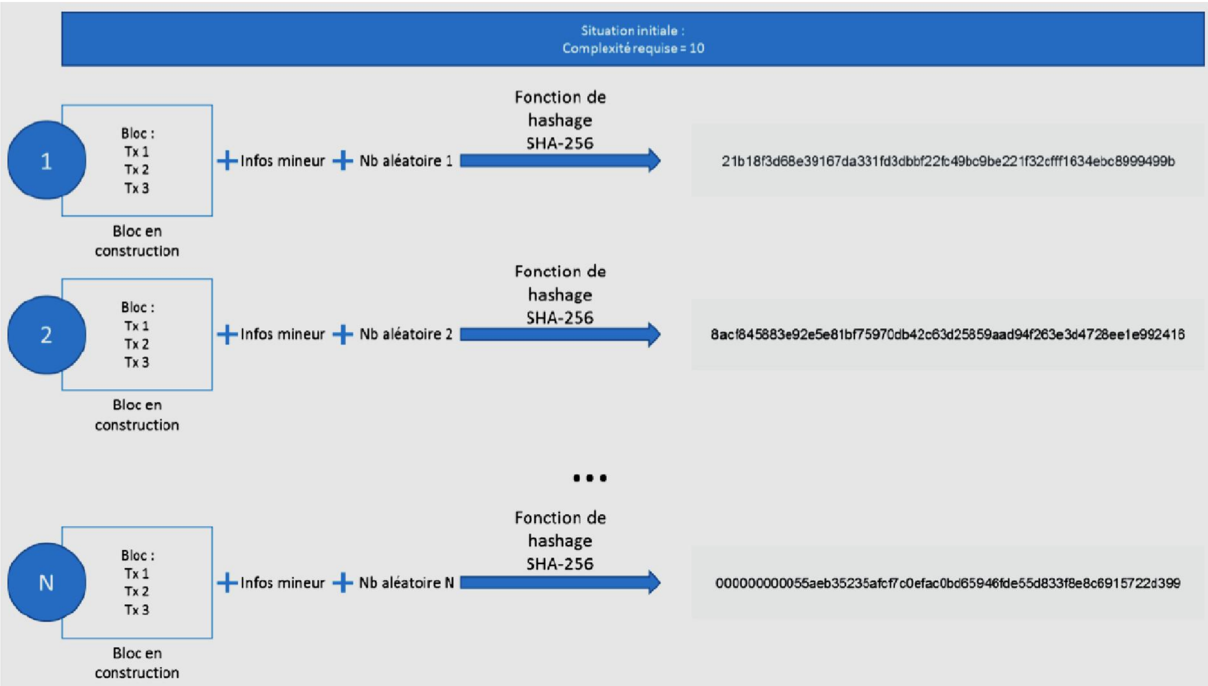


Figure 16 : Réalisation de la preuve de travail trouvée en N essais[43]

Si le bloc est validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. Camille possède maintenant ses deux bitcoins.

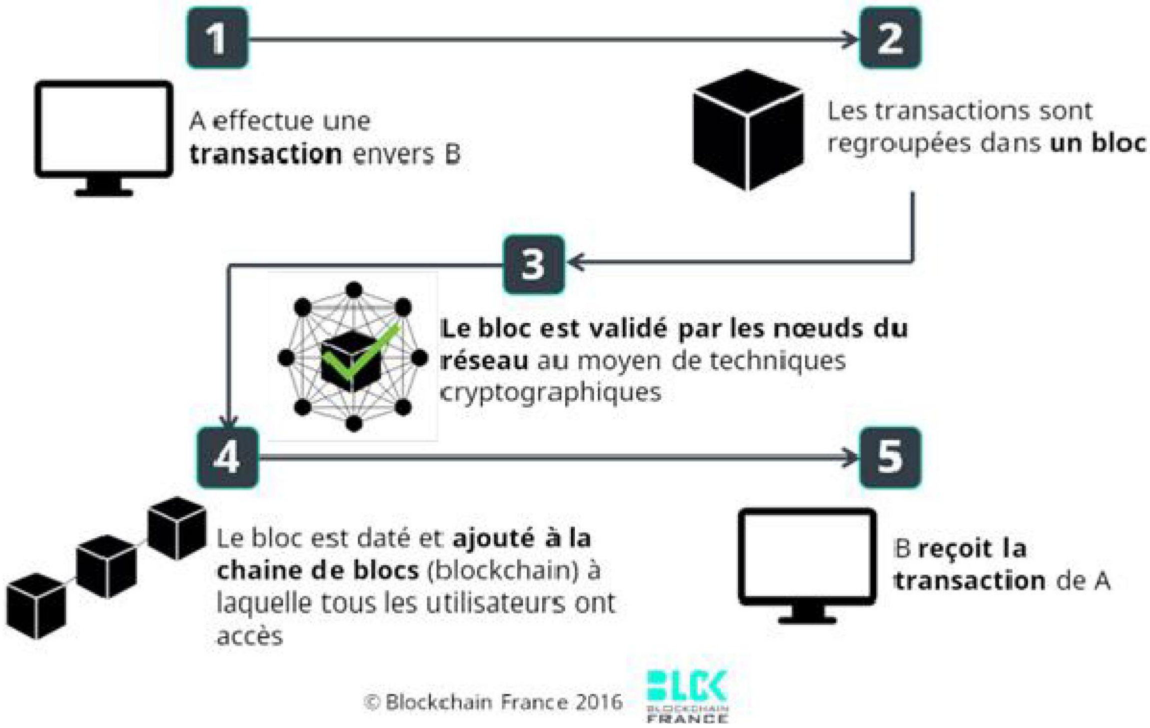


Figure 17 : Processus exécution d'une transaction avec la technologie Blockchain

Ce processus prend un certain temps selon la blockchain considérée (environ une dizaine de minutes pour Bitcoin, 15 secondes pour Ethereum). Le protocole modifie la difficulté du calcul afin que celui-ci ait toujours la même durée, celle prévue dans le code source.

3.5.Avantages et inconvénients du blockchain

De par sa structure décentralisée et transparente, la technologie de la blockchain comporte de nombreux avantages. Mais elle pose aussi certains problèmes.

3.5.1. Avantages de la blockchain

Absence d'intermédiaire

La blockchain pourrait révolutionner le système monétaire car elle ne nécessite plus l'intervention d'une structure bancaire. Avec les monnaies numériques qui utilisent la technologie blockchain, il est possible de faire des transactions directement de particulier à particulier sans intermédiaire. Plus besoin de banquier, d'une administration qui note et stocke toutes les informations concernant vos échanges monétaires. Toutes ces informations seront reprises dans les blocs de la chaîne. La monnaie cryptée est en quelque sorte sa propre administration bancaire [44].

Une économie de plusieurs milliards

Selon un rapport de la Goldman Sachs, la suppression de tous ces intermédiaires pourraient faire gagner chaque année plusieurs milliards de dollars aux institutions bancaires, aux marchés financiers et à de nombreuses industries. Le rapport parle de 2 milliards de dollars pour les États-Unis et de 6 milliards à l'échelle mondiale. Mais de nombreux autres secteurs pourraient également économiser de très importantes sommes monétaires en utilisant cette technologie [44].

"Ubériser Uber"

La blockchain pourrait également amener une réelle transformation de ce qui est aujourd'hui souvent appelé, à tort, l'économie participative ou l'économie du partage. Des entreprises comme Uber, AirBnb et Deliveroo ont construit leur empire sur ce système qui consiste à mettre en commun des travailleurs indépendants et des clients. Ces entreprises ont engrangé des bénéfices en retirant une commission chaque fois qu'un service était accompli. Comme l'explique Usine Digitale, à technologie de la chaîne de blocs pourrait faire disparaître ces intermédiaires en connectant directement les clients avec les vendeurs de services. Et toutes les questions administratives seraient conservées... dans les blocs [44].

Traçabilité et transparence

Les informations contenues dans la chaîne de blocs ne peuvent être effacées ni modifiées. Une fois qu'une opération a été réalisée, elle restera gravée à jamais dans la chaîne de blocs : ce qui permet de savoir exactement le chemin parcouru par les informations. Cette traçabilité et cette transparence sont un atout de taille pour les institutions bancaires - et ceux qui les surveillent. Avec ce système qui pourrait "révolutionner la finance", les banques pourraient retrouver la confiance d'une partie de la population [44].

Lutte contre la fraude

Puisque la fraude est souvent une affaire de manipulation de chiffres et de lettres sur des papiers, quoi de mieux qu'une technologie avec laquelle on pourrait stocker toutes sortes d'informations sans les modifier ? La blockchain joue ce rôle. Vente de logements sociaux, arnaque au kilomètres sur véhicules d'occasion, sociétés offshores... toutes ces informations pourraient se retrouver de façon chronologique dans un fichier sécurisé et aisément consultable [44].

Recherche scientifique et médicale

La création de la série des robots Sophia est un bon exemple de l'utilité de la blockchain. La start-up Singularity NET a pu développer ces intelligences artificielles articulées à visage humain grâce à un système de blockchain. Aucune information n'a pu se perdre en chemin et les chercheurs ont pu travailler sur le projet depuis plusieurs coins du globe. Cette absence de fragmentation du travail propre à la chaîne de blocs a également intéressé l'Union européenne qui y voit des applications dans le domaine de la santé, de la gestion des données personnelles ou encore dans le traitement de questions logistiques [44].

3.5.2. Les inconvénients du blockchain

Latence de traitement

La blockchain repose sur le réseau de nœuds pour valider les transactions, une opération qui prend en moyenne 8 minutes. En l'état actuel, la lenteur de ces vérifications freine l'adoption de cette technologie, en dépit de son caractère novateur. Le réseau et notamment les technologies de networking sont nécessaires pour accélérer les échanges mais aussi les sécuriser [45].

Absence de supervision réglementaire

Le système peer-to-peer distribué semble ne laisser aucune place à une instance de régulation. La législation et les réglementations sont à la traîne, laissant ouverte la question d'un fonctionnement sans cadre juridique [45].

Déficit de compétences techniques

Dans toute entreprise, une nouvelle technologie peut semer la confusion dans l'esprit de ceux qui sont en phase d'apprentissage. Les employés qui ne se tiennent pas au fait d'une technologie radicalement différente risquent de commettre des actions dangereuses pour la sécurité et de ralentir les opérations [45].

Incompatibilité avec les systèmes informatiques existants

Cette technologie révolutionnaire exige de profonds changements dans les systèmes existants et des investissements élevés au moment de la transition [45].

3.6.Autre application des blockchaine

La blockchain peut sembler abstraite sans exemples concrets. Nous avons choisi de présenter un certain nombre de cas d'usage destinés à illustrer le potentiel de cette technologie complexe et à montrer l'étendue de ses possibilités. Ces cas d'usage sont loin d'être exhaustifs, d'autant que la plupart des applications restent encore à construire. Ils suffisent néanmoins à comprendre l'étendue des possibilités offertes par la technologie.

3.6.1. Médicaments traçés et dossiers médicaux certifiés

Peut faire de cette technologie un moyen efficace de lutter contre la contrefaçon de médicaments. Tracés par son biais, ils pourraient tous être inscrits dans une unique base de données accessibles aux laboratoires pharmaceutiques comme aux particuliers. Ce même système pourrait également s'appliquer aux dossiers médicaux : La Blockchain décryptée évoque le partenariat conclu entre le gouvernement estonien et la start-up Guardtime, chargée de sécuriser pas moins d'un million de dossiers [46].

