canton de vaud
LIBERTÉ ET PATRIE

RAPPORT DU CONSEIL D'ETAT AU GRAND CONSEIL

sur le Postulat Vassilis Venizelos et consorts –

Blockchain : le web 3.0 peut changer les rapports entre l'administration et les administrés. (17_POS_017)

Rappel de l'intervention parlementaire

Texte déposé

Issue de la technologie qui a permis l'essor des bitcoins, la blockchain représente probablement les prémisses de la prochaine étape du développement du web. Construite sur une chaîne de blocs, la base de données est ainsi décentralisée, transparente et ultra-sécurisée. Avec une telle approche, les données concernées sont impossibles à falsifier.

La blockchain trouve de plus en plus de débouchés. Non seulement au niveau du secteur privé, en premier lieu la finance, pour la traçabilité des produits et pour les échanges de biens et de services, mais également au niveau des administrations publiques.

En Europe, l'Estonie se distingue particulièrement par son engagement à offrir une véritable numérisation des actes entre son administration et sa population. Ses habitants ont ainsi une identité numérique qui leur permet de signer des contrats, payer des impôts, voter, accéder à leur dossier médical, créer une entreprise, intervenir en justice, échanger avec l'administration, etc. Toute cette architecture est basée pour l'essentiel sur la technologie blockchain qui est aussi utilisée par d'autres institutions, telles que l'organisation du traité de l'Atlantique Nord (OTAN), le Département de la défense ou celui de l'énergie aux Etats-Unis, et bien d'autres.

En Suisse, le canton de Schaffhouse vient de débuter un partenariat avec la start up « Procivis » pour mettre en place une identité numérique qui permet à ses citoyens de payer ses impôts, de s'inscrire au contrôle des habitants et à terme de voter de façon électronique.

Par ailleurs, Procivis vient d'annoncer, fin septembre, un partenariat avec l'Université de Zurich pour la mise en place d'une solution de e-voting basée sur la technologie Blockchain.

Cette technologie présente de nombreux intérêts :

- *Economique : en fluidifiant les relations entre l'administration et les administrés, y compris les entreprises, ce qui permet un gain en compétitivité et une réduction des coûts.*
- *Social : cela démocratise l'accès au service et promeut aussi un rapport plus décentralisé et horizontal.*
- *Sécuritaire : cette technologie représente une réponse sérieuse et efficace aux risques de cybercriminalité et à la protection de la sphère privée.*
- *Ecologique : elle permet une très bonne traçabilité des produits.*

L'application d'une telle technologie dans le canton de Vaud nous permettrait d'être véritablement à la pointe de l'innovation.

Ainsi, par ce postulat, nous demandons au Conseil d'Etat d'étudier les possibilités d'utiliser la technologie blockchain dans les services que le canton pourrait offrir en matière de cyberadministration et de e-voting.

RAPPORT DU CONSEIL D'ETAT

1. RAPPEL DU CONTEXTE ET DES ENJEUX

Ce document constitue le rapport demandé par le Grand Conseil, sur préavis de sa Commission thématique des systèmes d'information (CTSI), en réponse au postulat Vassilis Venizelos et consorts – *Blockchain : le web 3.0 peut changer les rapports entre l'administration et les administrés*. La Direction générale du numérique et des systèmes d'informations (DGNSI), mandatée pour réaliser le présent rapport, a pris en considération la requête émise dans le postulat ainsi que les commentaires formulés lors de la réunion de la CTSI le mardi 23 janvier 2018.

À la suite de la demande de la CTSI, la première section de ce rapport sera consacrée à une présentation de la technologie blockchain[1]. Si le terme de blockchain est généralement utilisé au singulier, il recouvre en fait une multitude de réalités différentes aujourd'hui, du paiement d'un rançongiciel en cryptomonnaie au développement d'une cyberadministration au service de la population. Même si la blockchain est souvent présentée comme une technologie autonome, l'objectif de cette première section consiste à montrer qu'une action humaine est nécessaire à toutes les étapes de la blockchain. Le déploiement de cette technologie ne peut en effet se faire qu'avec le concours de milliers d'individus dispersés à travers le globe, attirés par la blockchain pour différentes raisons (idéologique, économique, sécuritaire), qui participent au maintien, voire au développement, d'une blockchain. Afin de saisir cette technologie dans sa globalité, une première partie présente le socle technique qui définit la blockchain, puis une seconde partie expose différents choix possibles dans la mise en œuvre de cette technologie.

La deuxième section s'attardera sur la possibilité d'utiliser la blockchain au sein de l'État. En remontant à l'origine de la blockchain, il apparaît que cette technologie fait écho à une idéologie que l'on peut qualifier de « libertarienne ». A l'heure actuelle, de nombreuses administrations publiques se dotent toutefois de solutions basées sur la blockchain ce qui peut paraître paradoxal. Au niveau suisse, plusieurs initiatives ont été lancées. Le canton de Genève a, par exemple, élaboré en 2017 un *Proof of Concept* (PoC) sur la livraison électronique d'extraits et autres documents officiels du registre du commerce avec la technologie blockchain[2]. Le canton du Jura se base sur la blockchain pour développer sa cyberadministration. Il propose ainsi déjà une solution pour les extraits des poursuites demandés par les citoyens et devrait poursuivre avec d'autres documents officiels[3]. L'objectif de cette section sera alors de comprendre quels sont les apports qui peuvent mener une administration publique à adopter une solution basée sur la blockchain, et les risques que cette technologie comporte.

Enfin, la dernière section de ce rapport sera consacrée à l'illustration du cas concret de l'identité électronique (e-ID), dans lequel le recours à la blockchain peut s'avérer opportun. En effet, à la suite du rejet de la Loi fédérale sur les services d'identification électronique (LSIE) lors des votations populaires du 7 mars 2021, six motions[4] ont été déposées le 10 mars 2021 pour demander un nouveau projet d'e-ID, détenu par l'État cette fois-ci. Le Département fédéral de justice et police (DFJP), en charge de ce dossier, a élaboré un document de travail[5] qui a été ouvert à une consultation publique à l'automne 2021. Les retours de plusieurs cantons, entreprises et associations[6] ont mis en lumière la pertinence du modèle d'identité auto-souveraine (*self-sovereign identity*), qui peut demander de recourir à la technologie blockchain. L'Etat de Vaud s'est engagé dans ces réflexions et prépare actuellement un PoC. L'objectif de la dernière section du présent rapport vise ainsi à présenter de manière succincte le principe du modèle d'identité auto-souveraine et le travail en cours au sein de la DGNSI afin de répondre à la demande formulée dans le postulat. Le rapport se limitera toutefois à décrire les possibilités offertes par la blockchain dans le domaine de la cyberadministration en excluant le vote électronique. En effet, le Conseil d'État a formulé à réitérées reprises ses réserves à l'égard du vote électronique, en l'état actuel, pour des questions de sécurité[7].

---

[1] Le terme blockchain sera préféré à celui de chaîne de blocs dans ce rapport afin de concorder avec le titre du postulat.
[2] Preuve de concept blockchain appliquée au registre du commerce, Vincent Pignon, Compte-rendu de projet, 12.12.2017.
[3] Les documents officiels de l'Administration jurassienne sécurisés numériquement à l'aide de la Blockchain, Communiqué de presse du Canton du Jura, 07.03.2022.
[4] La motion « À l'État de mettre en place une identification électronique fiable » a été déposée le 10.03.2021 par Gerhard Andrey (21.3124), Franz Grüter (21.3125), Min Lin Marti (21.3126), Jörg Mäder (21.3127), Simon Stalder (21.3128) et par le groupe libéral-radical (21.3129)
[5] Document de travail concernant le projet d'identité électronique (e-ID), Publication de l'Office fédéral de la justice (OFJ), 15.09.2021.
[6] Rapport sur les résultats de la consultation publique concernant le projet d'identité électronique (e-ID), Publication de l'Office fédéral de la justice (OFJ), 17.12.2021.
[7] Le Conseil d'Etat s'oppose à l'avant-projet de loi concernant le vote électronique, Communiqué de presse du Conseil d'Etat vaudois, 22.03.2019.

2. PRESENTATION DE LA TECHNOLOGIE BLOCKCHAIN

La blockchain – notamment par le biais de la cryptomonnaie bitcoin – est aujourd'hui devenue un terme couramment utilisé, alors même que la technologie sous-jacente demeure bien souvent opaque. Le caractère nébuleux de cette technologie se reflète jusque dans sa définition. Si l'origine de la blockchain est généralement attribuée à la conception de la chaîne Bitcoin en 2009 par Satoshi Nakamoto, les organismes de normalisation n'en ont défini les caractéristiques, aussi bien fonctionnelles que techniques, que récemment. Ce n'est ainsi qu'en 2019, soit 10 ans après les débuts de Bitcoin, que le National Institute of Standards and Technology (NIST), organisme de normalisation américain, publie sa définition de la blockchain[8]. L'organisation internationale de normalisation (ISO) poursuit encore ses travaux. En France, l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) a défini la blockchain en ces termes :

> *Ce que l'on appelle par métonymie blockchains (ou chaînes de blocs) désigne des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués (distributed ledgers), sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers.*[9]

Cette section propose de détailler dans une première partie cette définition afin d'avoir une compréhension du socle technique de la blockchain. Une seconde partie sera consacrée à la présentation de divers choix qui peuvent être effectués et qui vont mener à différents types de gouvernance possibles pour cadrer cette technologie.

