_swissprivacy.law

E-ID : quelles implications pour l'État en cas de recours à la blockchain ?

Ludivine Epiney, le 6 février 2024

Près de 15 ans après l'avènement de la blockchain – qui a ouvert la voie à de nombreux espoirs et spéculations –, cette technologie peut offrir le moyen de concrétiser le nouveau projet d'identité électronique (e-ID). Cette contribution vise à présenter les raisons qui mènent à envisager cette technologie, mais aussi ses implications pour l'État, sur la base d'une expérimentation menée dans le Canton de Vaud.

I. Introduction

Au-delà des initiatives développées dans le secteur privé, la blockchain[1] a également suscité une vague d'intérêt dans l'administration publique, qui y voit l'opportunité de développer sa relation numérique avec la population grâce à des services innovants, transparents et sécurisés. Cet engouement s'est concrétisé dans plusieurs projets sur sol helvétique, comme pour le registre du commerce à Genève ou pour la création d'une identité numérique pour la Ville de Zoug.

Dans le Canton de Vaud aussi, cette technologie a éveillé une attention particulière, à l'image du postulat déposé en 2017 par M. Vassilis Venizelos et consorts demandant d'étudier les possibilités d'utilisation de la blockchain au sein de l'administration cantonale vaudoise. Si la blockchain est ainsi fréquemment abordée du point de vue de ses avantages, le Conseil d'État vaudois a rappelé dans sa réponse au postulat que toute technologie comporte des aspects ambivalents et doit ainsi faire l'objet d'une pesée d'intérêts.

Alors que la technologie blockchain pourrait être utilisée pour concrétiser le nouveau projet de loi sur l'e-ID – dont le message a été adopté par le Conseil fédéral le 22 novembre 2023 –, cette contribution propose des pistes de réflexion sur les implications du recours à cette technologie pour l'administration publique. Il s'agira dans un premier temps d'exposer les raisons qui mènent à plébisciter une solution décentralisée comme la blockchain, puis, sur la base d'un travail mené au sein du Canton de Vaud, d'interroger les implications de la mise en œuvre effective d'une telle solution et ce qu'il est réellement possible d'espérer.

II. Une identité électronique souveraine et de confiance pour la Suisse

Offrir la possibilité à la population d'obtenir une identité électronique reconnue par l'État – qui puisse permettre de s'identifier formellement en ligne et ainsi encourager la confiance numérique – apparaît comme une nécessité dans une société toujours plus marquée par les interactions en ligne. C'est ce qui explique qu'après le rejet en votation populaire de la Loi fédérale sur les services d'identification électronique (LSIE) le 7 mars 2021, des représentants et des représentantes des principaux partis politiques suisses ont déposé six motions de même teneur au Conseil national pour demander de travailler sur une nouvelle proposition de loi. Celle-ci doit tenir compte de certaines exigences fondamentales qui répondent aux préoccupations exprimées par la population lors du rejet de la LSIE.

Contrairement au projet initial, qui prévoyait de tirer profit de l'infrastructure déjà existante déployée par des acteurs privés, l'État devra avoir la charge de l'émission et de la gestion du nouveau système. Cette condition ne suffit toutefois pas à garantir la confiance de la population, qui souhaite également que l'e-ID ne soit pas un moyen supplémentaire de tracer leurs activités en ligne. Ainsi, la nouvelle solution devra également prendre en compte la protection de la vie privée dès la conception (*privacy by design*) et minimiser la collecte et l'utilisation de données personnelles. En sus, les motions requièrent que les données soient enregistrées de manière décentralisée, par exemple auprès de l'utilisateur ou de l'utilisatrice en ce qui concerne les données d'identification.

Pour répondre à ces demandes, le Département fédéral de justice et police (DFJP), en charge du dossier, a élaboré un document de travail mis en consultation publique à l'automne 2021. En s'appuyant sur les retours de plusieurs cantons, entreprises et associations, la Confédération a donné son accord de principe pour expérimenter le modèle d'identité auto-souveraine, une approche qui vise à accorder à l'individu une meilleure maîtrise de ses données. Ce dernier pourra gérer, autoriser et partager ses informations personnelles, ce qui renforce son contrôle et son autonomie sur l'utilisation de ses données. Concrètement, lors de l'émission d'une telle e-ID, la Confédération contrôle et confirme l'identité d'une personne physique, puis lui délivre son e-ID. À partir de là, l'utilisateur ou l'utilisatrice détient son e-ID et peut en disposer à sa guise, sans que la Confédération ne sache quand ni pourquoi l'identité est utilisée, de la même manière qu'avec sa carte d'identité physique, ce qui répond aux exigences de protection de la vie privée. L'identité auto-souveraine se distingue ainsi des modèles traditionnels basés sur des registres centralisés et requiert d'expérimenter de nouvelles formes d'architecture.