3.6.2. Officialiser et sécuriser les cadastres

Dans de nombreux pays en développement, certaines terres ne sont pas enregistrées dans une base de données officielle.d'ou le probleme de certain habitants qui ne possede pas d'adresse officiel. En Afrique, par exemple, 90 % des territoires ruraux ne sont pas inscrits dans un cadastre. Une absence de sécurité foncière qui, selon les auteurs de *La Blockchain* *décryptée*, "freine les investissements nécessaires au développement de la productivité agricole" et limite le développement du e-commerce, par exemple, "puisqu'il est tout simplement impossible aux foyers de se faire adresser des colis". Sans compter que cela limite le recours à l'emprunt pour les particuliers et peut être la source de conflits.

Ainsi, au Ghana, la start-up Bitland propose d'enregistrer les actes fonciers sur une blockchain. En 2015, le gouvernement du Honduras a fait répertorier l'intégralité de son territoire sur une blockchain grâce à l'organisme Epigraph pour éviter que les plus riches ne s'octroient des propriétés qu'ils ne possèdent pas [46].

3.6.3. Assurance

Le secteur de l'assurance est l'un des premiers avec le secteur financier à avoir manifesté son intérêt pour la blockchain. Des entreprises comme Lloyds ou Allianz France ont exprimé assez tôt leur volonté de lancer des expérimentations sur la blockchain, et début 2016, Axa a investi 55 millions de dollars dans la start-up Blockstream, qui doit permettre, entre autres, une interopérabilité entre différentes blockchains.

Alors que des modèles d'assurance peer-to-peer avaient déjà commencé à apparaître (par exemple Friendsurance), la blockchain y donne un nouvel élan grâce à des systèmes d'assurance automatisés fondés sur des smart contracts. Des entités appelées "oracles" permettent ainsi de gérer les données des smart contracts et de déterminer, par exemple, si les conditions sont bien remplies pour déclencher le paiement.

L'exemple souvent cité est celui de l'assurance dite indicielle ou paramétrique, autrement dit l'assurance liée à un indice tel que la température ou le niveau de pluie. Le smart contract conclu entre l'agriculteur et l'assureur peut par exemple stipuler que le paiement est effectué après 30 jours sans précipitations. Le contrat est alimenté par des données externes fiables (par exemple du service national de météorologie), qui permettent aux oracles de déclencher automatiquement le paiement après 30 jours de sécheresse, sans l'intervention d'un expert ni nécessité de déclaration ou revendication de l'assuré.

En automatisant l'exécution des contrats, ces mécanismes permettraient aux assurés comme aux assureurs de s'émanciper des phases déclaratives : formulaires, réclamation, vérification, déclenchement de l'indemnisation… La blockchain, en faisant office de tiers de confiance automatisé, ouvre ainsi la voie à une diminution des coûts de structure tout en fiabilisant et en accélérant les processus de décision. A terme, cela génèrerait également une plus grande satisfaction des assurés via la mise en place de nouveaux services plus intuitifs et plus rapides [46].

3.6.4. Reseaux sociaux

Steemit est un excellent exemple de ce que va devenir internet dans un futur proche, c'est pourquoi il est essentiel de se familiariser avec ce nouveau type de média. Il s'agit de la première plateforme de social media reposant sur une blockchain et qui rémunère pour les participations dans le développement de la plateforme.

Steemit fonctionne de la même manière que ses ancêtres (facebook, twitter…), les membres ouvrent des comptes, créé un profile, postent du contenu écrit/vidéo/audio, peuvent suivre les personnes qui les intéressent et avoir leur propre followers. La grande différence réside dans le fait que chaque membre peut voter pour le contenu posté par les autres membres et ainsi lui accorder une rémunération. En effet, dès qu'un membre vote pour un autre, Steemit va créer des Steem et les offrir au membre qui à posté le contenu. Ce membre peut soit décider d'échanger des Steem contre des monnaies nationales sur un échange crypto, ou de les conserver sur la plateforme et ainsi augmenter son influence [47].

3.7.Conclusion

A partir de l'étude menée dans les précédentes parties, on peut dégager plusieurs points clés liés à cette nouvelle technologie qu'est la blockchain.

Les éléments clés sont dans un cas général :

- Une information répartie entre tous les participants à la blockchain :
  - Un historique disponible pour tous (dans le cas d'une blockchain publique)
  - L'émission des transactions accessible à tous
  - Une validation réalisée par n'importe quel noeud (dans le cas d'une blockchain publique)
- Un système de comptes et de noeuds :
  - Des comptes de tiers et des comptes de contrats, les uns sécurisés par une

clé privée, les autres par le code qui les caractérise

- Des noeuds qui participent directement système distribué de la blockchain et permettent l'ajout de transactions à celle-ci

• Un système de preuve à fournir par les noeuds afin d'inscrire un nouveau bloc dans la blockchain, qui se caractérise par :

- Une résolution d'équation, ou d'inéquation
- Une difficulté (qui peut varier au cours du temps pour s'adapter à la situation)
- Une légitimité à pouvoir déposer un bloc sur la blockchain

Ces principes généraux sont malléables et peuvent être adaptés à des situations particulières. On peut citer comme exemple la différence entre les blockchains privées, publiques, ou de consortium.

Chapitre 4

4. Gérer l’authentification dans un réseau social décentralisé à l’aide de blockchaine

4.1. Introduction

La blockchain est une technologie émergente qui vise à ouvrir des capacités innovantes. Leur utilisation ne cesse d’augmenter et ceci dans de nombreux domaine qu’ils soient médicale, financière, administrative…etc .parmi ces domaine on peut citer l’utilisation du blockchain dans les réseaux sociaux décentralisés.

Dans ce chapitre, nous nous intéresserons à présenter notre contribution, Nous commençons par présenter l’authentification de manière détaillée. Ensuite on va expliquer notre proposition pour gérer l’authentification décentralisée à base du blockchain.

4.2. Authentification dans un réseau social centralisé

4.2.1. Définition

Lorsqu’un utilisateur veut accéder à un système d’information, il doit dans un premier temps effectuer une procédure d'identification et d'authentification.

L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question : "Qui êtes-vous ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur" ou "User" en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

Le code secret d'un utilisateur est une information personnelle qui ne doit en aucun cas être divulgués. Il est aussi communément nommé "mot de passe» ou "Password" en anglais.

Le mot de passe ne permet pas de donner un droit d'accès, il permet uniquement d'assurer l'imputabilité dans l'usage de ces droits d'accès

4.3.Motivation

D'après nous études on a trouvé que la concaténation de la décentralisation et la Blockchain réponde à tous les critères de la sécurité d'information (la confidentialité, l'intégrité et la traçabilité) et en plus une vie privé réel.

Vié privé réel

Les réseaux sociaux d'aujourd'hui, c'est la centralisation. Ainsi, Facebook sait tout sur ces utilisateurs, ses algorithmes connaissent les préférences, les souhaits, la façon de cliquer, les interactions… Seul Facebook possède ces données précieuses et les vend au plus offrant. Nous somme en tant que des utilisateurs des réseaux sociaux centralisé des merveilleuses publicités ciblées, ci par ce que tout simplement « le réseau social est gratuit, donc nous somme le produit ! ».

En décentralisant, les données appartiennent à leurs utilisateurs et non plus au réseau. Nos données privées ne sont alors plus publiques et retrouvent leur état d'origine : des données privées.

4.4.Contribution

Lancer la technologie de la décentralisation des réseaux sociaux vers une nouvelle ère, celui de la décentralisation de l'authentification on utilisant la Blockchain.

Durant cette partie une présentation conceptuelle du fonctionnement de notre idée sera présenter dans un premier temps, après suivront les détails liée à cette proposition.

4.4.1. Présentation

Comme nous l'avons expliqué précédemment dans le chapitre précédent, la Blockchain contient plusieurs blocs reliés entre eux sous forme de bus, la modification dans un bloc, nécessite des modifications dans les blocs suivant. Vu que chaque bloc contient une empreinte qui change en fonction des données, cette empreinte sera attribuée au composant du bloc suivant d'où l'impossibilité de modification des blocs précédent.

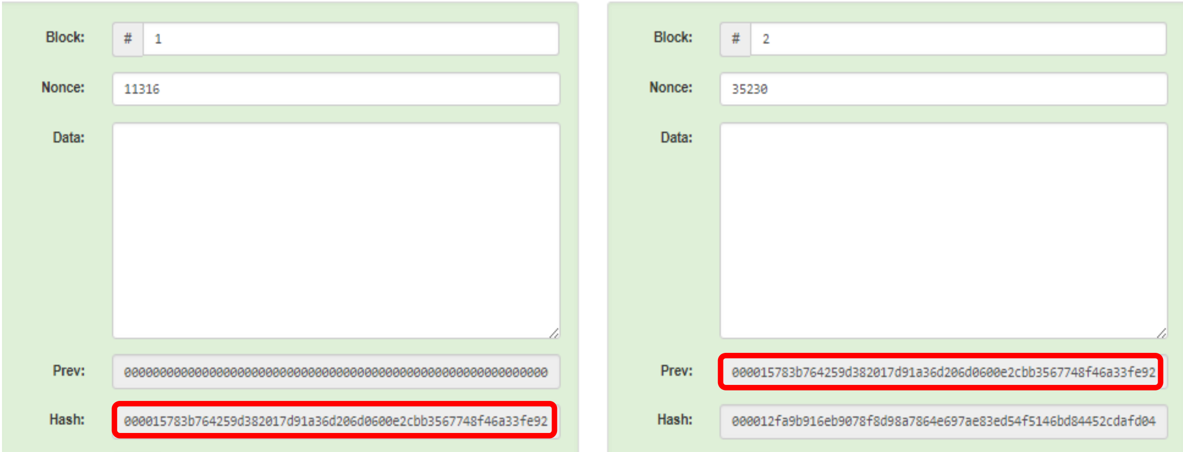


Figure 18 : Blockchain de deux blocs

Dans notre proposition, on a utilisé ce principe pour éviter la modification, et on va réserver chaque bloc pour contient l'empreinte des informations d'authentification (nom d'utilisateur+mot de passe) dans l'espace « Data » de chaque utilisateur.

L'empreinte est le résultat de fonction de hachage SHA256 du nom d'utilisateur+mot de passe, cette fonction est irréversible. Donc, une entité dispose la Blockchain, ne peut pas recalculer l'empreinte pour avoir les informations confidentielles.

La création d'un profil utilisateur implique un enregistrement dans le registre blockchain au niveau de son appareille et au niveau de blockchain dans le réseau.S'il utilise le même appareil, il c'authentifie directement à partir de son propre appareil. Sinon, dans le cas où l'utilisateur change son appareil ou il a perdu son registre enregistré au niveau de son appareil, il a besoin d'authentifier au niveau d'extérieur de son appareil (au niveau de réseau décentralisé).

4.4.2. Principe de fonctionnement

A. Le contenu du bloc

Dans notre proposition chaque bloc possède quatre attribues chaque un a un rôle qu'on va le préciser par la suite. La [figure 19] illustre d'une manière générale la structure de notre bloc.