2.1 La base technique de la blockchain

D'un point de vue technique, la technologie blockchain repose sur une combinaison entre une architecture distribuée et des fonctions de cryptographie. Elle permet ainsi de proposer un système fiable et sécurisé, dans lequel la transparence permet *in fine* de garantir l'intégrité et l'immuabilité des informations stockées dans la chaîne.

2.1.1 Une architecture distribuée

La définition de la blockchain mentionne qu'il s'agit d'un registre répliqué et distribué. Ces caractéristiques font référence à l'architecture, c'est-à-dire à la manière dont un système d'information ou un réseau est organisé. La structure d'un réseau informatique peut prendre diverses formes, allant d'une architecture complètement centralisée à une architecture totalement distribuée.

Dans une architecture centralisée, également appelée client-serveur, un serveur central alimente un réseau de clients, comme illustré sur le schéma ci-dessous. La relation est donc asymétrique. En ôtant le client, le réseau sera toujours opérationnel, alors qu'en retirant le serveur central, c'est l'entier du système qui s'écroule. Ce type d'architecture présente l'avantage de faire bénéficier l'ensemble du réseau de compétences (stockage, sécurité, puissance de calcul, gestion des accès, etc.) concentrées en un seul pôle et de garantir l'intégrité des informations véhiculées. À titre d'exemple, une application informatique peut être fournie et gérée par la DGNSI à l'ensemble des collaborateurs et collaboratrices de l'Administration cantonale.

Dans une architecture décentralisée coexistent plusieurs serveurs centraux qui assurent la pérennité du réseau. La disparition d'un « nœud » central entraînera en principe la redistribution des nœuds qui y sont liés sur d'autres nœuds centraux sans ébranler l'entier du système. L'infrastructure informatique de l'État est décentralisée car, pour assurer le maintien des systèmes d'information, les données sont répliquées dans plusieurs serveurs.

[8] Blockchain Technology Overview, D. Yaga, P. Mell, N. Roby & K. Scarfone, National Institute of Standards and Technology, Octobre 2018.
[9] Les enjeux technologiques des blockchains (chaînes de blocs), Rapport au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, 20.06.2018.

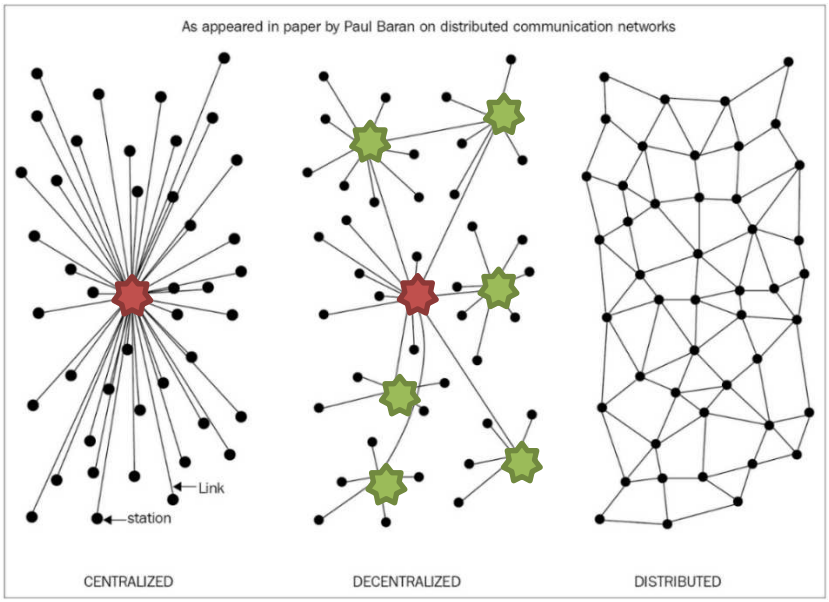


Figure 1 - Différents types d'architecture, adapté de Paul Baran (1964)[10]

Dans une architecture distribuée, chaque nœud (unité informatique indépendante) possède le même poids. Il existe alors des interconnections entre les nœuds qui permettent au réseau de distribuer l'information et de perdurer même si certains nœuds devaient disparaître. La mise en œuvre d'une telle architecture est toutefois complexe pour assurer une solution viable, avec des informations fiables, une sécurisation du réseau et la possibilité de faire évoluer le système. La technologie blockchain parvient à mettre en place un tel réseau[11]. En distribuant l'information à un grand nombre de nœuds qui la répliquent, chacun de ces nœuds participe à assurer l'immuabilité des données du système. Il faudrait en effet manipuler l'information non pas sur un nœud, mais sur la majorité des nœuds du réseau pour parvenir à falsifier une information. A l'immuabilité des données permise par leur réplication au sein d'un réseau de nœuds s'ajoutent des mécanismes assurant qu'elles ne puissent être corrompues ou modifiées : les fonctions de cryptographie.

2.1.2 Des fonctions de cryptographie

Comme la définition de la blockchain le mentionne, le registre des transactions qu'une chaîne de blocs contient est distribué, c'est-à-dire que les informations sont partagées entre les nœuds du réseau, et de ce fait, ce registre est transparent. Il a ainsi fallu établir un moyen d'encoder les données qui permette de sécuriser le contenu des données tout en garantissant la transaction effectuée.

Afin de sécuriser le contenu des données qui seront enregistrées dans la blockchain, il est nécessaire d'avoir recours à une procédure cryptographique : la fonction de hachage. Une fonction de hachage est un algorithme qui consiste à convertir des données, quelles qu'elles soient (texte, image, etc.), en une chaîne de caractères de longueur fixe, qui constitue l'empreinte numérique de ces données. La force de la fonction de hachage réside dans deux caractéristiques. D'une part, elle permet d'assurer l'intégrité des données enregistrées car une seule modification des données, si minime soit-elle, produirait une empreinte complètement différente. D'autre part, la fonction de hachage est irréversible, ce qui signifie que, s'il est facile de produire une empreinte numérique à partir de données, il est en revanche presque impossible de reconstituer les données originelles à partir d'une empreinte (du moins avec les technologies actuelles). En somme, l'empreinte agit comme preuve : elle garantit que les données originelles n'ont pas été modifiées sans qu'il soit nécessaire d'y accéder effectivement.

[10] On Distributed Communications Networks, Paul Baran, Mars 1964.

[11] Un réseau distribué n'est cependant pas propre à la blockchain. D'autres technologies reposent également sur une architecture distribuée, comme le protocole BitTorrent qui repose sur un modèle d'égal à égal (*peer-to-peer* ou P2P). Dans ce type de réseau, le nœud est à la fois client et serveur, ce qui facilite la diffusion d'information qui ne provient plus d'une source unique, mais potentiellement d'une multitude de sources.

Une fois les données encodées, il faut encore un moyen pour identifier les utilisateurs de la blockchain pour que les transactions inscrites dans la blockchain aient du sens. Pour y parvenir, le concept de clé privée et clé publique, déjà largement utilisé dans des solutions informatiques, est mobilisé. Les clés sont liées aux fonctions de cryptographie et jouent le rôle de codeuses et/ou décodeuses d'informations. Elles permettent de se prémunir contre une divulgation des données, mais également contre une éventuelle modification malintentionnée de celles-ci. Ainsi, l'intégrité des données est assurée et seuls les détenteurs d'une clé seront capables d'encoder ou de décoder les informations.

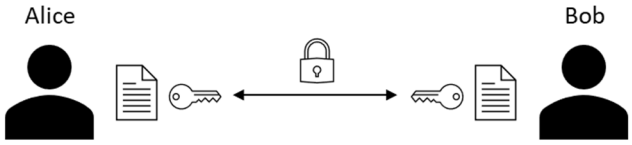


Figure 1 - Système de chiffrement symétrique

Dans un système de chiffrement symétrique, par exemple pour sécuriser des données, une même clé pourra coder et décoder l'information. Ainsi, sur le schéma ci-dessus, Alice encode ses données grâce à une clé, rendant le contenu de son document inintelligible. En transmettant la clé à Bob, ce dernier sera en mesure de décoder l'information. Les deux personnes auront ainsi accès au même contenu, mais celui-ci sera encodé durant la transmission. Le système de chiffrement symétrique prend habituellement la forme d'un mot de passe (la clé) qu'il est nécessaire d'entrer pour accéder par exemple à un document ou à un disque dur.

