Chaîne de blocs pour la tenue de registres : une bonne idée ?

Certains cantons et communes expérimentent déjà la technologie de la chaîne de blocs. Est-ce judicieux de l'utiliser pour tenir des registres de personnes ? *Andreas Spichiger*

Abrégé Par sa disponibilité et son intégrité, la technologie de la chaîne de blocs semble idéale pour la tenue de registres, par exemple de personnes. Un examen plus attentif révèle cependant que la confidentialité et la possibilité d'intervenir, tout aussi importantes, ne sont pas garanties. Des moyens et mesures supplémentaires sont donc nécessaires afin de respecter pleinement la sécurité de l'information et la sphère privée. Il faut également s'adjoindre les services d'organisations de confiance. La technologie de la chaîne de blocs ne convient donc que de manière limitée à la tenue de registres.

Registres des habitants, du commerce ou foncier : la tenue de registres est l'une des tâches centrales de l'État. Après des siècles de recueils sur support papier, la numérisation ouvre de nouvelles voies. En 2006, la Suisse a ainsi, pour des raisons statistiques, imposé le format électronique pour les registres des habitants tenus par les communes[1].

Depuis près de dix ans, la technologie de la chaîne de blocs (ou « blockchain ») permet le stockage décentralisé des données de transactions. L'intégrité garantie des informations semble la prédestiner pour la tenue de registres. Nous examinerons ici la question de savoir dans quelle mesure la technologie blockchain actuelle convient pour un registre de personnes.

Les processus pertinents pour tenir un tel registre sont l'identification, l'enregistrement, la révocation et l'authentification. L'identification est la procédure qui permet de constater de façon univoque l'identité des personnes. À ce stade, le registre n'est guère utile, car l'attribution des caractéristiques personnelles identifiantes doit être assurée d'une autre manière. Il est important de recueillir assez d'informations identifiantes sur une personne et que celles-ci se distinguent suffisamment des anciennes et – si possible – de toutes les futures entrées. Une réidentification ultérieure devra établir avec certitude qu'il s'agit de la même personne.

Lors de l'enregistrement, les données identifiantes sont inscrites au registre. Normalement, un certificat simplifiant beaucoup l'identification au quotidien est délivré au terme de l'enregistrement. Ce certificat est également enregistré. Les registres publics pourraient être tenus dans une chaîne de blocs publique afin de permettre aux citoyens de contribuer au consensus.

La révocation sert au retrait du certificat et concerne uniquement le registre des certificats, mais pas les données du registre. L'authentification permet de confirmer qu'il s'agit de la personne concernée. Cette opération s'effectue en général sans recourir au registre, au seul moyen du certificat. L'élément le plus critique dans ces processus est la (ré)identification, qui doit être confiée à des personnes de confiance qualifiées, typiquement une administration.

Expériences à Zoug et à Genève

Bien que la technologie blockchain soit récente, plusieurs administrations y font déjà leurs premiers pas avec l'aide d'entreprises technologiques. La ville de Zoug propose ainsi une « identité numérique » qui n'est pas stockée sur un serveur municipal, mais sur le smartphone de la personne. La ville procède uniquement à l'identification de la personne concernée et la chaîne de blocs garantit l'intégrité des données sur le smartphone. Le canton de Zoug s'essaie lui aussi à cette nouvelle technologie : son registre du commerce a, avec des partenaires, fait la démonstration d'un procédé entièrement basé sur la chaîne de blocs pour créer une société anonyme, jusqu'à l'inscription au registre du

1 Assemblée fédérale (2015).

commerce. Si la tenue du registre continue de s'effectuer au moyen de la solution existante, la création avec participation de plusieurs parties est supportée par des « contrats intelligents » (« smart contracts ») dans la chaîne de blocs. Les paramètres de ces protocoles sont inscrits dans une chaîne de blocs et s'y exécutent automatiquement lorsque les conditions sont réunies. Personne ne peut contrôler leur exécution, ce qui les rend sûrs pour toutes les parties impliquées.

Dans le canton de Genève, la technologie des chaînes de blocs permet de commander un extrait de registre. Elle garantit en même temps l'authenticité et l'origine du document.

Dans tous ces exemples, aucune donnée des registres n'est enregistrée dans les chaînes de blocs. Leur technologie sert en première ligne à simplifier un processus distribué ou à valider des certificats.