Id
Données
Prev
Hash

Figure 19 : Structure d'un simple bloc

Les attributs du bloc sont présentés comme suit :

Id : identificateur du bloc (numéro de bloc ajouter à la Blockchain).

Données : contient les informations nécessaires pour l'authentification.

Prev : champ contient l'empreinte (hash) de bloc précédant.

Hash : l'empreinte du bloc actuel.

B. Création d'un bloc

Dans la création, l'algorithme récupère le nom d'utilisateur et le mot de passe parmi les informations entrées par l'utilisateur, puis utilise la fonction de hachage SHA256 afin d'obtenir une empreinte de 64 chaine de caractères en hexadécimale pour l'ajouter à la fin au « données » de bloc comme c'est illustré dans la figure [20].

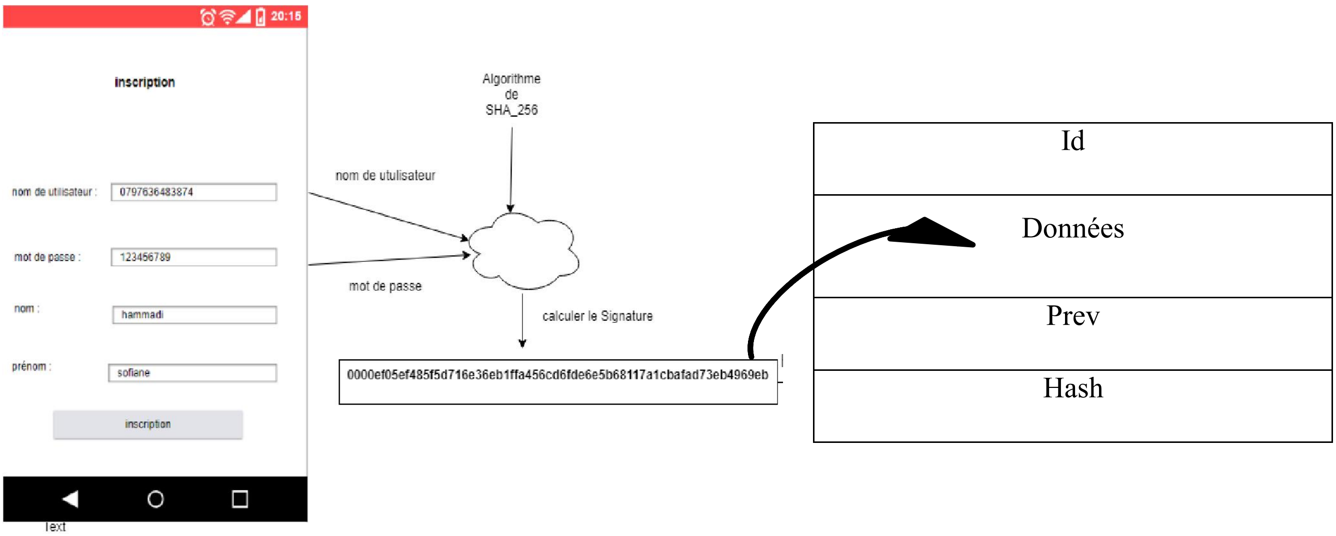


Figure 20 : Processus de création d'un bloc

L'algorithme suivant présente le principe de création d'un bloc.

Algorithme 1 : Création de bloc

Déclaration :

Did : dernier identificateur d'un bloc dans la Blockchain.
Dhash : dernier hash de Blockchain.
SHA-256() : la fonction de hachage.
user : nom d'utilisateur ;
password : le mot de passe ;
début
1 :Id← Did+1 ;
2 :Données← SHA-256(user+password) ;
3 :Prev←Dhash ;
4 :Hash←SHA-256(Id+Données+Prev) ;
fin.

Apres la création, le bloc sera ajouter au Blockchain. Puis tout l'utilisateur actif synchrone leur registre Blockchain afin de le stocker dans ses appareils.

C. Processus d'authentification

Après la création du compte (techniquement on parle de 'bloc'), On peut maintenant s'authentifier directement par la saisie du nom d'utilisateur et mot de passe puis calculer le hash et parcourir la chaine de bloc s'il existe dans l'appareil comme c'est présenter dans la figure[21].

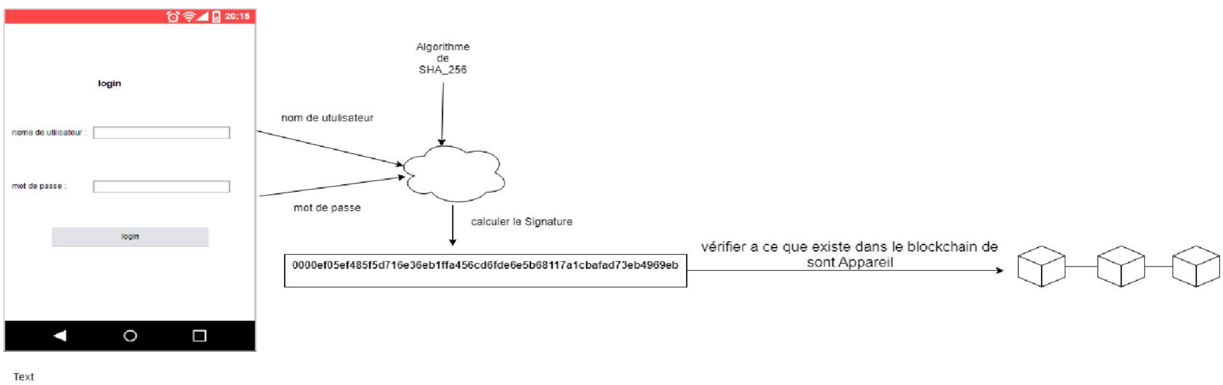


Figure 21 : L'authentification par Blockchain d'appareil

Si ce n'est pas le cas, dans le cas où l'utilisateur change son appareil ou il a perdu son registre enregistré au niveau de son appareil. Il a besoin d'authentifier au niveau de l'extérieur de son appareil (au niveau du réseau décentralisé).

Algorithme 2 : Authentification à partir d'appareil

Déclaration :

SHA-256() : la fonction de hachage.
user : nom d'utilisateur saisi.
password : le mot de passe saisi.
empreinte : variable qui contient le résultat de hash (user+password) saisi par l'utilisateur
Bapp <I> : registre Blockchain qui contient les blocs des utilisateurs à l'intérieur de l'appareil.
existe_empreinte : variable booléendéfini par **faux**
début
empreinte← SHA-256(user+password) ;
pouri allant de 1 **à** Bapp.length **faire**
si **(**Bapp<i>.données = = empreinte**)** **faire**
existe_empreinte ← vraie ;
fin si.
fin pour.
Si **(**existe_empreinte == vraie**)**faire
// utilisateur authentifier
sinon // échec d'authentification
fin sinon.
fin si.
fin.

Dans ce cas on a proposé des architecteurs de partage des Blockchains.

4.4.3. Blockchain dans tous les nœuds « broadcast »

Notre première proposition et que chaque nœud du réseau contient tous les blocs des utilisateurs. Autrement dit, dans le cas normale d'où y a pas des modifications et les nœuds récemment actif entraine de synchrone ça blockchain, chaque nœud contient la même Blockchain, donc pour qu'un nœud s'authentifier, il faut d'abord que le réseau valider une correcte Blockchain par un principe démocratique (plus que 51% des utilisateurs contient la même Blockchain). Puis parcourir la Blockchain, s'il existe une signature pareille à celle envoyé par l'utilisateur.

La procédure d'authentification est illustrée dans la [figure22]

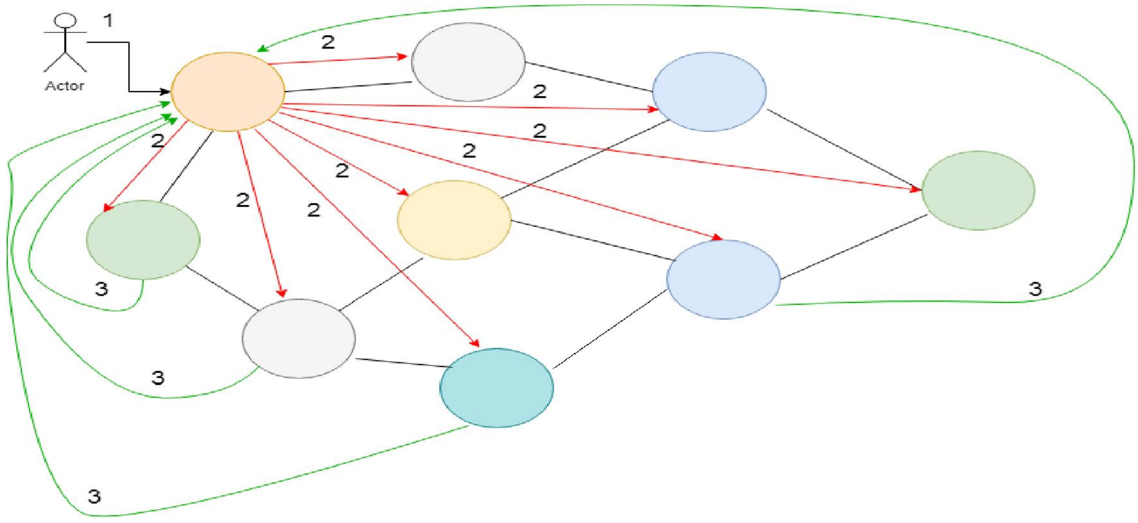


Figure 22 : Processus d'authentification broadcast

1. Un utilisateur par un nouvel appareil et introduit son nom d'utilisateur et son mot de passe et demande l'authentification.
2. L'appareil envoyé l'empreinte produit à tous les nœuds disponibles dans le réseau (requête d'authentification).
3. Chaque nœud réponde par son dernier Hash de Blockchain, puis l'algorithme valide la Blockchain correct et complet comme suit.

Algorithme 3: Authentification par la technique broadcast

Déclaration :

Déclaration :

SHA-256() : la fonction de hachage.
user : nom d'utilisateur saisi.
password : le mot de passe saisi.
empreinte : variable qui contient le résultat de hash (user+password) saisi par l'utilisateur
N : nombre des utilisateurs ayant reçu l'empreinte.
Tdh [] : tableau contient le dernier hash de chaque Blockchain dans chaque nœud.
getDhash () : fonction qui retourne le dernier hash dans la Blockchain de làle nœud
HPF : variable contient le hash le plus fréquent.
getBlockchain () : fonction qui returne la Blockchain de chaque neud
BlockchainV : variable contient la blockchain valide.
début
1 :empreinte← SHA-256(user+password) ;
2 : // diffuser l'empreinte dans tout le reseau.
3 :pour i allant de 1 **à Nfaire**
4 : // remplire dans le tableau le dernier hash de chaq**ue** utilisateur.

```
Tdh[i] ← getDhash() ;
fin pour
// parcourir le tableau Tdh[] et touver le hash le plus fréquent HPF .
// trouverla Blockchain dont son dernier hash égale à HPF .
pour i allant de 1 a N faire
Si (getDhash == HPF) faire
BlockchainV ← getBlockchain() ;
fin si
fin pour
pour i allant de 1 à BlockchainV.length faire
Si (Blockchain<i>.données == empreinte) faire
existe_empreinte ← existe_empreinte +1 ;
sinon
Ne_existe_pas_empreinte ←Ne_existe_pas_empreinte +1 ;
Fin sinon
Fin si
Fin pour
Si (existe_empreinte >Ne_existe_pas_empreinte )faire
// utilisateur authentifier
Sinon
// échec d'authentification
Fin sinon
fin si.
fin pour.
fin.
```

A. Les limites

Problème de stockage : avec l'augmentation des utilisateurs le nombre de blocs augmente, donc à un certain temps, le nœud ne peut pas supporter le volume de la Blockchain.