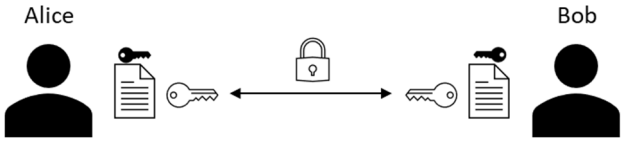


Figure 2- Système de chiffrement asymétrique

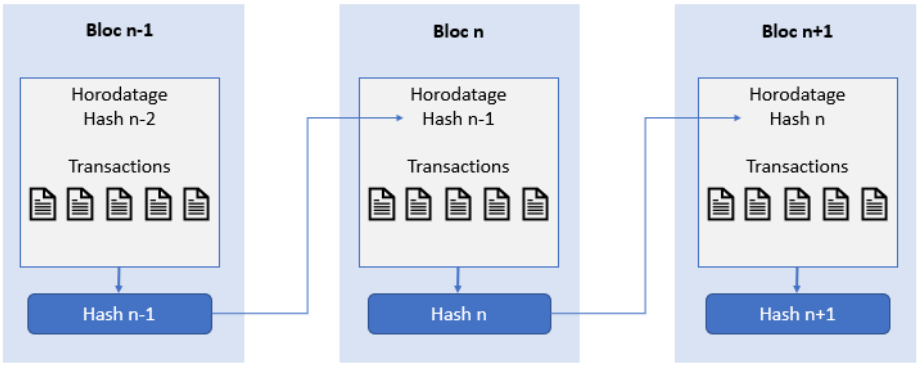
Dans un système de chiffrement asymétrique, il existe deux types de clés différentes : une clé privée, nominative, et une clé publique, partagée. Dans le schéma ci-dessus, Alice signe un document avec sa clé privée, ce qui signifie qu'elle ajoute une marque indélébile dans l'information attestant que c'est bien elle, et personne d'autre, qui transmet cette information. Elle chiffre ensuite les données avec la clé publique de Bob, permettant à ce dernier de déchiffrer le contenu du document grâce à sa clé privée. Pour s'assurer que la signature apposée dans le document est bien celle d'Alice, Bob utilise la clé publique d'Alice. Le chiffrement asymétrique est largement utilisé aujourd'hui pour les services de messagerie ou de visioconférences.

Dans le cas de la blockchain, l'intérêt d'utiliser un système basé sur le couplage entre clé privée et clé publique repose sur la possibilité d'anonymiser les utilisateurs tout en ayant un moyen de garantir qu'ils ont effectivement effectué certaines transactions. Lorsqu'un utilisateur souhaite rejoindre une blockchain et créer un portefeuille virtuel[12] (*wallet*), il se voit attribuer une combinaison aléatoire qui constitue son adresse unique. Celle-ci permet ensuite de calculer sa clé publique ainsi que son numéro de compte. Ces trois composantes permettront de l'identifier dans la blockchain et d'effectuer des transactions mais n'ont pas forcément de lien direct avec une quelconque identité attestée (passeport, carte d'identité, etc.). En cas de perte, de vol ou de destruction de la clé privée, celle-ci ne pourrait être restaurée. Cette condition assure la protection des données, puisque l'utilisateur est le seul détenteur de son identifiant, mais peut également représenter un risque en cas de perte car personne ne sera en mesure de rendre cette clé à l'utilisateur.

[12] Le portefeuille virtuel prend la forme d'un logiciel ou d'une application permettant de stocker et gérer des données.

2.1.3 Construction d'une chaîne de blocs

Une fois les transactions cryptographiées, la dernière étape consiste à les enregistrer sur la blockchain. Pour cela, elles vont être regroupées dans des blocs horodatés et liés chronologiquement les uns aux autres. Tout comme les fichiers ont été convertis grâce à une fonction de hachage, le même procédé est appliqué à chaque bloc afin d'obtenir une empreinte du bloc, représentée dans le schéma ci-dessous par la notion de « Hash ». La chronologie est en effet importante car cela permet de se prémunir contre des tentatives de fraudes. Chaque bloc contenant dans son calcul le hash du bloc précédent, toute tentative de modification rendrait caduque toutes les vérifications de la chaîne. C'est ainsi que les données enregistrées dans une blockchain sont réputées immuables.



2.2 La blockchain, une technologie aux définitions multiples

Le terme de blockchain – et la définition technique présentée ci-dessus l'illustre – est généralement associé à une technologie autonome, proposant une réalité dans laquelle la confiance ne se situe plus au niveau de l'humain, mais au niveau de la machine. Une blockchain serait ainsi une plateforme neutre et impartiale qui traiterait chaque nœud – et par extension l'humain qui le possède – sans distinction. Le nouvel espace proposé avec la blockchain n'est pourtant pas aussi dénué de choix humains. Derrière chaque algorithme, chaque fonction de cryptographie, chaque nœud, se trouve un être humain, guidé par son idéologie, par son opinion, par ses intentions. Pour Bitcoin, la première blockchain, Satoshi Nakamoto a par exemple effectué un certain nombre de choix afin de créer un environnement qui soit le plus autonome possible. Il a décidé la manière de rejoindre le réseau, de valider un bloc et même le nombre maximum de bitcoins qui pourront être créés[13]. Si Satoshi Nakamoto s'est retiré de la gouvernance de Bitcoin, la blockchain continue pourtant d'évoluer grâce au travail d'informaticiens qui proposent des changements qui seront acceptés ou non par les membres du réseau[14]. Cette section a pour but de présenter différentes étapes décisionnelles qui vont influencer la forme d'une blockchain.

2.2.1 L'accès à la blockchain – public ou privé

La première question à laquelle il est nécessaire de répondre au moment de développer une blockchain consiste à définir la manière dont les nœuds vont pouvoir rejoindre le réseau. Habituellement, les fonctions et applications visées avec ladite blockchain vont orienter le choix.

Les blockchains les plus connues, Bitcoin et Ethereum, sont toutes les deux des chaînes publiques, c'est-à-dire que n'importe qui peut télécharger le logiciel et créer un nœud du réseau. Le fonctionnement de ce type de chaîne repose principalement sur l'hypothèse que plus le projet proposé par la blockchain séduit, plus nombreux seront ceux qui rejoindront le réseau, en constituant un nœud supplémentaire. Et plus il y aura de nœuds dans le réseau, plus il sera difficile de corrompre la blockchain car chaque nœud possède une copie de la blockchain. Mais si ce système est robuste, il n'en demeure pas moins que les aléas liés aux comportements humains peuvent également constituer une faiblesse. Si la réputation d'une blockchain publique faiblit, le nombre d'utilisateurs pourrait lui aussi diminuer et constituer une vulnérabilité pour la stabilité de la chaîne. Si la blockchain illustre l'idéologie d'un système exempt d'organe de contrôle centralisé, il demeure néanmoins nécessaire d'assurer l'équilibre de l'ensemble du système par d'autres moyens, comme le protocole de consensus qui sera décrit ci-dessous.

[13] Avec une limite de 21 millions de bitcoins, Satoshi Nakamoto a souhaité doter sa cryptomonnaie d'une rareté intrinsèque, la rendant plus désirable tout comme le sont les métaux précieux dans le monde physique.
[14] Ce type de gouvernance se retrouve dans d'autres projets open source comme Linux.

Certains souhaitent tirer profit des avantages de la blockchain sans pour autant passer par une structure aussi complexe qu'une chaîne publique. C'est pourquoi ils optent pour une chaîne dite privée. Les chaînes privées sont détenues par des acteurs – entreprises, institutions, collectivités – qui décident qui peut rejoindre le réseau. Ce type de chaîne est généralement préféré pour des fonctions ou des applications précises, notamment pour le traçage de chaînes d'approvisionnement. Une entreprise peut ainsi s'assurer de la conformité de son produit à toutes les étapes du processus. De même, les collectivités publiques peuvent être intéressées par ce type de blockchain pour développer leur cyberadministration.

Depuis 2012, l'Estonie déploie la blockchain privée KSI de l'entreprise Guardtime dans plusieurs de ses systèmes en production, par exemple le registre foncier et de propriété, le registre des entreprises ou encore le registre des successions.

2.2.2 Le protocole de consensus

Comme vu dans la section sur la construction d'une chaîne de blocs, lors de la validation d'un bloc, les données sont passées dans une fonction de hachage pour obtenir le « Hash », une valeur qui est reprise dans le bloc suivant et assure l'immuabilité et l'intégrité des données de la chaîne. Si aucune condition supplémentaire n'était ajoutée, il suffirait, pour calculer ce « Hash », de passer les données du bloc dans une fonction de hachage et d'ajouter le nouveau bloc à la chaîne. Dans un tel cas, n'importe qui pourrait ajouter un bloc et potentiellement introduire des transactions frauduleuses. Afin d'encadrer la validation des blocs, des mécanismes régissent les blockchains – qu'elles soient publiques ou privées – afin de renforcer l'intégrité des données enregistrées et prévenir les pratiques malveillantes. Chaque chaîne de blocs utilise un ou plusieurs algorithmes ou protocoles de consensus qui permettent de déterminer divers éléments primordiaux afin de garantir l'équilibre du système : combien de transactions peuvent être inscrites dans un bloc, quand un bloc peut être validé, comment et par qui, etc. En somme, ces algorithmes font office de régulateurs de la blockchain.

.1 La preuve de travail

Le premier mécanisme de consensus, adopté pour la blockchain Bitcoin, repose sur la preuve de travail (*Proof of Work*). Pour valider un bloc, il ne suffit pas d'obtenir un « Hash » quelconque, mais il faut que celui-ci débute par une suite définie (par ex. « 00000 »). Les nœuds qui souhaitent valider un bloc vont devoir chercher une valeur (appelée « nonce ») à ajouter aux autres données (« Hash » du bloc précédent et transactions à enregistrer) qui permet de répondre à la suite imposée. Comme il n'est pas possible de prédire le résultat d'une fonction de hachage, il est nécessaire de tester de très nombreuses combinaisons avant d'en trouver une valide. Les nœuds qui valident un bloc prouvent alors qu'ils ont fourni un travail considérable, à travers la puissance de calcul nécessaire pour trouver une combinaison qui satisfasse la suite imposée. Pour encourager les membres du réseau à mettre à disposition leur force de calcul, le système est basé sur la récompense. Dès qu'une entité responsable d'un nœud détermine une solution – et que les autres nœuds la valident – elle reçoit une rémunération sous forme de cryptomonnaie. Ce phénomène s'est largement répandu dans le sens commun sous le nom de « minage » pour désigner la création de monnaie, prévue dans le protocole de la chaîne de blocs, pour récompenser le nœud qui valide le bloc. Ce modèle de consensus peut être qualifié d'innovation disruptive. Dès lors que la participation à une blockchain impose un certain investissement – soit via des équipements informatiques, soit en convertissant une devise physique – pour obtenir des cryptomonnaies, une large majorité de membres souhaite défendre ses intérêts plutôt que de tricher, ce qui permet finalement la stabilité du réseau.

