

## DIPLÔME NATIONAL DE DOCTORAT

(Arrêté du 25 mai 2016)

Date de la soutenance : **12 décembre 2023**

Nom de famille et prénom de l'auteur : **Monsieur RAMOS TUBINO Rafael**

Titre de la thèse : « *Une étude des utilisateurs, des flux réels et de l'activité temporelle dans l'écosystème bitcoin* »

### Résumé



Le bitcoin est la plus ancienne crypto-monnaie et l'une des plus actives. Toutes ses données de transaction sont stockées dans un registre décentralisé – la blockchain Bitcoin – librement accessible à toute personne désireuse de l'analyser. L'analyse du contenu de ces données est l'objet de cette thèse. Le manuscrit se concentre sur deux questions de recherche principales : l'identification des utilisateurs de Bitcoin, et la caractérisation de l'activité de ces utilisateurs. Dans la première partie, nous proposons une méthode pour améliorer la construction d'agrégats d'adresses Bitcoin appartenant à un même utilisateur, en identifiant la sortie de changement d'une transaction à l'aide de l'apprentissage automatique supervisé.

La qualité du résultat est évaluée à l'aide d'une vérité de terrain basée sur des données on-chain et off-chain. Nous montrons que les résultats sont plus performants que les travaux précédents, mais aussi que l'identification des modifications apportées par un seul utilisateur pourrait être une meilleure stratégie que l'objectif habituel consistant à considérer l'ensemble de la blockchain comme un seul problème.

La deuxième partie du travail se concentre sur l'interprétation de l'activité des utilisateurs dans la blockchain Bitcoin. Nous visons définir l'activité économique réelle présente dans la blockchain Bitcoin, par opposition aux transactions artificielles induites par le protocole ou par des utilisateurs déplaçant de l'argent d'une adresse à l'autre pour des raisons techniques. Une heuristique est proposée pour classer les utilisateurs en trois catégories : Les récepteurs fréquents (FR), les voisins des FR et les autres. Les travaux montrent que les FR (qui sont une approximation des entités commerciales) représentent une petite fraction des entités, mais concentrent la plupart des paiements, ce qui témoigne d'une centralisation dans l'écosystème du bitcoin. Une étude temporelle est également menée, nous permettant d'estimer la localisation géographique des utilisateurs. Nous utilisons notamment ces informations pour quantifier le biais d'un ensemble de données couramment utilisé dans la littérature pour le marquage des entités.