Problème de temps de réponse : avec l'augmentation des utilisateurs, la procédure prendre beaucoup de temps pour valider une Blockchain et même pour parcourir les blocs un par un d'une Blockchain très volumineuse.

B. Constat

Malgré ces limites, cette proposition est très sécurisé est rapide si on parle d'un réseau social qui ne contient pas beaucoup d'utilisateur, donc si faisable si on l'appliqué sur un réseau social spécifique.

Exemples : Réseau social d'une université, entreprise …

Afin d'amélioré notre première proposition. Et tant que notre demain d'application basé sur les réseaux sociaux on a ajouté les liens (relations) d'amitié.

4.4.4. Blockchain chez les amis « Clusturing »

On a proposé une deuxième proposition consiste que chaque nœud a une Blockchain spéciale, qui se compose de défirent blocs de ses amis, donc nous avons devisé notre vaste réseau en groupes d'amitié, maintenant pour authentifier un nœud il suffit que ses amies valident son bloc.

La procédure d'authentification dans ce cas :

Tant que chaque nœud a tous les blocs de ses amis, donc forcément chaque nœud à une blockchain déferrent de l'autre.

L'authentification ce fait dans ce cas par le principe de vote (oui, non), le nœud envoyé son empreinte d'authentification et ses amis vote par [oui, j'ai cette empreint parmi mes blocs] ou [non], ensuite l'algorithme calcule le nombre des oui et des non, puis si y a plus que 51% des oui, le nœud authentifier, si non le nœud n'authentifier pas. La technique est illustrée dans la [figure 23].

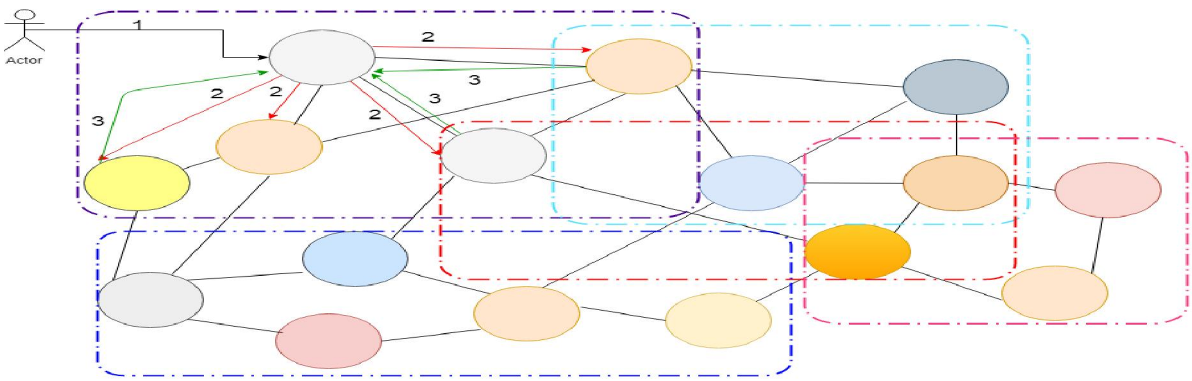


Figure 23 : Processus d'authentification par les liens d'amitié

1. Un utilisateur utilise un nouvel appareil et introduit son nom d'utilisateur et son mot de passe et demande l'authentification.
2. L'appareil envoyé l'empreinte produit à tous les amis disponibles dans le réseau afin de vérifier s'il existe l'empreinte dans leur Blockchain.
3. Chaque amis donne une réponse par (Oui ou Non), puis l'algorithme calcule le résultat de vote et authentifier si [nombre Oui > nombre Non] comme suit.

Algorithme 4 : l'authentification par amis

Déclaration :

SHA-256() : la fonction de hachage.
user : nom d'utilisateur saisi.
password : le mot de passe saisi.
empreinte : variable qui contient le résultat de hash (user+password) saisi par l'utilisateur
Blockchain<i> : liste des Blockchains pour chaque amis.
existe_empreinte : variable entier contient le nombre d'existence de l'empreinte dans tous les Blockchains des amis.
Ne_existe_pas_empreinte :variable entier contient le nombre d'absence de l'empreinte dans tous les Blockchains des amis.
N : nombre des amis ayant reçu l'empreinte

début

empreinte← SHA-256(user+password) ;

// l'envoi d'empreinte à ses amis.

pour i allant de 1 **à N faire**

Si (Blockchain<i> .données == empreinte) **faire**

existe_empreinte ← existe_empreinte +1 ;

sinon

Ne_existe_pas_empreinte ← Ne**_existe_pas_empreinte** +1 ;

Fin sinon

Fin si

Fin pour

Si (existe_empreinte >Ne_existe_pas_empreinte) faire

// utilisateur authentifier

Sinon

// échec d'authentification

Fin sinon

Fin si

FIN.

A. Limites

L'utilisateur ne peut pas s'authentifie si :

- Il n'y a aucun ami actif parmi tous les amis.
- L'utilisateur est nouveau et il n'a pas encore des amis.

- Un petit groupe d'amis qui peuvent modifier la blockchain, et puis n'autorise pas l'authentification bien qu'il appartient au réseau.

B. Constat

Indépendamment des limites mentionnées précédemment, cette proposition très efficace dans les aspects temps de réponse et stockage en raison du nombre réduit des nœuds qui contiennent le bloc ciblé. Afin de combler les lacunes, nous avons proposé une autre proposition d'utiliser une entité de confiance.

4.4.5. Tout la Blockchain dans des supers nœuds « Nœud de sauvetage »

Dans cette proposition on a modifié la structure de bloc pour se conformer à la proposition.

A. Le contenu du bloc

Chaque bloc possède sept attribues chaque un a un rôle qu'on va le précisé par la suite. La [figure 24] illustré on manière générale la structure de notre bloc.

Id
Données
Prev
Hash
prevF
hashF

Figure 24 : Structure de bloc dans la Blockchain de super noeud

Les attributs de bloc sont présentés comme suit :

Id : identificateur du bloc (numéro de bloc à ajouter à la Blockchain)

Données : contient les informations nécessaires pour authentification.

Prev : champ contient l'empreinte (hash) de bloc précédant.

Hash : l'empreinte de bloc actuel

prevF : champ contient l'empreinte (hash) de bloc d'ami précédant.

hashF : contient le hash de bloc entière après les liens d'amitié

B. La création de bloc

Cette etape nécessite une entité dite entité de confiance (super nœud ou nœud de sauvetage) qui va contient une Blockchain globale (tous les blocs du réseau).

Entité de confiance : nœud avec des performances élevé dans le reseau pour assurer la disponibilité du Blockchain (tout le temps en etat actif).peut etre une ou plusieurs avec une gestion de stockage précise, repartie (distribué) ou bien repliquée.

L'étape de création se fait on deux parties principales. Une partie qui se fait dans la phase de création, et une autre qui se fait dans l'entité de confiance :

Au niveau de la phase de création : A la saisie de nom d'utilisateur et de mot de passe pour la création, ces deux variantes sont concaténer et hachées en utilisant l'algorithme de hachage sha256, un hash de 64 chaines de caractère en hexadécimale chaque caractère codé sur quatre bits sera produit.

Phase de transit : le hash sera envoyé à l'entité de confiance.

Au niveau de l'entité de confiance : Comme mentionner en dessus chaque création de compte au niveau de l'interface implique une création d'un bloc, pour qu'un bloc soit crier l'entité de confiance attribuer à chaque bloc un id qui s'incrémente automatiquement en plus du résultat de hachage précèdent, et l'empreinte du bloc précédent, ces variante sueront hachés à leur tour afin d'obtenir un hash de bloc par rapport à la Blockchain.

Algorithme 5 : Création d'un bloc dans Blockchain de l'entité de confiance

Déclaration :

Did : dernier identificateur d'un bloc dans lablockchaind'entité de confiance.
Dhash : dernier hash deblockchaind'entité de confiance.
SHA-256() : la fonction de hashage.
user : nom d'utilisateur ;
password : le mot de passe ;

Enregistrer_block() :fonction qui sauvegarde le block dans blockchain d'entité de confiance

Blockchain_node <i> : blockchain qui enregistré dans l'entité de confiance
début
1 : Id← Did+1 ;
2 : Données← SHA-256(user+password) ;
3 : Prev←Dhash ;
4 : Hash←SHA-256(Id+Données+Prev) ;
5 : Blockchain_node <Id> ← Enregistrer_block (id, Donées, prev, Hash);
fin.

C. Authentification d'un nœud par l'entité de confiance

Comme le cas normal dans les réseaux sociaux. L'utilisateur entrer son nom d'utilisateur et son mot de passe, puis les hache par l'algorithme de hachage SHA256 dedans l'appareil afin d'obtenir une chaine de caractères. Cette dernière sera envoyée comme une requête au nœud de confiance et parcourir la chaine jusque on se trouve dans les données de bloc le même chaine de caractères envoyée par l'utilisateur donc on autorise cet identificateur à accéder à son compte.

D. Le cas des liens d'amitiés

Dans ce cas on propose de créer une nouvelle Blockchain spéciale avec la meme téchnique d'autentifier à partir des amies. Supposant les nœuds qui ont les identifiants suivant (3, 5,7) sont desamies pour le nœud (1), et il a ajouté un nouvel ami (9).Dans ce cas l'algorithme créer une Blockchain d'amitié de la même façon qui on a créé dans le nœud de confiance on utilisant les deux reste attribue PrevF qui contient le hashF d'entité précédente, et le hashF qui contient le résultat de hachage de toutes les informations du bloc.

Donc pour un utilisateur qui a des amis authentifiés, il n'est plus besoin d'authentifier de la part de nœud de confiance, car il y a des copiés de son bloc chez ses amis.Sauf dans les cas suivantes :

- Aucun de ses amis n'est en ligne.
- Le resultat d'authentification par son groupe d'amis est negatif.

Algorithme 6 : Authentification par l'entité de confiance

Déclaration :

SHA-256() : la fonction de hashage.
user : nom d'utilisateur saisi.
empreinte : variable qui contient le resultat de hash (user+password) saisi par l'utilisateur
existe_block : variable qui représente l'existence de block dans appareil ou no
user : nom d'utilisateur ;
password : le mot de passe ;
Blockchain_entité<i> : liste qui contient tout le block qui dans entité de confiance
Amie_online : variable qui contient nombre des amis qui sont online

Début
1 : **empreinte ←** SHA-256(user+password**)** ;
2 : // calculer le nouveau l'empreinte
3 : i← 0
4 :si (existe_block == 0 ou Ami_online == 0)faire
5 : Tanque (i **<**à **Blockchain_entité**.length**) faire**
6 : Si (Blockchain_entité<i>.données ==empreinte) faire
7 : // Connecté**et** sorte de la boucle
8 : Sinon //Pas connecté
9 : **Fin sinon**
10 : Fin si
11 : Fin si
FIN

La figure [25] suivante illustre notre proposition.