Cependant, le consensus basé sur la preuve de travail montre certaines limites. S'il était possible à l'origine de calculer une preuve avec un ordinateur ordinaire et de gagner des bitcoins, il est désormais nécessaire d'avoir un grand nombre d'unités de calcul dédiés et une énergie bon marché pour être rentable. Cela génère également un fort impact écologique comme détaillé ci-après. Une autre limite repose sur la scalabilité, c'est-à-dire la capacité à s'adapter lorsque la demande de transactions augmente. Dans le cas de Bitcoin, il est possible d'inscrire 7 transactions par seconde et d'enregistrer un bloc toutes les 10 minutes. À l'échelle mondiale, ces chiffres ne sont pas suffisants pour répondre à l'essor de la demande.

.2 La preuve d'enjeu

L'évolution de la technologie a permis de surmonter les limites de la preuve de travail grâce à d'autres modèles de consensus, comme celui de la preuve d'enjeu (*Proof of Stake*) sur lequel Ethereum, une des principales chaînes de blocs avec Bitcoin, a décidé de migrer récemment. Pour valider un bloc avec ce modèle de consensus, les nœuds doivent mettre en jeu des jetons – qui représentent des monnaies virtuelles particulières – pour participer au processus. Ensuite, un algorithme, grâce à une combinaison entre la mise en jeu et la présence du nœud dans la chaîne, désigne le prochain nœud à créer un bloc. Les nœuds qui n'ont pas été désignés par l'algorithme valident ou non le bloc proposé. Si le bloc est validé, le nœud qui l'a créé est récompensé sous la forme de cryptomonnaies.

En revanche, si le nœud qui a créé le bloc a tenté de corrompre la chaîne et que son bloc n'est pas validé par les autres nœuds, alors il perd les jetons mis en jeu. S'il existe un débat pour savoir si ce modèle est moins sécurisé que celui basé sur la preuve de travail, il demeure que ce consensus présente l'avantage de consommer beaucoup moins d'énergie.

.3 La preuve d'autorité

Les deux premiers mécanismes de consensus, la preuve de travail et celle d'enjeu, présentent une complexité dans l'élaboration des algorithmes pour que le système puisse trouver une certaine stabilité tout en demeurant complètement ouvert et décentralisé. Dans le cas des chaînes privées cependant, la blockchain est généralement détenue directement par un acteur qui détermine les accès, mais également la façon de valider un bloc dans la chaîne. C'est pourquoi ce type de mécanisme s'appelle la preuve d'autorité (*Proof of Authority*). Les vérificateurs sont en général prédéterminés et connus de tous. C'est leur réputation qu'ils mettent en jeu et non un capital financier.

3. LES POSSIBILITES D'UTILISATION DE LA BLOCKCHAIN POUR L'ETAT

Afin de répondre à la principale demande formulée dans le postulat, cette section propose d'évaluer la blockchain en présentant les principaux apports et risques identifiés dans l'utilisation de cette technologie. Il ne s'agit pas là d'envisager des applications où la blockchain se substitue à l'autorité garantissant l'exactitude et la fiabilité de données (par exemple en matière foncière) qu'est l'Etat dans de nombreux cas mais bien d'utiliser le potentiel de cette technologie en matière de sécurité et de traçabilité des informations. Cette analyse reprend également certains éléments de la section précédente pour offrir des pistes de réflexions sur les avantages et inconvénients des différents types de blockchain et rendre ainsi compte de la complexité de recourir à cette technologie.

3.1 Les apports de la blockchain pour l'État

Le principal apport de la blockchain consiste, comme sa définition le mentionne, à stocker et transmettre des informations de manière sécurisée. Concrètement, cela signifie que les données que l'État détient restent dans ses serveurs, mais qu'une solution basée sur la blockchain pourrait attester de l'existence et de l'authenticité de données. Cette caractéristique est particulièrement intéressante dans deux cas de figure qui sont détaillés dans cette sous-section : l'interopérabilité et la minimisation des données collectées.

3.1.1 Une opportunité pour accroître l'interopérabilité

La transition numérique transforme le quotidien et amène aujourd'hui bien souvent à une hybridation des habitudes et des usages, par exemple en ce qui concerne le commerce, la réservation de services ou la gestion administrative. Ces nouvelles pratiques appellent à une interopérabilité entre les applications pour permettre aux individus de se mouvoir aisément dans ce nouvel environnement. La diversité de choix en matière technologie rend parfois difficile la communication entre les solutions choisies.

Dans le domaine de la cyberadministration par exemple, il n'existe pas en Suisse d'architecture unifiée pour plusieurs raisons. L'organisation politique du pays, basée sur le principe de subsidiarité, octroie une large autonomie aux différentes administrations. Il en résulte une multitude de solutions adoptées, qui reflètent généralement des particularismes régionaux (politiques, topographiques, économiques, etc.). En comparaison, la performance d'un pays comme l'Estonie s'inscrit dans un contexte très différent de celui de la Suisse. À son indépendance de l'URSS dans les années 1990, l'Estonie a construit son administration de toute pièce en misant sur les nouvelles technologies. Elle a ainsi intégré dès la conception les enjeux d'une administration numérique. A l'inverse, les administrations suisses se sont construites de manière bien plus ancienne et leur organisation le reflète.

Aujourd'hui pourtant, la transition numérique appelle à une plus grande interopérabilité entre les solutions adoptées afin de correspondre à la complexité de l'organisation de la société. Lors de l'élaboration de nouvelles prestations en ligne, il devient indispensable d'observer ce qui est déjà mis en place par les communes, les cantons, la Confédération et dans une certaine mesure les autres pays. Les discussions en ce sens sont encouragées, notamment par la création depuis le 1er janvier 2022 de l'organisation « Administration numérique suisse » (ANS). L'objectif de cette organisation consiste à mutualiser les efforts et les réflexions pour accompagner la numérisation de l'administration en Suisse.

La technologie blockchain offre des perspectives prometteuses à cet égard, et dont l'utilisation mériterait d'être analysée au cas par cas. Alors que les premiers projets blockchain s'attelaient essentiellement à démontrer leurs valeurs sur les aspects fondamentaux que sont les registres distribués, les contrats autonomes, les consensus ou encore la sécurité, il existe à présent des applications concrètes de cette technologie. Certaines initiatives se focalisent ainsi sur la normalisation et la production d'outils et de passerelles pour permettre d'échanger de l'information entre des systèmes différents. Il existe également de nombreux projets de type *cross-chain bridge*[15] qui doivent permettre de transférer des actifs numériques entre les chaînes. Alors que la numérisation accroît la nécessité de communiquer avec les autres cantons, la Confédération et l'Europe, ces initiatives offrent des perspectives d'interopérabilité.

Ainsi, la technologie blockchain peut présenter l'avantage d'accroître l'interopérabilité tout en préservant le rôle de chaque entité. Outre la nécessité de se baser sur une infrastructure blockchain, chaque entité est libre de développer la solution qu'elle désire selon ses besoins. L'interopérabilité entre les solutions est ensuite facilitée afin de correspondre à la complexité de l'organisation de la société et de proposer une continuité entre les solutions pour la population.

[15] Littéralement « pont entre les chaînes », désigne la capacité à établir des liens entre différentes chaînes de blocs.

3.1.2 Vers une minimisation de la collecte de données

Les questions de collecte, transfert et utilisation de données sont intrinsèquement liées à la cyberadministration. Certaines de ces données peuvent être sensibles et leur traitement doit donc être correctement encadré afin de minimiser les risques pour la population. Dans ce sens, les fonctions de cryptographie sur lesquelles repose la blockchain pourraient permettre un haut degré de sécurité des données. Cette caractéristique n'est cependant pas spécifique à la blockchain et peut donc se retrouver avec d'autres technologies. En revanche, une solution développée sur la blockchain pourrait améliorer la maîtrise sur les données transmises : le contrat autonome (*smart contrat* ou contrat intelligent[16]).

Dès 2013, la deuxième génération de blockchain, incarnée par Ethereum, a permis de mettre en œuvre la notion de contrat autonome. Ce concept prend forme grâce à Nick Szabo dans les années 1990, mais n'a pu être réellement déployé qu'avec la technologie blockchain. Le contrat autonome consiste à établir des conditions qui devront être respectées afin qu'une autorisation soit délivrée de manière automatique si elles sont réunies. Ces règles et conditions sont mises en œuvre dans la blockchain et sont ainsi visibles et appliquées de la même manière à tout le monde. En outre, la blockchain permet de protéger le contrat contre la falsification ou la modification des conditions. La force de ce concept réside ainsi dans la possibilité d'établir un contrat sur la blockchain qui s'exécute de manière indépendante, sans tiers de confiance, lorsque les conditions sont remplies. Elle permet ainsi de s'affranchir des rapports de force qui pourraient retarder voire empêcher l'exécution du contrat par des procédures judiciaires chronophages.

