Gestion d'identité distribuée

Advisers
Emmanuelle Anceaume, emmanuelle.anceaume@irisa.fr
Romaric Ludinard, romaric.ludinard@irisa.fr

Keywords gestion identité distribuée, registre distribué non permissionné et permissonné

Context L'identité distribuée (*self-sovereign identity*) est le concept selon lequel les utilisateurs devraient pouvoir contrôler leur propre identité numérique. Les personnes et les entreprises peuvent stocker leurs propres données d'identité sur leurs propres appareils et fournir leur identité à ceux qui doivent la valider, sans avoir à s'appuyer sur un dépôt central de données d'identité, ou sur des institutions de confiance. Il donne à l'utilisateur un contrôle total, une sécurité et une portabilité totale de ses données.

L'émergence des registres distribués (*blockchain*) semble être le cadre idéal pour le développement de plateformes de gestion d'identités numériques offrant aux utilisateurs le contrôle complet de leur identité, tout en simplifiant la gestion des identités du point de vue des fournisseurs de services. La quasi totalité des reflexions en cours se concentre sur des registres distribués permissionnées, c'est-à-dire controlés par un consortium d'institutions de confiance, en général bancaires (par exemple le consortium R3 [2]).

L'objectif de ce stage est d'étudier l'adéquation des registres non permissionnés (c'est-à-dire ouvert en écriture et lecture à tous et dont le représentant est Bitcoin) pour développer des plateformes de gestion d'identités pour lesquelles l'utilisateur aurait réellement le contrôle complet de son identité [1].

Cette étude sera décomposée en deux parties. La première partie consistera à étudier les propositions actuelles dans les contextes permissionnés et non permissionnés en exhibant pour chacune d'elles les hypothèses nécessaires à la construction de ces plateformes et les garanties offertes aux utilisateurs. A l'issue de cette étude, l'étudiant proposera une solution permettant d'offrir à l'utilisateur un contrôle le plus complet possible de son identité sans recourir à des autorités de confiance.

Pré-requis Connaissances en algorithmique distribuée, et fort intérêt pour la protection de la vie privée et des données personnelles.

References

[1] D. Augot, H. Chabanne, and W. George. Practical solutions to save bitcoins applied to an identity system proposal. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (CISSP)*, 2019.

[2] A. Mühle, A. Grüner, T.Gayvoronskaya, and C. Meinel. A survey on essential components of a self-sovereign identity. https://arxiv.org/pdf/1807.06346.pdf, 2018.