Fonctionnement :

1 ==>L'utilisateur introduit son nom d'utilisateur et son mot de passe.

2 ==> L'algorithme de hachage SHA-256 calcule l'emreinte de (USER + PASSWORD).

3 ==> L'algorithme choit un de trois méthodes d'authentification

4 ==> Authentifier à partir de son propre appareil.

5 ==> Sinon ; authentifié à partir de ses amis.

6 ==>Sinon ; authentifier à partir de nœud se souetage (super nœud, nœud de confiance).

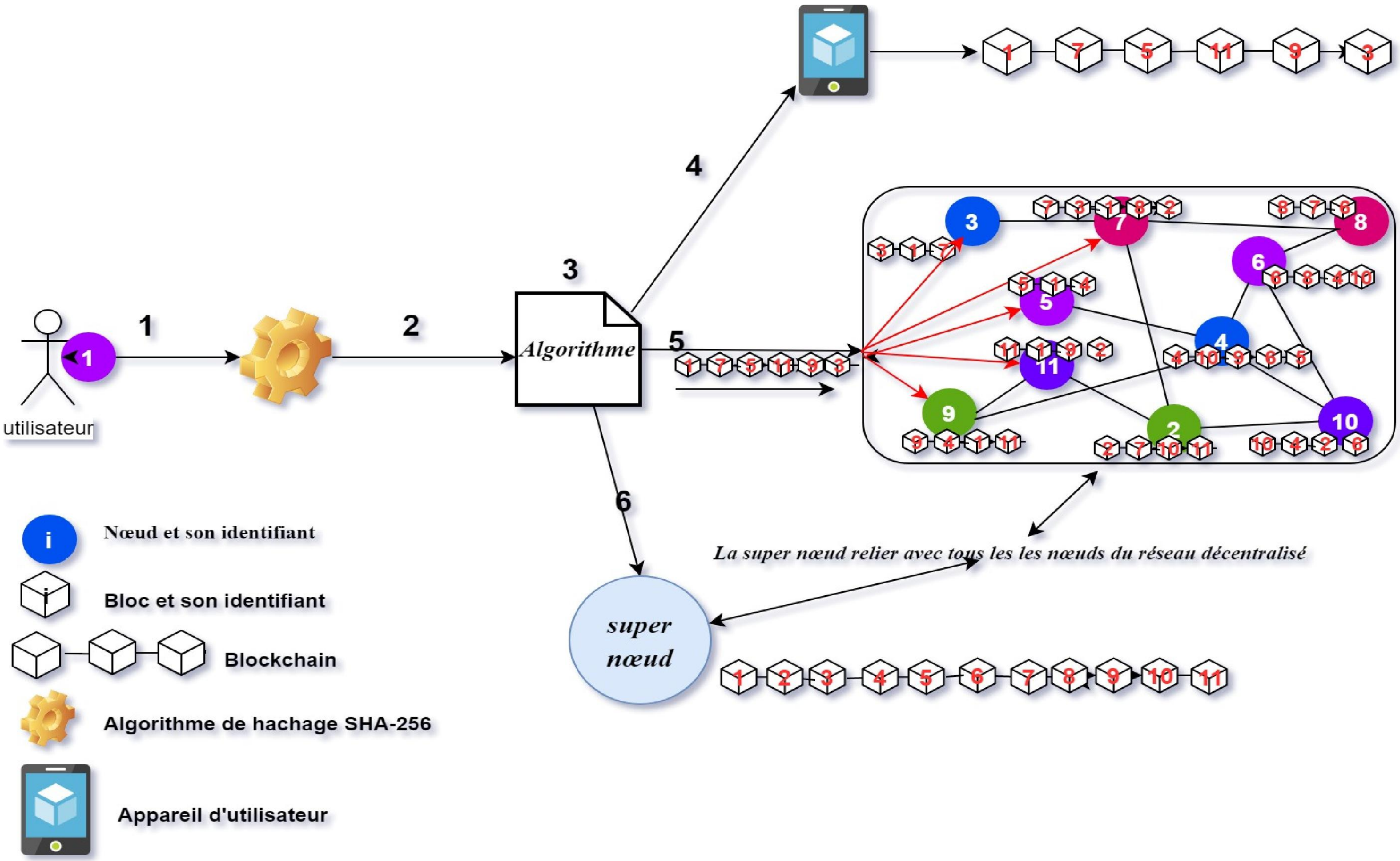


Figure 25 : Authentification par les trois possibilités

E. Les limites

Changement de mot de passe : Tant qu'on ne peut pas modifier et supprimer les blocs, on ne peut pas modifier le mot de passe d'un utilisateur.

F. Constat

Cette proposition donne une très bonne solution pour éviter de tomber dans les limites des proposions déjà citées.

4.4.6. Gestion de mot de passe

Il est evident qu'on ne peut pas modifier un bloc par ce que c'est on le modifier, l'empreinte change et donc tous les blocs suivants seront invalides. Le mot de passe modifié ne peut plus etre utilisé pour l'authentification mais il est toujours stockés dans la Blockchain.

C'est pour cela on a proposé d'ajouter un attribue « ChP » comme c'est présenté dans la [figure 26], qui sert à connaitre si ce mot de passe est ancien (modifié par l'utilisateur ou non).

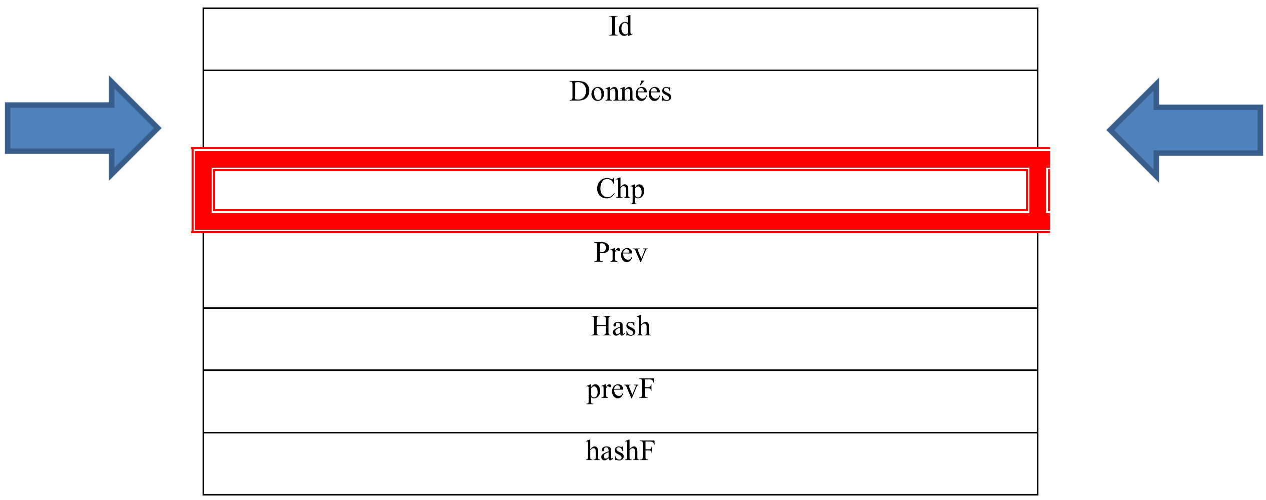


Figure 26 : Le bloc complet

ChP : ce champe indique que l'utilisateur a changé le mot de passe.

Mis à jour de mot de passe

On a proposé d'ajouter un bloc dans la Blockchain et on n'autorise pas l'accès à l'ancien bloc. Pour changer le mot de passe il faut d'abord entrer l'ancien et le nom d'utilisateur, puis on les hache au niveau d'appareil, puis on l'envoye vers le nœud de confiance afin de parcourir la Blockchain bloc par bloc jusqu'on le trouve, on récupère son identificateur (Id) puis on crée un nouveau bloc de la même façon qu'on a déjà précisé, et motionné l'identificateur du bloc qui contient l'ancien mot de passe dans l'attribue ChP du nouveau bloc.

Algorithme 7 : Changement de mot de passe

Déclaration :

Did : dernier identificateur d'un bloc dans lablockchain
Dhash : dernier hash deblockchain
SHA-256() : la fonction de hashage.
user : nom d'utilisateur saisi.
empreinte : variable qui contient le resultat de hash (user+password) saisi par l'utilisateur
new_password :variable qui contient le nouveau mot de passe
Chp :variable qui représente modification de mot passe
Block : block d'utilisateur
CréeBlock() : fonction qui crée un bloc
début
1 :empreinte← SHA-256(user+new_password);
2 :// recalculer le nouveau l'empreinte
3 : chp←Block.ID ;
4:// changement la valeur de cp par ID de dernière block
5:Prev←Dhash ;
6 **:**Hash←SHA-256(Id+ empreinte +Prev) ;
7 : CréeBlock(Prev, Hash,empreinte ,chp) ;
8 ://création block avec nouveau champ dans block qui définir si le mot de passe est changer ou pas
Fin

4.5.Conclusion

A partir de l'étude préalable on a inspérer des idées et on a amillioré a partir des critique de chaque idée, l'une après l'autre jusque on a trouvé une solution qui réponde à tous les critères d'authentification et on plus securisé et utile dans notre domaine d'etude les reseaux decentralisés.

Pour s'authentifier il a maintenant trois possibilités :

- A partir de son propre appareille s'il a le registre Blockchain.
- A partir du Blockchain de ses amis.
- A partir du Blockchain globale de l'entité de confiance.

Chapitre 5

5. Implémentation

5.1. Introduction

Pour étudier la faisabilité des propositions présentées dans le chapitre précédant, nous avons réalisé une application en utilisant des outils suivants :

- langage JAVA version 8.0.1520.16
- IDE(Integrated development environment)NetBeans,
- Bibliothèquegson-2.6.2

Dans ce chapitre, nous allons donc présenter quelques notions de notre application.

5.2. Outils de développement

- **Langage JAVA**

Java est un langage de programmation orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au SunWorld.

La société Sun a été ensuite rachetée en 2009 par la société Oracle qui détient et maintient désormais Java.

- **IDE NetBeans**

NetBeans est un environnement de développement intégré (EDI), placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License) et GPLv2. En plus de Java, NetBeans permet la prise en charge native de divers langages tels le C, le C++, le JavaScript, le XML, le Groovy, le PHP et le HTML, ou d'autres (dont Python et Ruby) par l'ajout de greffons. Il offre toutes les facilités d'un IDE moderne (éditeur avec coloration syntaxique, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web).

➢ Bibliothéque gson-2.6.2

Gson est une bibliothèque Java open source pour sérialiser et désérialiser les objets Java en JSONpour traitement des fichiers JSON avec langage java.

Cette bibliothèque utiliser pour convertir n'importe quel fichier dans notre application à fichier JSON pour faciliterles traitements de fichier

- **Fichier JSON :**

JavaScript Object Notation (JSON) est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Il permet de représenter de l'information structurée comme le permet XML par exemple. Créé par Douglas Crockford entre 2002 et 2005, il est décrit par la RFC 7159 de l'IETF.