L'exemple suivant permet d'illustrer en pratique l'apport du contrat autonome. Une entreprise désire fournir un service à des clients, mais pour pouvoir délivrer ce service, le client doit répondre à un certain nombre de critères :

- Il doit être domicilié dans le canton de Vaud.
- Il doit être majeur.
- Il ne doit pas faire l'objet de poursuites.

Cette entreprise pourrait déployer un contrat autonome qui interroge les registres de l'État avec l'accord de ce dernier. Ce processus se déroulerait de manière transparente, les conditions et les règles sont connues et s'appliquent de la même manière pour tout le monde. Les contrats autonomes comportent en outre l'avantage de minimiser la collecte de données, et ce par deux mécanismes. Premièrement, si la première condition fixée par le contrat n'est pas respectée, alors les conditions suivantes ne sont pas vérifiées. Ensuite, seules les informations utiles sont transmises. Ceci permet par exemple de se limiter à vérifier si le client est majeur par un « oui » ou par un « non » plutôt que de devoir avoir accès à sa date de naissance, cette donnée impliquant la transmission de plus d'informations que nécessaire. Cette caractéristique est importante car la protection des données et de la vie privée des utilisateurs passe en grande partie par la minimisation des données récoltées. Grâce au concept de contrat autonome et à la blockchain, il est ainsi possible de vérifier certaines informations sans pour autant devoir fournir de nombreuses données personnelles superflues.

3.1.3 La résilience d'une solution basée sur la blockchain

Une des missions de la DGNSI consiste à assurer la disponibilité des moyens informatiques et de télécommunication nécessaires quotidiennement au bon fonctionnement de l'Administration. Concrètement, cela nécessite :

- D'avoir des prestations minimales en cas de catastrophe majeure ou de destruction de l'infrastructure.
- D'avoir une solution de communication en cas de panne des numéros d'urgence (117, 118, 144, etc.).
- D'avoir une alternative en cas de cyberattaque de type DDOS[17] .
- D'avoir des réplications de données en cas de cyberattaque sur les données.

Il convient dès lors d'évaluer la résilience des solutions choisies afin de répondre positivement à ces exigences.

Dans ce sens, une solution basée sur les chaînes de blocs offre l'avantage de ne pas dépendre de la stratégie d'un fournisseur, qui peut décider de retirer un produit ou un service. Par exemple, pour les solutions dans le nuage (*cloud*), il est d'usage, chez les fournisseurs, de ne laisser qu'une année aux clients pour migrer ou s'adapter à un changement. De plus, les données sont stockées chez le prestataire. Une migration ou des changements peuvent être dans ce cas coûteux, voire difficiles.

---

[16] La notion de *smart contract* est généralement traduite par « contrat intelligent » en français. Cette proposition peut toutefois porter à confusion car l'exécution du contrat est simplement automatisée et ne nécessite aucune forme de compréhension ou d'adaptation propre à l'intelligence. C'est pourquoi le terme de contrat autonome est préféré dans ce rapport.

[17] Une attaque par déni de service (communément abrégée DDOS pour *Distributed Denial of Service attack*) vise à perturber ou rendre indisponible un service.

Basée sur un réseau distribué, la technologie blockchain permettrait *a priori* une meilleure stabilité. De plus, il est possible d'avoir une copie des données et donc de garder un certain contrôle en cas d'adaptation. En revanche, il est nécessaire d'évaluer correctement le projet choisi, qui doit pouvoir compter sur un réseau suffisamment grand et stable pour garantir la sécurité et la résilience du système.

3.2 Les risques de la blockchain pour l'État

En tant qu'État de droit, le canton de Vaud doit veiller à développer sa cyberadministration en conformité avec les bases légales et aux tâches qui lui incombent. Cette section examine ainsi les risques pour l'Etat que pourrait comporter l'utilisation de la blockchain, dans les domaines d'économie, de la sécurité, de la protection des données personnelles, de l'écologie. Elle conclura sur une réflexion mettant en perspective le rôle de l'État et le système de gouvernance proposé pour la blockchain.

3.2.1 La difficulté à déterminer les coûts financiers d'une solution basée sur la blockchain

En tant qu'institution publique, l'Etat de Vaud doit veiller à utiliser de la manière la plus judicieuse l'argent public. À cet égard, l'adoption d'une solution basée sur la technologie blockchain peut s'avérer problématique dans la mesure où elle a un coût très variable. La difficulté à estimer le coût représente un enjeu majeur pour une administration publique. En effet, lorsque l'État fait réaliser un projet d'envergure et doit pour cela se tourner vers des entreprises privés, cette opération est soumise à la loi sur les marchés publics avec un coût déterminé pour une prestation définie et limitée dans le temps.

Lors de l'évaluation d'une solution basée sur la blockchain, le choix entre une chaîne publique et privée peut avoir des répercussions importantes sur le plan financier. Dans le cas d'une solution basée sur une chaîne privée (par exemple une chaîne exclusivement en mains de l'Etat), il est possible d'établir une procédure classique de marchés publics car le contrat lie l'administration publique à un fournisseur. Dans le cas d'une solution basée sur une chaîne publique, à savoir ouverte à tous ceux qui souhaiteraient y adhérer, l'accès au réseau est libre et n'engendre pas de frais. En revanche, chaque information enregistrée sur la chaîne comporte un coût de quelques centimes, à payer dans la cryptomonnaie de la chaîne. La volatilité des cryptomonnaies (qui ne sont précisément pas adossées à une banque centrale) ne permet ainsi pas de prédire les coûts à moyen ou long terme de ces opérations. Ainsi, même en imaginant à l'avance le volume de données à enregistrer, il serait impossible d'évaluer le coût d'une solution basée sur une chaîne publique.

Une approche pour atténuer le problème rencontré dans le cas des chaînes publiques consisterait à ce que l'État participe de manière active au réseau. En mettant à disposition du stockage ou des ressources de calcul pour valider les transactions, l'État pourrait ainsi être rémunéré dans la devise virtuelle utilisée. Ces fonds permettraient de pallier la conversion entre francs suisses et cryptomonnaie pour les projets basés sur la blockchain et donc de prévenir le problème de la volatilité. En outre, ces réserves de ressources pourraient être utiles en cas de charges non prévues ou temporairement exceptionnelles, ainsi qu'en cas de pannes d'une partie des ressources techniques.

3.2.2 Des risques de cybercriminalité persistent avec la blockchain

Pour assurer ses missions, l'Etat collecte et traite de nombreuses informations sur sa population, son territoire, et les entreprises qui y sont actives. Certaines de ces données peuvent être sensibles, notamment celles portant sur l'identité, et doivent obligatoirement être fournies dans le cadre de certaines prestations. L'Etat a alors le devoir d'assurer la sécurité des prestations qu'il fournit en ligne ainsi que des données récoltées. Si la technologie blockchain est réputée pour sa dimension sécuritaire, comme la présentation de la technologie et de ses différents degrés de sécurité l'a montré, elle n'est toutefois pas exempte de potentielles vulnérabilités.

Une première vulnérabilité possible concerne l'affaiblissement d'une chaîne de blocs si le nombre de nœuds diminue. En temps normal, corrompre un ou plusieurs nœuds ne suffirait pas pour ébranler l'ensemble de l'écosystème : étant donné que la chaîne de blocs repose sur un registre distribué des transactions et que chaque nœud en possède une copie, les nœuds qui tenteraient de corrompre la chaîne en seraient exclus et formeraient une nouvelle chaîne. Cependant, si la majorité des nœuds tentent de corrompre la chaîne, alors la chaîne validera les données corrompues. Ce cas de figure est connu sous le nom de « l'attaque des 51% ». De manière générale, une chaîne publique sera moins sujette à ce type d'attaque qu'une chaîne privée car elle compte habituellement plus de nœuds. Cependant, la diversité des participants est également importante et constitue un facteur important de robustesse.

Une deuxième vulnérabilité se rapporte à la qualité des algorithmes. Les fonctions de cryptographie ainsi que le protocole de consensus appliqué doivent être suffisamment robustes pour garantir la sécurité du système. Les fonctions de cryptographie doivent assurer l'intégrité et l'immuabilité des données enregistrées alors que le protocole de consensus doit encadrer correctement les règles qui régissent la chaîne de blocs, afin de parer à l'éventualité d'une manipulation inopinée.

Une troisième vulnérabilité touche le portefeuille virtuel, à savoir le logiciel ou application permettant de stocker et gérer des données utilisé par un membre de la blockchain lorsqu'il en devient membre (voir point 2.1.2). D'une part, si le portefeuille devait être défaillant pour une raison ou pour une autre, alors des opérations frauduleuses peuvent être effectuées et elles seront valides pour la chaîne. D'autre part, les opérations de *phishing*[18], bien connues dans le domaine de la cybercriminalité, subsistent avec la blockchain et peuvent conduire à des pertes considérables pour des utilisateurs peu prudents.

