# ***Proposition de Sujet de Thèse CIFRE***

**Titre :** Réseau Social Anonyme de Confiance Dédié aux Applications Communautaires du Futur : Une Approche Guidée par le Capital Social

**Entreprises :** Laboratoire LIAS et l'entreprise SafeThing

**Responsables :**
**LIAS :** A. HADJALI (allel.hadjali@ensma.fr), S. JEAN (stephane.jean@ensma.fr) et M. BARON (mickael.baron@ensma.fr).

**SafeThing :** Mounir BECHCHI, m.bechchi@clipo.fr, Dominique CHABOT, d.chabot@clipo.fr

**Mots clés :** Réseaux Sociaux, Anonymat, Mesure de confiance, Proximité sociale, Humain-Blochchain

## Contexte et problématique

Avec la prolifération des technologies web, de nombreux réseaux sociaux sont de plus en plus présents sur Internet. La majorité de ces réseaux n'offrent pas de réelles garanties sur le respect de la vie privée des utilisateurs (c'est-à-dire, ils collectent des données d'identités des consommateurs). Ce travail de thèse s'inscrit dans le cadre de la famille des réseaux dits « *anonymes* » où l'anonymat des utilisateurs est complétement respecté (non collecte des informations liées à leurs identités : nom, prénom, numéro de téléphone, e-mail, etc.). Mais comment instaurer la *confiance* au sein d'un tel réseau anonyme pour favoriser l'entraide, l'échange et le partage ? Et comment en prévenir son utilisation à des fins malhonnêtes ?

Un exemple de systèmes de cette famille est décrit dans les travaux [1,2,3] où l'utilisateur échange de façon anonyme mais il est identifié auprès d'un tiers de confiance. En cas de comportement malhonnête, des procédures permettent de faire « marche arrière » c'est-à-dire de lever l'anonymat. Ceci est généralement confié au tiers de confiance ou à une autorité compétente, qui est la seule à détenir ce pouvoir de révocation d'anonymat. Un autre exemple de systèmes de cette famille est le système dit « Blockchains » utilisé par exemple pour les transactions de la monnaie Bitcoin. Il utilise des mécanismes robustes pour empêcher la fraude et compenser l'absence d'identité légale, comme, la Proof of Work [4] et la Proof of Stake [5].

L'entreprise SafeThing mise sur l'implication de l'utilisateur et de sa composante sociale dans le processus de la construction de confiance, une nouvelle thématique de recherche au croisement des sciences de l'informatique et des sciences humaines et sociales que SafeThing explore pour imaginer le réseau social de demain dédié aux applications

communautaires du futur. Une première application communautaire développée par SafeThing est un système de type « perdu/trouvé » qui aide les utilisateurs (inscrits) à trouver leurs objets perdus grâce aux *SafeCodes* et sans jamais dévoiler leurs identités pour ce système. Ce système peut également être utilisé dans le contexte d'un échange, d'un partage ou plus généralement d'une transaction entre utilisateurs anonymes. SafeThing ambition que ce système soit le numéro 1 dans la communauté d'applications futures des biens et des services.

Dans ce type de réseau social, pour favoriser l'entraide, l'échange et le partage entre les différents membres/groupes en toute confiance et en respectant la vie privée de chacun, il est essentiel d'instaurer un modèle confiance au sein du réseau social. La construction de ce modèle passe par l'implication des utilisateurs et de leurs composantes sociales/proximité sociale (famille, amis, voisins, associations, etc.). La proximité sociale aura donc un impact fort sur le comportement de l'utilisateur. De cette proximité sociale dérive la notion de responsabilité (ou capital social) et celle-ci peut être engagée dans le cadre d'une transaction anonyme : *human-blockchain*.