5.3.Fonctionnement d'application

Dans notre application on a utilisé la technologie Blockchain et l'algorithme de hachage SHA-256 afin de sécuriser l'authentification d'un utilisateur dans un réseau sociale décentralisé.
La figure [27] représente l'interface graphique « Login », par lequel l'utilisateur peut accéder à son compte (authentifier) ou créer un nouveau compte.

Figure 27 : L'interface Login

5.3.1. Inscription

L'utilisateur afin d'accéder à l'application (son compte) il faut d'abord inscrire dans la page d'inscriptions par saisir ses informations comme suit :

Figure 28 : Interface d'inscription

Si l'utilisateur n'a pas saisir ses informations et il appuyé sur le bouton enregistrer, l'application affichéun message d'erreur qui lui demande de compléterses informations. Cette procédure assure le remplissage de tous les champs nécessaires comme il est indiqué dans la figure [29] :

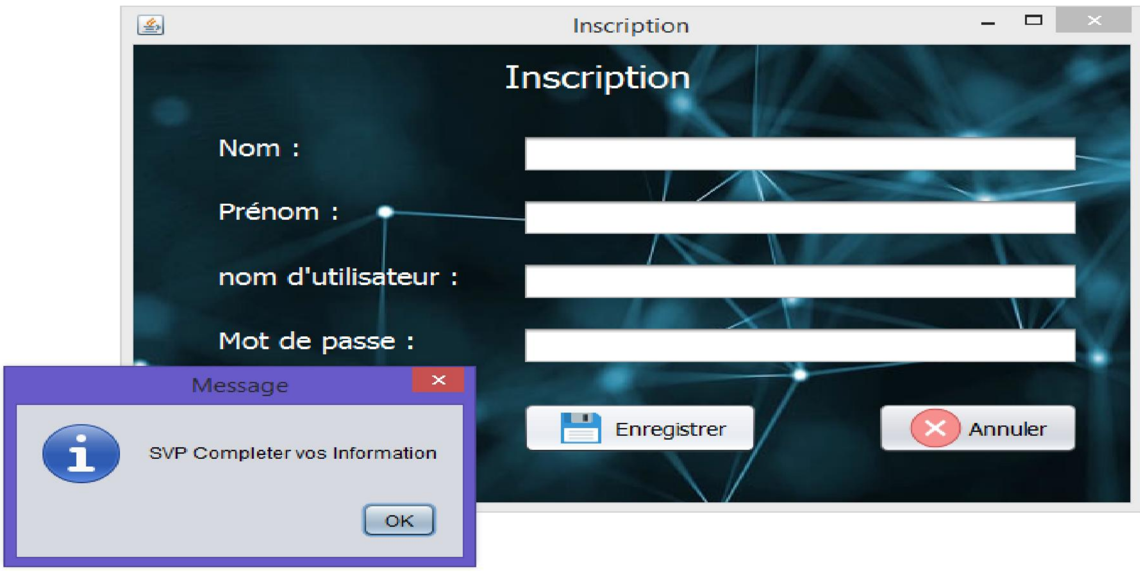


Figure 29 : message d'erreur

Si l'utilisateur rempli tous les champs et appuya sur le bouton « enregistrer » l'application va s'afficher un message de validation comme il est illustré dans la figure [30].

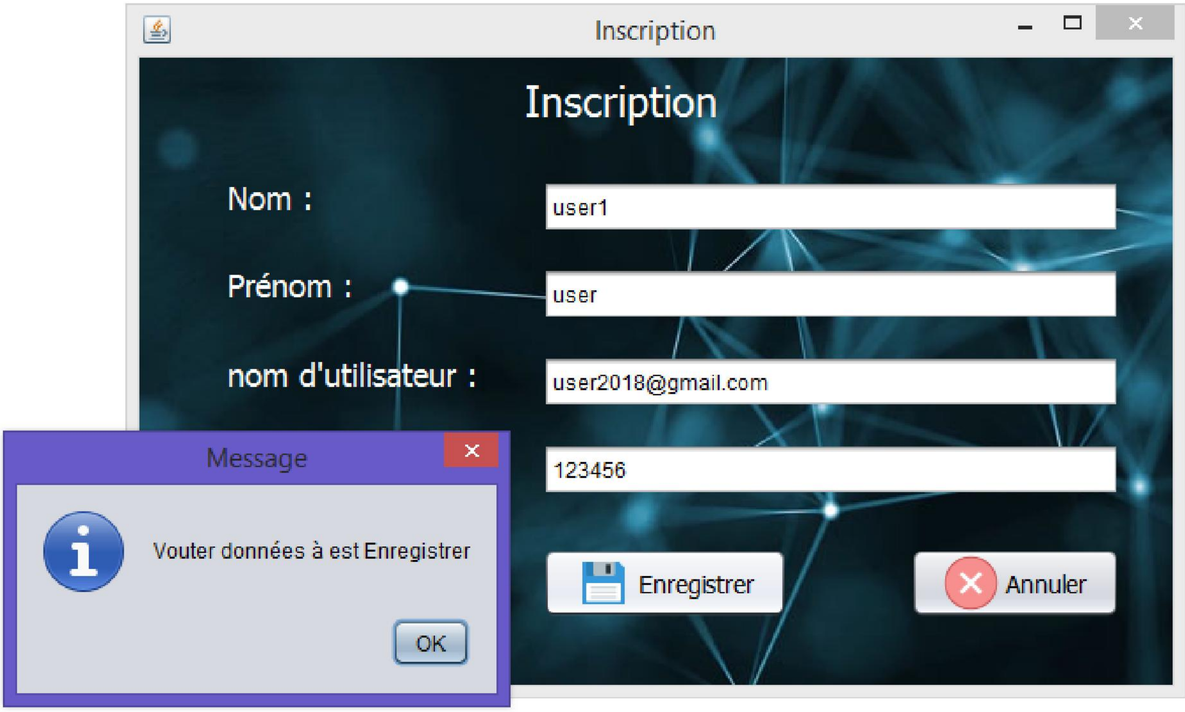


Figure 30 : Enregistrement des ifnoramtions

L'enregistrement dans le côté technique est une création d'un bloc dans un fichier de type JSON qui contient les attributs suivants :

"hash":"2c0ee067514a40bebb5fa1dd829ed192bbe76ff6f7593d2444e0dbd6f81c0801",

"previousHash":"0",

"data":"c3c97799bf69b0c366565618fe5a592d2ff68946b7cbdc44c1989fc782b68edc",

- **<u>Explication des attributs de fichier JSON :</u>**

hash : la signature (l'empreinte) de bloc courant créepar l'algorithme SHA-256, c'estle résultat de chiffrement de tous les données dans le bloc.

previousHash : la signaturedu bloc précédant. La valeur 0 dans le cas d'un premier bloc.

data : l'empreinte de [nom d'utilisateur + mot de passe].

- **Représentation de la Blockchain dans notre application :**

La Blockchain est unechainedes blocs liés entre eux.On va représenter le contenu du bloc dans notre application.

- Bloc :

Dans notre application on a représenté le bloc dans class qui s'appele« Block », dans lequel on a déclaré cinq (5)attributs. Le hash, la signature (l'empreinte) de bloc, la signaturedu bloc précédant« previousHash », data l'empreinte,user_name nom d'utilisateur, password : mot de passe d'utilisateur.comme suit :

```
public Block(String previousHash,String user_name,String Password ) {
            this.data = calculateSing(user_name,Password);
//Calculer  l'empreinte de  information d'utilisateur par fonction calculateSing
            this.previousHash = previousHash;
// Obtenir previous hash dans création block
             this.hash = calculateHash();
// Calculer   hash de block par fonction calculateHash
this.user_name= user_name;
this.password = Password;
            }
```

Pour créer un blocil faut faire une appele a le constructeur come suit :

```
Block new_Block = new Block ("0","user1","122345");
```

0 => La valeur 0 dans le cas d'un premier bloc.

Blockchain :

Comme nous l'avons dit plus tôt blockchain ce compose de plusieurs blocs est on a représenté dans notre application ce forme de ArrayList de type Block :

```
public static ArrayList<Block> blockchain = new ArrayList<Block>();
```

5.3.2. L'authentification

Figure 31 : interface d'authentification

Grace à cette étape on peut accéder à notre compte s'il existe dans la Blockchain, l'interface [31] présente deux champs (nom d'utilisateur et mode passe) a remplir. Au début on vérifiera d'abord si les deux champs ont saisi, comme il est présenté dans la figure [32].

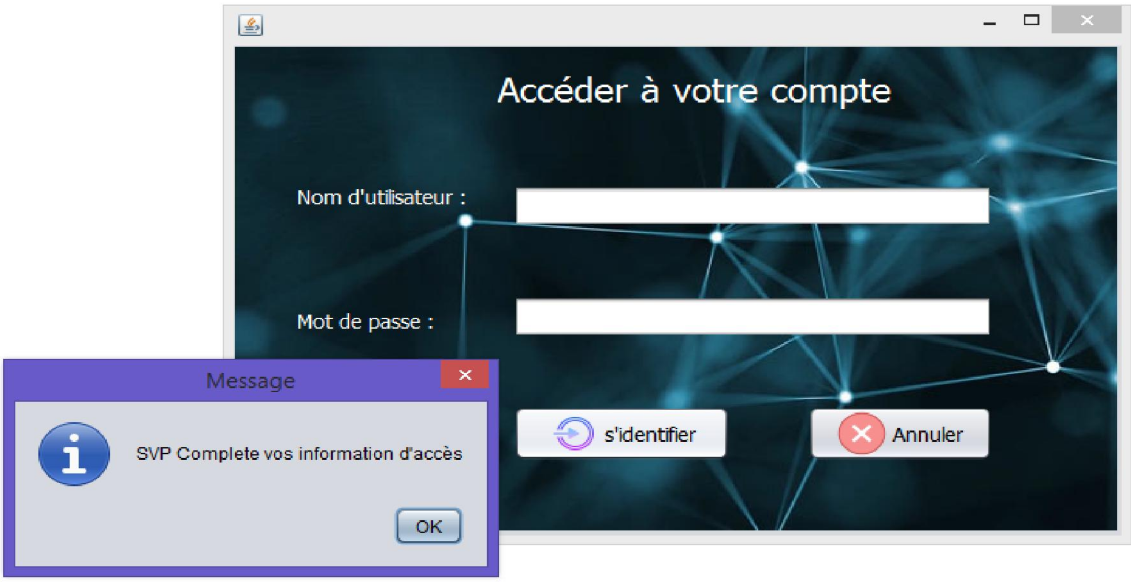


Figure 32 : vérification d'existence de deux champs

Si l'utilisateur clic sur bouton de « s'identifier » sans saisie ses informationsle programme affiche un message d'erreur qui demande àl'utilisateur de saisir ses informations.

Puis le programmeva récupérer le nom de utilisateur et le mot de passe saisie est calculer la signature (l'empreinte) par la fonction de chiffrement SHA-256 au niveau d'appareille afin de la vérifier si cette empreinte existe dans les Data «données » de blocs existants dans la Blockchain.

- **Cas de saisie des informations incorrectes :**

Dans ce cas veut dire y a pas l'empreinte d'utilisateur ni dans son propre appareille ni dans les Blockchain existants dans le réseau décentralisé. Donc le programme va afficherà l'utilisateur un message d'erreur qui lui demande de vérifier ses informations comme il est présentédans la figure [33].