Enfin, si la robustesse des outils de chiffrement utilisés est aujourd'hui éprouvée, il n'est toutefois pas certain qu'elle ne soit pas mise à mal dans le futur. En effet, l'évolution des technologies, et en particulier des puissances de calcul, rend probable l'éventualité que, dans quelques décennies, le chiffrement actuel puisse être déjoué.

3.2.3 L'immuabilité des données conservées sur une chaîne de blocs est contraire à la LPrD

La loi sur la protection des données personnelles du canton de Vaud (LPrD) vise à protéger les personnes contre l'utilisation abusive des données personnelles les concernant. À ce titre, la technologie blockchain soulève plusieurs questions. Avant tout, bien que plusieurs mécanismes permettent une « pseudonymisation » des utilisateurs sur une chaîne de blocs, ceux-ci demeurent potentiellement identifiables. La transparence permise par la traçabilité des données rend en effet possible l'identification à partir d'un croisement de données. De plus, le caractère immuable des données enregistrées sur une chaîne de blocs constitue une limite à la protection des données car il se heurte au principe d'exactitude[19] ainsi qu'au droit à l'effacement ou droit à l'oubli[20]. Si les données contenues hors de la chaîne de blocs peuvent effectivement être effacées, il demeurera une trace de celles-ci sur la blockchain.

La technologie blockchain n'est cependant pas complètement incompatible avec la protection des données. Par exemple, le recours à une chaîne privée (non ouverte à tous) est généralement plus compatible au regard de la protection des données qu'une chaîne publique. Il est aussi possible de recourir à une alternative à l'effacement des données en détruisant les clés cryptographiques, rendant ainsi les données enregistrées dans la blockchain inaccessibles[21]. Toutefois, une analyse au cas par cas demeure nécessaire.

3.2.4 Une technologie énergivore

Le bilan écologique de la blockchain est difficilement quantifiable car il dépend une nouvelle fois des solutions choisies. Cette sous-section offre un aperçu du coût énergétique de cette technologie ainsi que des potentielles économies que ses usages peuvent permettre, notamment en termes d'optimisation dans la gestion de ressources.

Comme évoqué plus haut dans ce rapport, les chaînes publiques reposent sur des protocoles de consensus qui peuvent être énergivores. La preuve de travail, encore utilisée par Bitcoin, est un modèle insoutenable à terme, car l'énergie demandée pour « miner » du bitcoin ne cesse de croître. Ceci amène par ailleurs une délocalisation des centres de calcul dans des pays où l'énergie est bon marché et produite avec des contraintes environnementales limitées. Le réseau qui soutient Bitcoin consommerait environ 120 térawatt-heure[22], soit plus de deux fois la consommation annuelle totale d'électricité en Suisse[23]. À titre de comparaison, le centre de données de l'Etat de Vaud a consommé 0,002 térawatt-heure en 2021.

---

[18] Le *phishing*, ou hameçonnage, consiste à piéger un internaute afin d'obtenir des informations personnelles, généralement dans le but d'usurper son identité.

[19] Art. 5 de la Loi fédérale sur la protection des données (LPD) du 19 juin 1992.

[20] Art. 17 du Règlement européen 2016/679 (RGPD) du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[21] Avec les technologies actuelles, la suppression complète et définitive d'une donnée devient très compliquée car 1) La commande *delete* (effacer) n'efface pas la donnée mais la marque comme effacée, alors qu'elle est toujours présente dans les couches basses ; 2) Il existe des copies (cache) ; 3) Il existe des sauvegardes. Dans ce contexte, la destruction de clés cryptographiques offre l'avantage de rendre illisibles les données, mais également les éventuelles copies et résidus.

[22] « Des pistes pour des cryptomonnaies plus durables », Sébastien Ruche, Article du Temps, 25.05.2021 (modifié le 12.09.2022).

[23] Consommation d'électricité 2020 : baisse de 2,6% en raison de la pandémie, Publication de l'OFS, 16.04.2021.

Aujourd'hui, le modèle de consensus basé sur la preuve de travail tend à être remplacé par des algorithmes comme la preuve d'enjeu, qui consomment considérablement moins d'énergie. Cependant, même avec un consensus moins énergivore, la nature même de la blockchain fait qu'elle n'est pas efficiente d'un point de vue énergétique. Pour atteindre et garantir les caractéristiques d'une blockchain publique, il est nécessaire d'avoir un grand nombre de nœuds, si possible distants les uns des autres. Il y a donc une partie non négligeable de l'énergie qui est utilisée dans le seul but de maintenir le système fonctionnel et en garantir la sécurité.

Malgré l'émergence d'applications innovantes, d'un point de vue des utilisations possibles au sein de l'Administration cantonale, en particulier pour la cyberadministration, il est ainsi nécessaire d'évaluer l'impact sur le plan énergétique et environnemental du recours à une solution de blockchain, en particulier sous l'angle de la durabilité du numérique telle que figurant dans la Stratégie numérique du Canton de Vaud et de l'Agenda 2030, étant entendu que le recours à la technologie de la preuve d'enjeu (Proof of Stake) est moins énergivore.

3.2.5 Une technologie transparente mais technocratique

Si la transparence constitue souvent l'argument premier pour soutenir le recours à la technologie blockchain, cela signifie avant tout que l'information est disponible. Toutefois, cela ne signifie pas encore qu'elle soit compréhensible pour n'importe quelle personne. L'évolution de la technologie offre davantage de cas d'utilisation mais s'accompagne dans le même temps d'une complexification toujours plus grande des algorithmes. C'est pourquoi il est aujourd'hui nécessaire d'être doté de solides compétences techniques pour pouvoir analyser et exploiter cette technologie.

Concrètement, cela signifie que l'hypothèse selon laquelle la blockchain permet de se passer totalement de tiers de confiance n'est vraie que dans le cas où les parties prenantes ont les connaissances nécessaires pour analyser l'algorithme qui régit les transactions. La majorité des utilisateurs·trices finaux de solutions basées sur une blockchain n'a pas la capacité d'attester par elle-même de l'authenticité du processus. Ces utilisateurs·trices n'ont donc d'autres choix que de faire confiance à un tiers – l'Etat, une entreprise, une association, etc. – qui dispose des compétences pour analyser les algorithmes. Le recours à la blockchain doit s'accompagner dès lors d'une réflexion sur les conséquences en termes d'égalité dans une société déjà marquée par une fracture numérique.

3.2.6 État de droit et blockchain – deux modèles d'organisation bien différents

La blockchain constitue le sous-bassement technologique de ce que d'aucuns appellent le web3. L'objectif affirmé de cette nouvelle génération de technologies du web est d'apporter une réponse à l'hégémonie des quelques grands fournisseurs qui ont façonné le web2, caractérisée par une certaine perte de maîtrise des données personnelles des utilisateurs, et par la difficulté pour les autres acteurs de notre société de choisir de contracter ou de développer des solutions alternatives, tant ces fournisseurs sont dominants dans leurs domaines. Face à cette centralisation, la blockchain permet d'offrir une alternative du point de vue technique mais aussi en matière de gouvernance, pour développer, déployer et utiliser des solutions informatiques dont les caractéristiques (interface, algorithme et données) sont déterminées par les utilisateurs eux-mêmes[24].

La solution DFINITY, fondée à Zürich, offre un bon exemple de l'intérêt – mais aussi des écueils – de ce type de solutions. Ce réseau de blockchain public propose une solution très innovante qui permet d'utiliser une infrastructure distribuée dans laquelle n'importe qui, sans condition, peut mettre à disposition un service ou une application, comme pourrait par exemple le faire un fournisseur de type Cloud[25]. A la différence de ce dernier toutefois, qui implique d'accepter des conditions d'utilisation souvent opaques fixées par un fournisseur[26], la gouvernance de la chaîne est directement entre les mains des utilisateurs ou propriétaires de la devise de cette chaîne, qui votent sur son fonctionnement concret et les aspects techniques et stratégiques de l'évolution du système. Ces solutions pourraient ainsi avoir un grand potentiel pour des organisations, Etats, ou communes qui chercheraient à gagner en autonomie vis-à-vis des solutions dominantes du marché, sans pouvoir développer elles-mêmes leur propre outil ou créer une législation et des contrats ad-hoc.

[24] En théorie, n'importe quel utilisateur rejoignant une blockchain publique peut participer à la gouvernance de celle-ci. En pratique cependant, il est nécessaire de disposer de solides compétences techniques et/ou d'un équipement informatique performant pour pouvoir effectivement participer activement au développement d'une blockchain.

[25] Le *cloud computing*, en français l'informatique en nuage, correspond à l'accès à des services informatiques (serveurs, stockage, mise en réseau, logiciels) via Internet (le « *cloud* » ou « nuage ») à partir d'un fournisseur.

[26] « Négocier un contrat cloud avec une multinationale ? « Un cauchemar ! » », Anouch Seydtaghia, Article du Temps, 11.03.2022.

Malgré ces avantages indéniables, le choix, pour un Etat, d'une solution du type de DFINITY ne va pas sans poser des questions essentielles en matière de démocratie, de souveraineté et d'Etat de droit. Le fait que ce soient les utilisateurs de la blockchain qui décident de son évolution constitue certes une alternative à l'oligopole dominant actuellement, mais n'implique pas pour autant un gain en matière de souveraineté pour l'organisation qui l'utilise : elle devrait en effet partager ses décisions avec les autres utilisateurs de la chaîne (situés dans le monde entier et aux suffrages inégalement répartis en fonction du volume de cryptomonnaie qu'ils détiennent), ce qui va à l'encontre de la forme de légitimité de nos sociétés démocratiques selon laquelle ce sont les citoyens, par l'intermédiaire des personnes qu'ils élisent, qui sont à l'origine des décisions collectives – indépendamment de leurs ressources.