Dans la vision de safeThing le concept de la human-blockchain doit favoriser l'entraide, l'échange et le partage entre ses utilisateurs (la communauté Safe) en toute confiance et en respectant la vie privée de chacun, pour ce, SafeThing mise sur la construction d'une communauté de confiance constituée de plusieurs sous réseaux de confiance responsables dont l'existence est bien réelle et basée sur la proximité et la rencontre physique (famille, amis, voisins, collègues, etc.). En effet, l'utilisateur souvent échange avec son voisinage social dont il partage les mêmes idées, les même règles et principes, les mêmes centres d'intérêt. Il préfère généralement obtenir un service d'un contact direct ou *recommandé par son voisinage* plutôt qu'à partir d'une source inconnue ou éloignée. Ces relations sociales de proximité entre les acteurs constituent une source d'évidence pour *mesurer la confiance.*

La human-blockchain SafeThing doit également disposer des mécanismes appropriés pour détecter et punir les diverses formes d'abus : utilisation du système à des fins malhonnêtes lors d'un échange, d'un partage ou plus généralement d'une transaction entre utilisateurs anonymes. La confiance comme décrite ici, n'est pas une marchandise que l'on peut acheter, elle ne se décrète pas, mais elle se construit dans la durée et se perd plus rapidement qu'elle se gagne. Il en résulte une communauté saine dont le devise est la collaboration désirable et la fraude indésirable.

**Verrous scientifiques :**

Dans le cadre de ce travail de thèse, les principaux verrous scientifiques à lever sont présentés ci-dessous.

- Après une définition (non ambiguë) du concept « capital social », proposer un modèle de confiance fondé sur ce concept. Il s'agit d'un modèle de confiance qui permet de spécifier et de représenter les relations sous une forme calculable ou prouvable. Cette

formalisation doit aussi indiquer quels sont les paramètres qui seront pris en compte pour évaluer la confiance.

- Enrichir ce modèle avec une algèbre rationnelle pour la gestion et la manipulation de la confiance dans un réseau social anonyme.
- Définir et intégrer un modèle de risque de prise de décision. Il s'agit d'un risque en rapport direct avec la sécurité. Dans le cas où la sécurité est assurée, il n'y a donc pas de risque et la question de la confiance ne devrait pas se poser. Par contre, quand il existe un risque, on se trouve dans un contexte incertain et la question sur la confiance se pose. Dans cette situation, on a besoin d'un mécanisme d'aide à la décision pour évaluer les conséquences possibles de l'action à entreprendre et leurs différentes probabilités d'occurrence.
- Concevoir et développer un langage dédié d'interrogation du réseau pour, par exemple 1/ chercher les utilisateurs dont le comportement pourrait être suspect, ou identifier des groupes/blocs d'utilisateurs selon un critère donné et 2/ extraire les risques éventuels depuis le modèle de risque de prise de décision.

**Bibliographie**


[1]. Signatures pour l'anonymat fondées sur les couplages et applications, 2007, Emeline Hufschmitt, Université de Caen, France.

[2]. Outils cryptographiques pour la protection des contenus et de la vie privée des utilisateurs, 2011, Amandine Jambert, Université de Bordeaux, France.

[3]. Design of privacy preserving cryptographic protocols for mobile contactless services, 2015, Ghada Arfaou,. University of Orléans, France.

[4]. Double spending fast payments in bitcoin, 2012, Karame & Androulaki, & Capkun, ACM Conference on Computer and communications security.

[5]. Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies, 2017, Maria Borge & Eleftherios Kokoris-Kogias & Philipp Jovanovic & Linus Gasser & Nicolas Gailly & Bryan Ford, in 1st IEEE Security and PrivacyOn The Blockchain.

[6]. Sonja Grabner-Kräuter & Sofie Bitter (2015) Trust in online social networks: A multifaceted perspective, Forum for Social Economics, 44:1, 48-68.

[7]. T. Grandison and M. Sloman, "Trust Management Tools for Internet Applications," Springer, Berlin, Heidelberg, 2003, pp. 91–107.

[8]. J.-H. Cho, K. Chan, and S. Adali, "A Survey on Trust Modeling," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 1–40, 2015.

[9]. [14] O. Richters and T. P. Peixoto, "Trust transitivity in social networks," *PLoS One*, vol. 6, no. 4, 2011.

[10]. Marc Jacquemain, Le Capital social : Une introduction, 2005, De Boeck Supérieur.

[11]. John Field, Social Capital, London and new York, Routtledge.