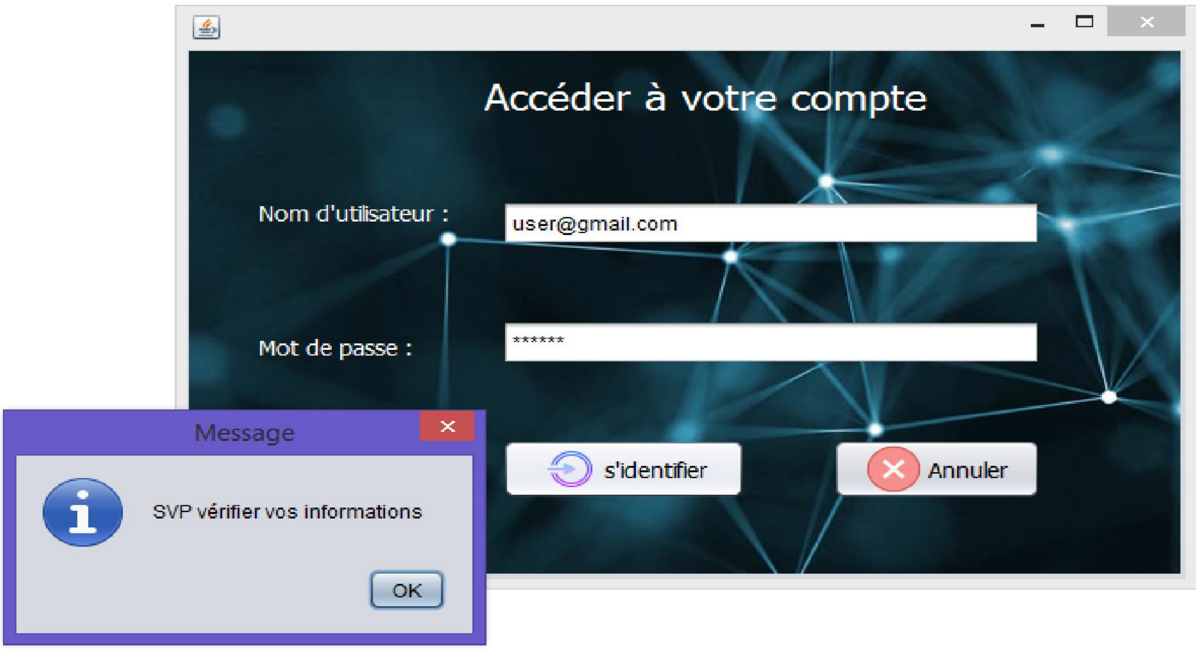


Figure 33 : vérification d'existence d'empreinte

- **Cas d'entrée des informations correctes :**

Dans ce cas l'algorithme a trouvé l'empreinte dans un bloc de Blockchain. . Donc le programme v'afficher à l'utilisateur un message de d'accès (la réussite d'authentification) comme c'est présenté dans la figure [34] et accéde a son compte [figure 35].

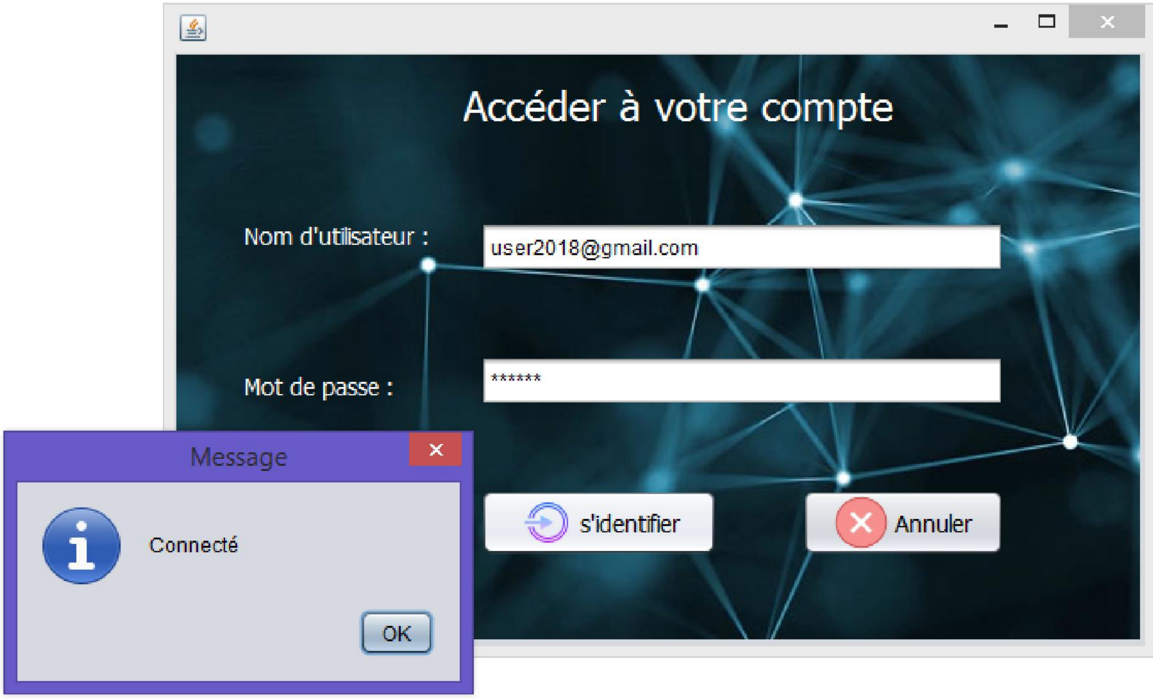


Figure 34 : La réussite d'authentification

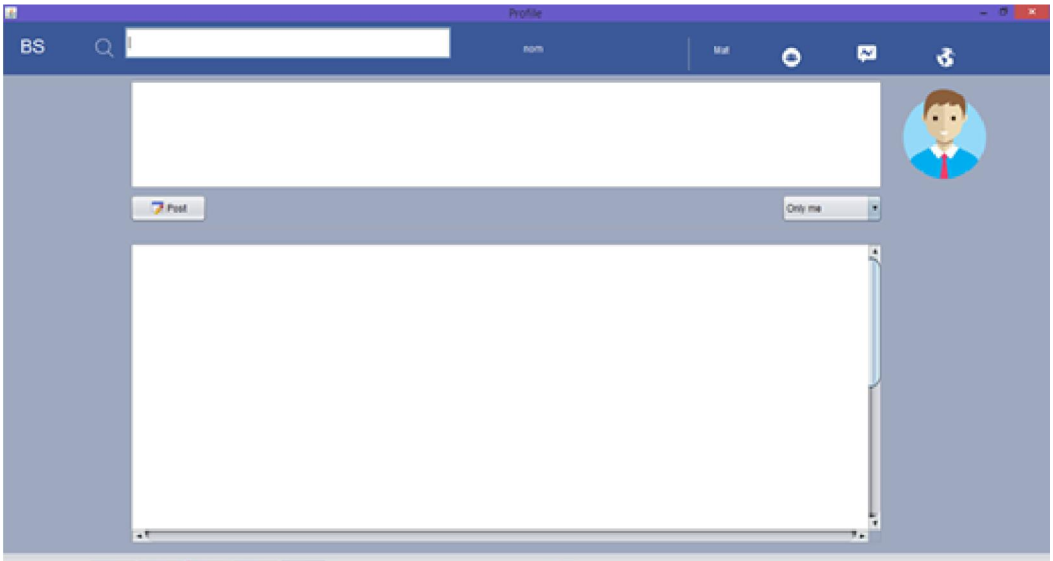


Figure 35 : L'utilisateur accéde à son compte.

5.3.3. Les fonctions

Dans un premier temps, lors de la création de l'utilisateur pour son propre bloc Au début, lorsque l'utilisateur crée son propre bloc et accède à son compte personnel, il n'a pas d'amis donc sa Blockchain contient un seul bloc. Dans chaque relation d'amitié entre un utilisateur et l'autre l'algorithme ajoute le bloc de nouveau ami dans la Blockchain.

Dans les réseaux décentralisés les nœuds jouent deux rôles (client/serveur), nous devons donc inclure deux fonctions, une fonction du serveur et une fonction du client.

1^er^ fonction pour le rôle de serveur :

```
Public static void envoyer_Fichier(intSocket_port,Stringfile_to_send) throws IOException{
// Socket_port représente le numéro du port envoyé via le fichier par un socket.
// file_to_sendreprésente le chemin du fichier à envoyer
FileInputStreamfis = null;
BufferedInputStreambis = null;
OutputStreamos = null;
ServerSocketservsock = null;
   Socket sock = null;
try {
servsock = new ServerSocket(Socket_port);//creation de socket
while (true) {
System.out.println("Waiting...");//Attendre acceptation de connexion
try {
sock = servsock.accept();
System.out.println("Connexion acceptée: " + sock);// Envoyer le fichier
File myFile = new File (file_to_send);
byte [] mybytearray  = new byte [(int)myFile.length()];
fis = new FileInputStream(myFile);
bis = new BufferedInputStream(fis);
bis.read(mybytearray,0,mybytearray.length);
os = sock.getOutputStream();
System.out.println("Envoi" + file_to_send + "(" + mybytearray.length + " bytes)");
os.write(mybytearray,0,mybytearray.length);
os.flush();
System.out.println("Done.");
      }
finally {
if (bis != null) bis.close();
if (os != null) os.close();
if (sock!=null) sock.close();//Fermer la connexion
      }
   }
   }
finally {
if (servsock != null) servsock.close();//Fermer la connexion
}
}
```

2eme fonction pour le rôle de client :

Si le fichier atteint le côté client, une fonction sera exécutée dans l'application client.

```
public static void reçu_fichier(intsokect_port,String server , String
file_to_received,intfile_size) throws IOException{
// sokect_port représente le numéro de port envoyé via le fichier via un socket.
//server  L'adressé IP de serveur.
//file_to_receivedest le chemin du fichier dans lequel le fichier envoyé est reçu
//file_sizeparamètre est la taille réservée pour le futur fichier.
intbytesRead;
int current = 0;
FileOutputStreamfos = null;
BufferedOutputStreambos = null;
   Socket sock = null;
try {
sock = new Socket(server, sokect_port);
System.out.println("Connecting...");      // recevoir le fichier
byte [] mybytearray  = new byte [file_size];
InputStream is = sock.getInputStream();
fos = new FileOutputStream(file_to_received);
bos = new BufferedOutputStream(fos);
bytesRead = is.read(mybytearray,0,mybytearray.length);
current = bytesRead;
do {
bytesRead = is.read(mybytearray, current, (mybytearray.length-current));
if(bytesRead>= 0) current += bytesRead;
     } while(bytesRead> -1);
bos.write(mybytearray, 0 , current);
bos.flush();
System.out.println("Fichier " + file_to_received
        + " téléchargé(" + current + " bytes read)");
   }
finally {
if (fos != null) fos.close();
if (bos != null) bos.close();
if (sock != null) sock.close();
}
// Appel à fonction copie
Copie(src,dist);
}
```