L'autonomie que la blockchain peut avoir vis-à-vis de l'Etat, en particulier de l'Etat de droit et de sa capacité à le faire respecter, peut être illustrée très concrètement. Récemment, un utilisateur a déployé, grâce à la chaîne DFINITY, une application qui ne respecte pas les droits de propriétés de Nintendo[27][28]. L'entreprise a déposé une plainte au Canada et elle a obtenu gain de cause : le juge a demandé à DFINITY de retirer cette application. La blockchain étant gouvernée par ses utilisateurs, la suppression de ce contenu par DFINITY requerrait un vote favorable de la majorité de ses utilisateurs. Or, 97% d'entre eux ont décidé de conserver l'application. Si celle-ci a finalement été supprimée par son propriétaire lui-même, cet exemple montre bien les limites que la blockchain pose à l'exercice de la souveraineté et au respect de l'Etat de droit : si le propriétaire n'avait pas fini par se plier à la décision de justice, l'Etat concerné n'aurait eu aucun moyen de la faire respecter. L'anonymat permis par la blockchain accentue encore cet écueil, puisque l'Etat ne peut pas imposer ses décisions à l'organisation à l'origine de la blockchain : il doit trouver l'auteur de l'infraction et trouver un moyen de l'obliger à supprimer le contenu en question.

En somme, si les chaînes de blocs et le web3 offrent des opportunités concrètes pour développer des solutions alternatives à celles des géants du web, leur utilisation par un Etat doit s'accompagner d'une réflexion quant au degré de contrôle démocratique et juridique qu'il doit exercer sur l'application utilisée. Car si le web3 fait la promesse d'un internet indépendant des géants du web, il peut aussi échapper au contrôle des Etats, tout en n'étant pas à l'abri d'être dominé par de nouveaux oligopoles formés par les détenteurs majoritaires des cryptomonnaies qui les sous-tendent.

3.3 Synthèse de l'évaluation de la blockchain

La diffusion de la technologie blockchain a entraîné une vague d'intérêt et de projets innovants à laquelle le domaine public n'a pas échappé. Cette technologie offre en effet des perspectives prometteuses en comparaison avec les deux autres grandes pratiques qui consistent soit à stocker des données et logiciels au sein de l'Etat soit à recourir à une solution Cloud. Avec une solution de type blockchain, la possibilité de rendre plus transparente pour certains utilisateurs spécialisés certaines des actions de l'administration publique permettrait d'accroître la relation de confiance avec une partie de la population, mais également de lui offrir une plus grande maîtrise de ses données. Dans une société toujours plus numérisée, une infrastructure basée sur la blockchain pourrait favoriser la cyberadministration en offrant des attestations numériques sécurisées, certifiées par les autorités compétentes et détenues par son titulaire, tout comme dans le monde physique (pièce d'identité, passeport, attestation de domicile, etc.).

Toutefois, l'évaluation de la blockchain montre que le recours à une telle solution requiert avant tout d'en analyser attentivement la gouvernance et les aspects techniques afin de garantir la sécurité et la résilience des services de l'État, en particulier à la lumière de la nécessaire souveraineté de l'Etat. Le manque de prévisibilité économique, le coût écologique ainsi que la question de la protection des données doivent également être pris en compte. Enfin, si l'utilisation de la blockchain poursuit l'objectif d'améliorer la relation de confiance entre l'État et la population, il est nécessaire de considérer les compétences numériques dont la population doit disposer pour comprendre les bénéfices, mais également les enjeux liés à cette technologie.

[27] Nintendo Incident : Feedback Summary and Open Questions, DFINITY Foundation, décembre 2021.
[28] Path forward on leveraging boundary nodes for content filtering, DFINITY Foundation, février 2022.

4. LA BLOCKCHAIN, UNE OPPORTUNITE POUR L'ADMINISTRATION SUISSE ET VAUDOISE ?

Les précédentes sections de ce rapport ont permis de mettre en lumière un certain nombre d'avantages et de promesses de la technologie blockchain (protection et minimisation des données, robustesse et sécurité, etc.). Ces qualités ont encouragé certains pays à expérimenter, voire implémenter, des solutions basées sur cette technologie. Le texte du postulat mentionne d'ailleurs le succès rencontré par l'Estonie, qui propose 99% des prestations de l'Etat sous format numérique et repose précisément sur une infrastructure de type blockchain, nommée KSI (*Keyless Signature Infrastructure*). D'autres pays se sont également profilés vers une identité électronique basée sur une infrastructure de type blockchain, par exemple le Luxembourg ou le Canada.

Au niveau suisse, le potentiel offert par l'essor des infrastructures distribuées est au cœur des réflexions menées par la Confédération sur la possibilité d'instaurer une identité électronique (e-ID). À la suite du rejet en votation populaire de la Loi fédérale sur les services d'identification électronique (LSIE) le 7 mars 2021, six motions de même teneur ont été déposées au Conseil national pour demander une nouvelle solution d'identité électronique, délivrée et gérée par l'État (et non pas par des entreprises privées comme le projet soumis le prévoyait). Le Département fédéral de justice et police (DFJP), en charge de ce dossier, a élaboré un document de travail qui a été ouvert à une 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, un concept ambitieux et innovant qui peut demander de recourir à la technologie blockchain. Le nouveau projet de loi[29] a été mis en consultation jusqu'au 20 octobre 2022.

4.1 Présentation du modèle d'identité auto-souveraine

Le concept d'identité auto-souveraine (en anglais *self-sovereign identity* et souvent abrégé SSI) décrit un modèle technologique dans lequel l'utilisateur possède un portefeuille virtuel (*wallet*), comportant des preuves d'identité similaires à celles qu'il pourrait détenir dans son portefeuille physique. L'objectif poursuivi consiste à offrir une plus grande maîtrise à l'utilisateur sur ses données.

Concrètement, le fonctionnement de ce modèle peut être résumé avec le schéma ci-dessous[30]. En prenant l'exemple de l'émission d'une pièce d'identité virtuelle, la Confédération endosse le rôle d'émetteur (*issuer*). Après vérification des attributs (nom, prénom, date de naissance, etc.), elle va procéder à deux démarches. D'une part, elle inscrit dans un registre (*registry*) qu'elle a contrôlé et qu'elle valide l'identité soumise. D'autre part, elle fournit à l'utilisateur (*holder*) le moyen de vérifier ces données dans le registre. L'utilisateur conserve cette preuve dans son portefeuille virtuel (*wallet*). Lors d'un contrôle, il lui suffira de présenter la preuve au vérificateur (*verifier*), qui procédera à la vérification dans le registre.

Ce schéma met en évidence deux éléments primordiaux pour construire un modèle d'identité auto-souveraine : le portefeuille virtuel et le registre. Le portefeuille virtuel vise à contenir les preuves numériques d'une personne et lui offre une meilleure maîtrise de ses données. À partir de son portefeuille virtuel, cette personne pourra ainsi visualiser ses données et décider lesquelles partager, à qui et pour combien de temps. Dans ce sens, le portefeuille virtuel doit être suffisamment sécurisé pour protéger de manière adéquate les données de la personne, mais également assez simple à utiliser pour être largement adopté au sein de la population. Le registre, quant à lui, doit présenter un haut degré de sécurité afin de préserver les preuves numériques qui y seront contenues tout en étant décentralisé afin de répondre à la volonté de désintermédier la relation entre l'émetteur de la preuve numérique et le vérificateur. Ces exigences rappellent les caractéristiques de la blockchain, raison pour laquelle certains projets de SSI font appel à cette technologie.

[29] E-ID : le Conseil fédéral ouvre la consultation, Publication du Département fédéral de justice et police (DFJP), 29.06.2022.
[30] Ce schéma provient du document de travail concernant le projet d'identité électronique (e-ID) (p.19), publié par l'Office fédéral de la justice le 15.09.2021.

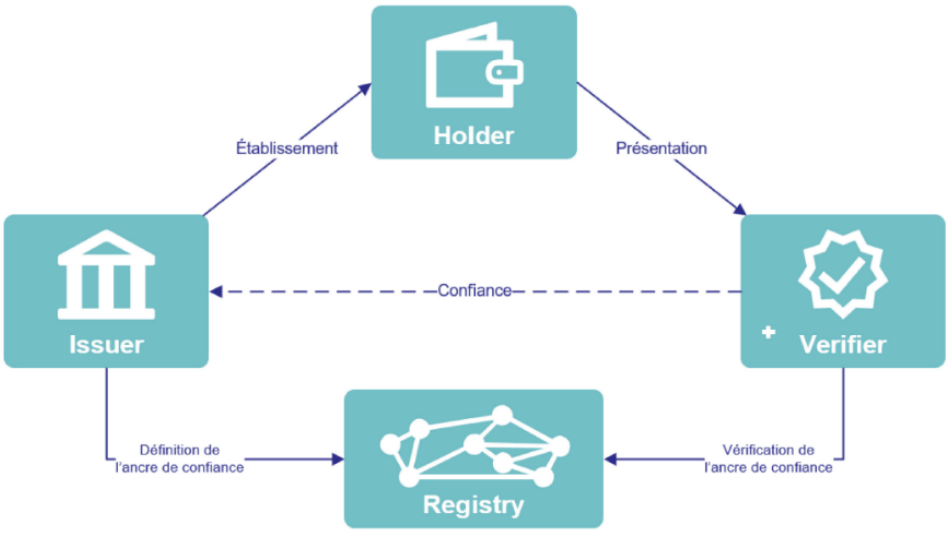


Figure 3- Architecture de base de la SSI présentée par la Confédération

4.2 Proposition vaudoise

Dans sa Stratégie numérique adoptée en 2018, le Conseil d'État a consacré trois principes forts : la souveraineté, la sécurité et la solidarité (prévenir et réduire la fracture numérique). Le modèle SSI permettrait de répondre positivement à ces trois principes dans le domaine de l'identité électronique, comme présenté ci-dessus. L'Etat a ainsi souhaité s'investir dans les réflexions actuellement en place au niveau national et travaille sur l'élaboration d'un PoC (*Proof of Concept*), dont l'objectif vise à évaluer ainsi qu'à éprouver le modèle SSI au travers d'une application concrète.