III. Recours à la blockchain pour concrétiser l'identité auto-souveraine

Dans le cadre des travaux préparatoires sur l'e-ID, le Canton de Vaud a mené une expérimentation sur le concept d'identité auto-souveraine, soutenu par un financement de l'Administration numérique suisse (ANS). Techniquement, il a opté pour une solution basée sur une blockchain, qui permet de garantir qu'une e-ID est bien valide sans pour autant interroger les registres de la Confédération, ce qui laisserait une trace numérique. La blockchain va donc jouer le rôle d'intermédiaire entre l'État et l'individu. D'un côté, l'État va y inscrire la preuve de l'émission d'une e-ID. De l'autre côté, le titulaire de l'e-ID se servira à sa guise de cette preuve – dont l'intégrité est assurée par les mécanismes de la blockchain. Si ce système répond en théorie aux exigences de protection de la sphère privée souhaitée à travers le nouveau projet d'e-ID, l'expérimentation pratique permet d'identifier certaines limites d'une identité auto-souveraine.

A. Enjeux démocratiques et juridiques liés à la blockchain

Dans un monde numérique qui s'est construit sur des relations d'interdépendance et de perte d'autonomie au profit de grands acteurs privés étrangers, la blockchain constitue une alternative en proposant une gouvernance distribuée au sein de son réseau. Avec l'idée que chaque nœud va participer à la pérennité de la blockchain et que toute information est transparente, cette technologie est souvent perçue comme neutre et équitable. Dans les faits pourtant, les blockchains dites publiques – que tout le monde peut rejoindre comme Bitcoin ou Ethereum – tendent vers une gouvernance technocratique. Certains utilisateurs et certaines utilisatrices s'investissent davantage dans la blockchain, ce qui leur permet d'obtenir un suffrage plus important dans la prise de décisions. Or, cette caractéristique va à l'encontre de la forme de légitimité de nos sociétés démocratiques, selon laquelle ce sont les citoyens et les citoyennes, directement ou par l'intermédiaire des personnes qu'ils et elles élisent, qui sont à l'origine des décisions collectives – indépendamment de leurs ressources.

Par ailleurs, le recours à la blockchain interroge le régime juridique relatif à la protection des données personnelles. En effet, les données enregistrées dans une blockchain sont réputées immuables. Néanmoins, cette caractéristique se heurte au principe d'exactitude ainsi qu'au droit à l'effacement ou droit à l'oubli car, si les données contenues hors de la blockchain peuvent effectivement être effacées, il demeurera une trace de celles-ci sur la blockchain. Avec l'évolution rapide des technologies, on ne peut pas exclure la possibilité de déchiffrer ces traces à l'avenir, ce qui soulève des questions en termes d'application de la loi sur la protection des données. En somme, le recours à la blockchain par l'État doit s'accompagner d'une réflexion quant au degré de contrôle démocratique et juridique qu'il parviendra à exercer sur l'application utilisée ainsi que sur le type de blockchain à utiliser.

Pour ces raisons, les administrations publiques optent généralement pour des variantes de blockchain dites privées – détenues par des acteurs définis (entreprises, institutions, collectivités) – ce qui permet d'instaurer certaines règles, relatives à un régime juridique particulier par exemple ou dans le but de déterminer qui peut rejoindre le réseau.. C'est le choix par exemple de l'Estonie qui, depuis 2012, déploie la blockchain privée KSI de l'entreprise Guardtime dans plusieurs de ses systèmes en production, comme le registre foncier et de propriété, le registre des entreprises ou encore le registre des successions. Cette option permet de conserver une certaine maîtrise sur l'évolution de la blockchain tout en rendant possible une solution décentralisée dans laquelle les données sont immuables. Pour autant, elle réintroduit une relation partenariale avec un ou plusieurs acteurs privés – avec de possibles conséquences sur la confiance des utilisateurs et sur la perte d'autonomie de l'Etat vis-à-vis de sa solution. En outre, elle n'offre aucune amélioration aux utilisateurs et utilisatrices en termes de protection des données personnelles.

Plusieurs expérimentations, dont celle du Canton de Vaud, envisageaient le déploiement de l'e-ID sur Hyperledger Indy, une blockchain basée sur une communauté. Cependant, un manque de maturité et un certain désintérêt pour la blockchain – qui pourrait mettre en péril la stabilité de la communauté – ont été invoqués par la Confédération pour écarter cette solution.