Après avoir accepté l'amitié, le bloc de l'ami « source » est envoyé dans un fichier vers le destinataire. À l'arrivée, la fonction « Copie » va copier l'empreinte « données » d'ami source, puis récrier un nouveau bloc et l'ajouterdans la Blockchain destinataire.

```
public static void Copie(String src , String dist)throws IOException{
// srcest le chemin du fichier source que nous sommes en train de copier
// distle chemin du fichier destinataire dans lequel nous allons copier le fichier source
File fin = new File(src);
FileInputStreamfis = new FileInputStream(fin);
BufferedReader in = new BufferedReader(new InputStreamReader(fis));
FileWriterfstream = new FileWriter(dist, true);
BufferedWriter out = new BufferedWriter(fstream);
String aLine = null;
out.write(",");
        //  out.write("\n");
                    while ((aLine = in.readLine()) != null) {
//Traiter chaque ligne et ajouter la sortie au fichier Dest.json
                              out.write(aLine);
                              out.newLine();
                    }
                    // do not forget to close the buffer reader
                    in.close();
                    // close buffer writer
                    out.close();
}
public static void main (String [] args ) throws IOException {
File dir = new File (".");//création d'objet de type File
String src = dir.getCanonicalPath() + File.separator + "block\\block1.json";
// Le chemin du fichier source
String dist = dir.getCanonicalPath() + File.separator+ "block\\block.json";
// Le chemin du fichier destinataire
reçu_fichier(SOCKET_PORT,SERVER,FILE_TO_RECEIVED,FILE_SIZE);
// La fonction qui reçoit le fichier
Prévios_hash = ReadFile(FILE_TO_RECEIVED);
//Récupérer le hash de block Précédent
data =  ReadFile2(FILE_TO_RECEIVED);
//Récupérer l'empreinte de client via le fichier envoyé par le client
New_Block =  new Block(Prévios_hash, data);
//Création  le block de client par recalculer le hash et leur empreinte
sv.crunchifyWriteToFile(gson.toJson(New_Block),src);
//Créer le block dans fichier json
copie(src,dist);//copie le block dans blockchain de serveur
  }
```

5.4.Conclusion

Dans ce chapitre on a choisie l'architecture « clustering » parmi les propositions qui nous avons proposé afin de géré l'authentification d'un réseau social décentralisé ou bien sécurisé l'authentification d'un RSD par la technologie puissante et récente Blockchain. Afin de prouver la possibilité d'utilisation de notre idée dans le domaine.

Conclusion générale et perspectives

On a proposédans ce mémoire de fin d'etude, l'authentification dans un réseau social decentralisé basée sur la technologie Blockchain. Une chaine des blocs reliés par des liens mathématique (fonction de hashage).

On a proposé quatre possibilités à un utilisateur pour accéder à son compte (s'authentifier) :

- A partir de son appareil qui contient une copie du Blockchain.
- En demandant aux utilisateurs en etat actif dans le reseau.
- En demandant à ses amisseulement.
- A partir d'une entité de sauvetage dans des cas particuliers.

D'après nos connaissances, notre proposition est parmi les premières tentatives pour exploiter la technologie Blockchain dans les réseaux sociaux. Malgré l'innovation qu'elle englobe, nous reconnaissons que notre solution souffre de plusieurs difficultés et nécessite plusieurs raffinement pour arriver à un état fiable et consistent.

Comme travail futur, nous envisageons :

- L'implémentation de la proposition dans une application qui assure au moins les fonctions de base d'un réseau social (amitié, messagerie, publication, partage).
- L'amélioration des algorithmes d'authentification pour optimiser le temps de cette opération.
- Minimiser le nombre de blocks stockés dans les nœuds à faible capacités.

Bibliographie

[1]: PS Dodds, R Muhamad and DJ Watts (2003), An experimental study of search in global social networks, Science 301: 827-829.

[2]: BARNES, J. « Class and communities in a Norwegian Island Parish», Human Relations, n°7, 1954

[3] : Torloting P. Enjeux et Perspectives des Réseaux Sociaux. Institut Supérieur du Commerce de Paris : Marketing, Management et Technologies de l'Information. 2006.

[4]: O'Reilly, T., (2005) What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, Communications & Strategies, No. 65, 17-37

[5] : Lazega E. (1998), Réseaux sociaux et structures relationnelles, Paris ; Que sais-je ? N° 3399, PUF.

[6]: Garton L., Haythornthwaite C., and Wellman B. (1997). « Studying Online Social Networks», Journal of Computer-Mediated Communication, Vol. 3, No. 1.

[7] : Lemieux Vincent, *Les réseaux d'acteurs sociaux*, Paris, Presses universitaires de France, 1999.

[8]: Burt R. S., (1992), Structural Holes. The Social Structure of Competition, Harvard University Press.

[9] : Boyd D. M., Ellison, N. B. (2007). « Social network sites: Definition, history, and scholarship". Journal ofComputer-Mediated Communication, 13 (1), article 11.

[10]: Joshi, P. and C.-C. Kuo (2011). Security and privacy in online social networks: A survey. Multimedia and Expo (ICME), 2011 IEEE International Conference on, IEEE.

[11]: LES Z'ED. http://les-zed.com/qu-est-ce-que-les-reseaux-sociaux/(consulté le 13/10/2018).

[12] : (Dupin A. (2010), Communiquer sur les réseaux sociaux, Editions Fyp, France.)

[13] : LEFEBVRE A., Les réseaux Sociaux, Pivot de l'Internet 2.0, M2 Editions, Paris 2005.

[14] : Cardon, D. (2011). « Pourquoi l'internet n'a-t-il pas changé la politique ? ». URL:http://internetactu.blog.lemonde.fr/2011/08/19/dominique-cardon-pourquoi-linternetna-t-il-pas-change-la-politique.

[15]: THELWALL Mike, "Social network sites: Users and uses," M. Zelkowitz (Ed.) Advances In computers Elsevier, vol. 76, pp. 19-73, 2009.

[16] : Ziryeb Marouf. (2011). Réseaux sociaux numériques d'entreprise : Etat des lieux et Raisons d'agir, Harmattan.

[17] :Cavazza, F. (2018). Description des différents types de médias sociaux. Mediassociaux.fr. 5 Mai 2018.
Repéré àhttps://fredcavazza.net/2018/05/05/panorama-des-medias-sociaux-2018/

[18] : Cavazza, F. (2012). Panorama des médias sociaux 2012. Mediassociaux.fr. 20 février 2012. [Consulté le 14-04-2018]
Repéré àhttp://www.mediassociaux.fr/2012/02/20/panorama-des-medias-sociaux-2012/

[19] :Delcroix É. Qu'est-ce que les réseaux sociaux ? [consulté le 14-04-2108]. Disponible :http://leszed.ed-productions.com/qu-est-ce-que-les-reseaux-sociaux.

[20] : http://www.webmarketing-com.com/2016/04/08/46793-5-tendances-social-media-2016 (consulté le 20-04-2018)

[21]: Mohamed Reda Bouadjenek, Hakim Hacid c, Mokrane Bouzeghoub,Social networks and information retrieval, how are theyconverging? A survey, a taxonomy and an analysis of socialinformation retrieval approaches and platforms. Information Systems, Elsevier, 2016,56, pp.1-18. <10.1016/j.is.2015.07.008>. <lirmm-01174843v4>

[22] :http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014 (consulté le 21-04-2018)

[23] :http://www.alexa.com/topsites (consulté le 21-04-2018).

[24] : http://newsroom.fb.com/company-info/(consulté le 13-10-2018)

[25] :https://twitter.com/search?q=until%3A2006-03-2%20%20lang%3Aen&src=typd

[26] :http://www.journaldunet.com/ebusiness/le-net/nombre-d-utilisateurs-twitter-0112.shtml(consulté le 13-10-2018).

[27] :https://about.twitter.com/fr/company (consulté le 21-04-2018)

[28] :https://wearesocial.com/fr/blog/2018/01/global-digital-report-2018

[29]:Francesca Musiani. Connectés mais protégés : le pari des réseaux sociaux décentralisés. ParisTech Review, 2011

[30]: ThomasPaul, Antonino Famulari, Thorsten Strufe: A survey on decentralized Online Social Networks, 2014

[31]: Luca Maria Aiello, Giancarlo Ruffo, And Lotusnet: tunable privacy for distributed online social network services, Comput. Commun. 35 (1) (2012) 75–88

[32]: Luca Maria Aiello, Marco Milanesio, Giancarlo Ruffo, Rossano Schifanella, Tempering Kademlia with a robust identity based system, in: IEEE P2P, 2008

[33]:S. Buchegger, D. Schioberg, L. Vu, A. Datta, Peerson: P2p social networking – early experiences and insights, SNS, 2009

[34]: A. Cutillo, R. Molva, T. Strufe, Safebook: a privacy preserving online social network leveraging on real-life trust, IEEE Commun. Mag. (2009).

[35]: K. Graffi, S. Podrajanski, P. Mukherjee, A. Kovacevic, R. Sreinmetz, A distributed platform for multimedia communities, in: Tenth IEEE International Symposium on Multimedia, 2008.

[36]: Antony Rowstron, Peter Druschel, and Pastry: scalable, decentralized object location, and routing for large-scale peer-to-peer systems, Middleware, 2001.

[37]: Peter Druschel, Antony Rowstron, Past: a large-scale, persistent peer-to-peer storage utility, in: Hot Topics in Operating Systems, 2001

[38]: Sonia Jahid, Shirin Nilizadeh, Prateek Mittal, Nikita Borisov, Apu Kapadia, Decent: a decentralized architecture for enforcing privacy in online social networks, SESOC (PERCOM Workshops), 2012, pp.326–332

[39]: Sonia Jahid, P Mittal, Nikita Borisov, EASiER: encryption-based access control in social networks with efficient revocation, in: ASIACCS, 2011

[40]:source :https://bitcoin.fr/que-contient-un-bloc-de-transaction/(consulté le 13-10-2018).

[41]: source : https://anders.com/blockchain/tokens.html(consulté le 13-10-2018).

[42]: GODEBARGE FERREOL,ROSSAT ROMAIN: Principes clés d'une application blockchain : PROJET DE FIN D'ETUDES . EM Lyon Business School. 15/12/2016

[43] :Bitcoin.it. (2010). *Preuve de travail*. Récupéré sur Bitcoin.it: https://fr.bitcoin.it/wiki/Preuve_de_travail .

[44] : source :https://fr.express.live/2018/06/15/blockchain-les-avantages-et-les-inconvenients-de-cette-technologie(consulté le 13-10-2018).

[45] : source : https://www.blockchaindailynews.com/La-blockchain-opportunites-avantages-et-limites_a25673.html(consulté le 13-10-2018).

[46]:source : https://www.7x7.press/7-applications-possibles-de-la-technologie-blockchain(consulté le 13-10-2018).

[47] : source : https://www.blockchains-expert.com/steemit-reseau-social(consulté le 13-10-2018).

[48] : https://www.cnetfrance.fr/news/scandale-facebook-ce-qu-il-faut-savoir-pour-comprendre-l-affaire-et-proteger-ses-donnees-39865776.htm(consulté le 09 /09/2018).

[49] : https://www.latribune.fr/technos-medias/cambridge-analytica-le-scandale-de-trop-pour-facebook-774873.html(consulté le 09/09/2018).

[50]: http://parisinnovationreview.com/article/connectes-mais-proteges-le-pari-des-reseaux-sociaux-decentralises.html (consulté le 09/09/2018).

[51]: Stephan Schulz, Thorsten Strufe, d2 deleting diaspora: practicalattacks for profile discovery and deletion, in: ICC, 2013, pp. 2042–2