La prestation sélectionnée pour l'expérimentation est celle de l'extrait de l'office des poursuites. Délivrée par l'État de Vaud mais utilisée auprès d'autres organismes (banques, régies immobilières, concessionnaires automobiles, etc.), cette prestation répond à l'ambition portée par le modèle SSI et la Confédération d'offrir une solution compatible entre les autorités publiques et les entités privées. Par ailleurs, le Conseil d'État souligne dans sa Stratégie numérique l'importance d'assurer la protection des hommes et des femmes qui vivent sur le territoire d'une utilisation abusive de leurs données personnelles. Dans ce domaine, l'extrait de l'office des poursuites tel que fourni actuellement présente des limites pour lesquelles le développement du concept SSI présente des pistes intéressantes.

Prenons l'exemple d'une recherche de location d'appartements par un particulier : ce dernier dépose généralement plusieurs dossiers, et donc plusieurs exemplaires de son extrait du registre des poursuites, avant de se voir proposer un contrat de location. Actuellement, les régies s'engagent à supprimer les dossiers non retenus dans un délai raisonnable. Cependant, cette mesure n'est pas suffisante pour se prémunir contre des pratiques frauduleuses. En septembre 2021, le journal 24 heures[31] révélait un cas d'usurpation d'identité par ce biais, avec des conséquences qui auraient pu être dramatiques pour la victime.

Dans ce contexte, le concept SSI peut contribuer à améliorer la situation pour la population en offrant à l'utilisateur une meilleure maîtrise sur ses données. Alors que l'utilisateur n'a jusqu'à présent qu'un rôle d'intermédiaire entre l'entité émettrice (ici l'État) et le destinataire (ici une gérance immobilière), le développement d'un extrait de l'office des poursuites sur le modèle SSI lui permettrait d'obtenir un rôle actif dans cette relation. D'abord il pourrait s'assurer que ses données ne sont accessibles qu'aux régies autorisées. En effet, les droits d'accès sont nominatifs, ce qui permet de réduire le risque que les données ne soient transférées sans le consentement de l'utilisateur, comme cela peut être le cas avec un document PDF, même signé numériquement (selon la LSCSE[32]), ou une photocopie d'un document signé à la main. Ensuite, il pourrait restreindre les données communiquées aux seules informations nécessaires, car le modèle SSI prévoit de minimiser les données transmises dans une perspective de protection des données. En restreignant les données fournies, il devient plus compliqué de collecter et d'utiliser les données à d'autres fins qu'à celles prévues. Enfin, après avoir obtenu un contrat de location,

[31] « Victime d'usurpation d'identité : « Je me suis sentie violée » », Article du 24 heures, 14.09.2021.
[32] Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques, du 18 mars 2016.

l'utilisateur pourrait révoquer les droits d'accès à son extrait de l'office des poursuites pour les autres régies auprès desquelles il avait déposé un dossier.

Si le modèle SSI promet des avantages indéniables, cette approche est relativement récente et nécessite d'approfondir l'étude des questions techniques pour mettre en place une telle infrastructure. C'est dans ce cadre que l'Etat souhaite développer un PoC. Pour cela, la DGNSI a rencontré plusieurs fournisseurs suisses disposant d'expérience dans ce domaine et prêts à collaborer dans cette direction. Le but du PoC ne se limite toutefois pas à intégrer une solution clé en main au sein de la DGNSI, mais à se confronter aux questions techniques[33] que peut amener la mise en place d'un tel modèle. Ainsi, le PoC servira tant à alimenter la réflexion générale sur l'identité électronique que sur une montée en compétences à l'interne de la DGNSI sur des technologies innovantes qui pourraient se généraliser.

Par ailleurs, l'intérêt d'un dispositif de type auto-souverain pour la cyberadministration est multiple :

- Pour la Confédération et le Canton de Vaud, l'intérêt est de collaborer et déterminer la manière dont un écosystème de preuves numériques (principalement du Canton) pourrait interagir avec l'eID (de la confédération) :
    - Démontrer la faisabilité d'une eID étatique sous forme de preuve numérique auto-souveraine utilisable pour une démarche administrative.
    - Démontrer l'utilisation de cet eID pour délivrer une preuve réglementée par l'Etat (Ex. l'extrait du registre des poursuites).
    - Démontrer l'utilisation d'une preuve réglementée par l'Etat dans le cadre d'une démarche des usagers avec l'économie (Ex. faire un contrat de leasing).
- Pour la Canton de Vaud, la mise en œuvre de cette initiative permet d'étudier les impacts d'intégration de la future eID fédérale sur son système de gestion des identités et de production de preuve numériques.

Le PoC vise à produire des premiers résultats fin 2022, et un rapport finalisé au premier trimestre 2023.

[33] Si le PoC se concentre sur les questions techniques, cela n'exclut pas la prise en considération des enjeux juridiques, économiques, politiques et sociaux liés à l'identité autogérée. Le caractère exploratoire du PoC permettra en effet de préciser le périmètre d'action dans ces domaines.

5. CONCLUSION ET REPONSE DU CONSEIL D'ETAT

Ce rapport a permis de mettre en lumière l'ambivalence de la technologie blockchain et de son utilisation par l'Etat. D'un côté, la technologie permet des apports intéressants : en tant que base de données réputée infalsifiable, elle permet de garantir la protection des informations détenues, en particulier les données personnelles. Le développement de la blockchain a également permis le déploiement d'applications inédites, comme les contrats autonomes, avec la promesse d'un système moins intrusif grâce à une minimisation de la collecte de données. Les individus seraient ainsi en mesure d'avoir une meilleure maîtrise de leurs données tout en évoluant plus librement dans une société de plus en plus numérisée. Enfin, la blockchain apparaît comme une opportunité pour améliorer l'interopérabilité entre plusieurs acteurs, publics comme privés, qui conserveraient la souveraineté sur leurs choix de solutions informatiques.

D'un autre côté, certaines caractéristiques de la blockchain interrogent sur son adéquation avec le rôle de l'État, et son impact écologique. Les modèles d'organisation parfois proposés par la blockchain peuvent avoir pour conséquence des choix intéressés qui ne servent pas forcément l'entier de la population, à l'encontre d'un système démocratique.

Aujourd'hui, la DGNSI poursuit sa veille attentive autour des développements liés à la blockchain, comme le démontre le projet d'innovation autour de l'identité électronique (PoC) présenté dans ce rapport et en cours au sein de la DGNSI. Orienté vers l'objectif de fournir aux usagers une meilleure maîtrise de leurs données, ce projet permet d'évaluer, parmi d'autres solutions, la technologie blockchain. Il a également permis de mettre en place un partenariat avec une entreprise active dans le domaine de la blockchain et plus spécifiquement de l'identité numérique auto-souveraine (SSI) et membre du pôle de compétences TrustValley qui promeut l'expertise de la région lémanique en matière de confiance numérique. Cette approche globale présente l'avantage de faire monter en compétences les collaborateurs et collaboratrices de la DGNSI et d'évaluer à partir d'un cas concret la plus-value réelle de la blockchain et les enjeux qu'elle pose au sein de l'infrastructure du Canton, tout en renforçant les échanges avec le secteur privé et en promouvant l'innovation numérique et l'utilisation de nouvelles technologies au sein de l'administration cantonale.

Le Conseil d'Etat constate que le panorama de la blockchain présenté dans ce rapport montre que cette technologie ne doit être utilisée que lorsqu'une pesée d'intérêts justifie sa mise en œuvre et explique la prudence dont il fait preuve. Ainsi, le choix d'une solution informatique doit être motivé par les objectifs à atteindre et non pas par la technologie utilisée. Au final, le Conseil d'Etat rappelle qu'il a chargé la DGNSI de ce travail régulier de veille technologique. La DGNSI appréhende régulièrement, par des projets d'innovation divers, les nouvelles technologies émergentes afin de constater – ou non – leur adéquation avec le système d'information cantonal et la stratégie numérique du Conseil d'Etat. En ce sens, la technologie blockchain, actuellement en phase de test, sera mise en œuvre lorsque les conditions pour son déploiement optimal seront réunies.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 5 avril 2023.

La présidente :	Le chancelier :
C. Luisier Brodard	*A. Buffat*