B. Enjeux de sécurité et de protection de la vie privée liés à l'e-ID

L'identité auto-souveraine répond certes à l'exigence de protection de la vie privée souhaitée dans le nouveau projet de loi sur l'e-ID, mais elle entrave dans le même temps la mission de l'État qui consiste à protéger la population. Alors que dans le cas d'une solution centralisée, l'État endosse un rôle actif dans le suivi de la preuve électronique et peut intervenir plus rapidement en cas d'activité anormale, une identité auto-souveraine impliquerait que la personne détentrice de l'identité en ait une parfaite maîtrise, tant dans sa conservation que dans son utilisation.

Dans les faits, plusieurs scénarios illustrent les limites d'un tel modèle. Tout d'abord, en cas de perte de l'e-ID, à la suite par exemple d'une mauvaise manipulation ou de la perte de l'appareil sur lequel est détenue l'e-ID, aucune restauration de données ne pourrait être effectuée par l'État ou tout autre acteur. Il serait nécessaire de révoquer l'e-ID perdue et d'en demander une nouvelle, entraînant des conséquences administratives et financières. Pour y remédier, le projet de loi sur l'e-ID inclut à présent la possibilité que l'Office fédéral de l'informatique et de la télécommunication (OFIT) puisse mettre à disposition des titulaires

d'e-ID un système de copies de sécurité (art. 7 al. 2 projet LeID).

Par ailleurs, l'introduction d'une identité auto-souveraine soulève la question de la protection de la vie privée lors de l'utilisation de l'e-ID. Si le projet met l'accent sur la minimisation des données et plébiscite des mécanismes dans ce sens – par exemple de pouvoir indiquer que la personne est majeure sans fournir sa date de naissance complète –,ces efforts ne sont pas suffisants pour garantir la protection de la vie privée. Les acteurs dont le modèle d'affaires se base sur les données personnelles, à l'instar des réseaux sociaux, pourraient être tentés d'exiger une e-ID sans motif valable ou de demander plus que les éléments minimaux requis. Dans le but d'y remédier, le projet de loi sur l'e-ID prévoit à présent un article sur le devoir de diligence du vérificateur, qui réglemente la transmission des données personnelles contenues dans l'e-ID (art. 22 al. 1 projet LeID).

La concrétisation de l'identité auto-souveraine doit ainsi s'accompagner d'une réflexion sur les actions à mettre en place pour en limiter les risques pour la population. Il serait en effet illusoire de penser que tout individu sera en mesure non seulement de comprendre les enjeux de l'e-ID, mais également d'y répondre afin de maîtriser véritablement son identité numérique. L'État, en tant que garant de la cohésion sociale, devra accompagner l'introduction de l'e-ID afin de sensibiliser les utilisateurs et utilisatrices aux risques et déployer des services qui puissent répondre aux différents cas décrits ci-dessus. Cette nécessaire intervention de l'État pourrait relativiser la dimension de souveraineté des utilisateurs et utilisatrices vis-à-vis de leur e-ID.

IV. Conclusion

Théoriquement, le concept d'identité auto-souveraine représente une opportunité de développer une e-ID qui réponde aux attentes de la population en termes de protection de la vie privée et, plus globalement, de confiance numérique. Pour autant, les résultats de l'expérimentation du concept d'identité auto-souveraine par le Canton de Vaud en montrent les limites lorsqu'il s'agit de considérer ce modèle de manière plus globale. En effet, l'apparente autonomie d'une blockchain se heurte à la gouvernance d'un État de droit. Dans le cas où la blockchain demeure la technologie privilégiée pour développer l'e-ID, il apparaît nécessaire de restreindre le choix à une blockchain détenue par des acteurs reconnus – qu'il s'agisse d'entreprises, d'institutions, de collectivités – afin de conserver une certaine maîtrise sur l'évolution de la blockchain. Par ailleurs, la volonté exprimée d'offrir une plus grande liberté et autonomie des utilisateurs et utilisatrices s'accompagne d'une responsabilisation vis-à-vis de leur e-ID. L'État, en tant que garant de la cohésion sociale, devra assurer les

garde-fous nécessaires pour que les titulaires d'une e-ID puissent en tirer profit dans les meilleures conditions.

En somme, le cas présenté ici illustre parfaitement l'ambivalence autour de l'adoption d'une solution technologique, telle que soulevée par le Conseil d'État vaudois dans sa réponse au postulat de M. Vassilis Venizelos. Bien qu'un contexte particulier mène à considérer une solution technologique, il faut questionner cette dernière de manière globale et effectuer une pesée d'intérêt. Celle-ci doit comporter tant des aspects techniques, juridiques ou financiers que l'évaluation des transformations que ladite technologie peut avoir sur la société.

1. Par souci de simplicité, la notion de blockchain sera préférée dans cet article pour faire également référence aux technologies de registres distribués (DLT) au sens large.

Proposition de citation : Ludivine Epiney, E-ID : quelles implications pour l'État en cas de recours à la blockchain ?, 6 février 2024 *in* www.swissprivacy.law/281