# Blockchain publique pour la gestion d'identités auto-souveraines

L'identité est un des éléments fondateurs de la confiance. La gestion des identités numériques s'avère complexe et elle est généralement gérée de manière plus ou moins centralisée : les identités sont stockées sur des serveurs dédiés comme Active Directory sur lesquels les utilisateurs vont s'authentifier avant d'avoir accès à différentes ressources ou services. Cette approche s'est depuis légèrement décentralisée en passant à des systèmes fédérés (e.g., Microsoft Passeport) ou centrés sur l'utilisateur (e.g., OpenID, OAuth, FIDO...). néanmoins, la gestion des identités restent sous le contrôle d'entités tierces et peuvent être sujettes à des défaillances ou pourraient permettre la censure concernant l'utilisation de ces identités. Enfin, ces approches sont peu respectueuses de la vie privée dans le sens où les portails fournisseurs d'identités ont accès à l'intégralité de l'activité des utilisateurs.

Le concept d'identité auto-souveraine [1] (SSI) est une approche de l'identité numérique qui donne aux individus le contrôle de leur identité numérique. Cette approche permet aux utilisateurs de gérer leur identité sans avoir recours à des acteurs tiers pour stocker et gérer leur identité. La mise en œuvre de ce concept doit satisfaire [2] et est loin d'être simple, l'identité étant bien plus qu'un simple identifiant, mais peut, par exemple être représentée par des preuves d'interaction entre un utilisateur et un service. Dans ce cas, il faut donc implémenter des preuves de ces interactions qui soient à la fois vérifiable et intègres. Ce type de besoin, couplé à un aspect temporel (l'utilisateur a interagi avec tel service, puis plus tard avec tel autre, de manière auditable) fait rapidement penser au recours à une structure de type blockchain pour implémenter des identités auto-souveraines.

Des solutions basées sur des technologies blockchain (e.g., Hyperledger Indy[1], Sovrin[2]) pour implémenter les mécanismes SSI. Le framework européen eiDAS [3] fait également des propositions en ce sens. Ces approches restent néanmoins centralisées et permissionnées.

**Le projet BC4SSI cherche à étudier la faisabilité d'identités auto-souveraines dans le contexte d'une infrastructure ouverte et publique et permettant un usage au quotidien**. Le projet BC4SSI se focalise sur quatre verrous scientifiques [4] liés aux blockchains publiques qui sont aujourd'hui un frein majeur au déploiement de ce type de solution: (*i*) Alternatives à la preuve de travail, (*ii*) Réplication parcimonieuse, (*iii*) Débit adaptatif, et (*iv*) Consommation énergétique.

Afin de pallier ces limitations, le projet BC4SSI s'intéressera à des structures de données alternatives, telles que les graphes orientés acycliques [5] afin d'adresser les problématiques de débit, ainsi que des mécanismes de preuves alternatives [6] permettant une représentation parcimonieuse de l'état du système, réduisant ainsi drastiquement l'empreinte mémoire de ces structures de données. Enfin, ces mécanismes devront s'appuyer sur des alternatives à la preuve de travail [7] sans contrainte supplémentaire de synchronie (contrairement à la preuve d'enjeu [8]) afin, d'une part de limiter la consommation énergétique du système, et d'autre part éviter d'imposer aux participants d'être connectés en permanence. De cette manière, la faible empreinte en mémoire, en communications, et énergétique permettra le déploiement d'une telle solution sur des équipements du quotidien tels que les smartphones.

## References

[1] Mühle, A., Grüner, A., Gayvoronskaya, T. and Meinel, C. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review* 30.
[2] Allen, C. 2016. The Path to Self-Sovereign Identity.
[3] European Union Blockchain Observatory & Forum. 2019. Blockchain And Digital Identity.
[4] Direction générale des Entreprises. 2021. Les verrous technologiques des blockchains.
[5] **Anceaume, E.**, Guellier, A., **Ludinard, R.** and Sericola, B. 2018. Sycomore : a Permissionless Distributed Ledger that self-adapts to Transactions Demand. In: *17th IEEE International Symposium on Network Computing and Applications*. NCA.
[6] Kiayias, A., Leonardos, N. and Zindros, D. 2021. Mining in Logarithmic Space. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS.
[7] Back, A. 2002. Hashcash - A Denial of Service Counter-Measure.
[8] Kiayias, A., Russell, A., David, B. and Oliynykov, R. 2017. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In: *Advances in Cryptology*. CRYPTO.

[1] https://www.hyperledger.org/use/hyperledger-indy
[2] https://sovrin.org/