Sécurité de l'information et sphère privée

La sécurité de l'information est une dimension importante des registres[2] : elle concerne la disponibilité (soit la possibilité d'accéder rapidement à l'information), l'intégrité (c'est-à-dire la représentation correcte des données fournies), et enfin la confidentialité (soit la protection contre tout accès illicite).

Tandis que les chaînes de blocs offrent un soutien solide pour la disponibilité et l'intégrité, elles ne peuvent pas garantir la confidentialité à long terme. Comme les données stockées dans des chaînes de blocs y restent indéfiniment mais que leur protection cryptographique est limitée dans le temps, seules des informations non critiques devraient être stockées dans les chaînes de blocs. Dans la pratique, les chaînes de blocs sont donc utilisées pour assurer non pas la dis-

KEYSTONE

La technologie de la chaîne de blocs peut s'avérer utile pour confirmer l'authenticité de certaines données. Les archives du registre du commerce à Zoug.

ponibilité des données elles-mêmes, mais uniquement leur intégrité. Les différents exemples mentionnés plus haut en sont la preuve.

Parler de sphère privée implique des données se rapportant à des personnes. Ces références ne peuvent être totalement exclues même dans les registres d'objets, étant donné que des personnes sont impliquées dans l'identification ou que les objets permettent de tirer des conclusions sur des personnes. La propriété des données est secondaire en matière de sphère privée[3].

Alors que la transparence peut être assurée par les chaînes de blocs et que l'absence de connectabilité doit de toute façon être résolue à l'aide du contexte, la possibilité d'intervenir (en lien avec l'inaltérabilité des données) doit être réalisée séparément.

La tenue de registres, un défi à long terme

Comme ils sont utilisés longtemps, il est normal que les registres subissent des modifications. Pour anticiper la probable évolution technologique, la technologie choisie doit permettre un changement de système. En d'autres termes : la sécurité de l'information et la sphère privée doivent toujours être garanties en cas de changement au niveau technique, sémantique, organisationnel ou juridique.

Le processus peut aussi être sujet à des erreurs de contenu en rapport avec la (ré)identification et l'enregistrement. Le contexte est en fin de compte déterminant même pour un contrat intelligent : le contexte de la chaîne de blocs doit garantir une exactitude suffisante des données d'entrée par des réglementations techniques, sémantiques, organisationnelles et juridiques. Par le passé, il s'est donc avéré utile qu'un registre puisse être modifié. Un droit à l'oubli doit également pouvoir s'appliquer aux inscriptions aux registres. La correction de ces inscriptions doit ainsi être traitée comme un changement de contexte pertinent.

Prendre les inconvénients au sérieux

Quelle est la quintessence de ces explications ? La sécurité de l'information et la sphère privée sont des défis majeurs dans la tenue de registres. Vouloir utiliser des chaînes de blocs pour le stockage des données dans la tenue de ces registres se révèle toutefois irréaliste. Au lieu de cela, leur technologie peut aider à simplifier des processus et à valider l'intégrité des données des registres.

Pour garantir la confidentialité et la possibilité d'intervenir, il est nécessaire, du point de vue actuel, de trouver d'autres solutions pour le stockage des données proprement dit. La technologie des chaînes de blocs peut cependant servir à titre complémentaire, pour assurer l'intégrité et, selon le contexte, la transparence. Reste à savoir s'il ne serait pas plus facile d'y parvenir en utilisant d'autres technologies.

Andreas Spichiger
Directeur de l'Institut de cyberadministration, Haute école spécialisée bernoise (BFH), Berne

2 Hansen et al. (2015) ; voir aussi Spichiger et al. (2019).

3 Depuis 2018, le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD) règle la sphère privée à l'échelle européenne.

Bibliographie

Assemblée fédérale de la Confédération suisse (2015). *Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes* (Loi sur l'harmonisation de registres, LHR). Suisse, pp. 1–10.

Hansen M., Jensen M. et Rost M. (2015). « Protection goals for privacy engineering », *2015 IEEE Security and Privacy Workshops*, pp. 159–166.

Spichiger A., Rötzer H. et Neuroni A. (2019). « Hoheitliches Handeln und Registerführung », in : *Handbuch E-Government – Technikinduzierte Verwaltungsentwicklung*, R. Springer, J. Stember, W. Eixelsberger, A. Spichiger, A. Neuroni, F.-R. Habbel, et M. Wundara, éd. Wiesbaden : Springer Fachmedien Wiesbaden.