PROSPECTIF

NOTE DE VEILLE

www.vd.ch/statvd

Décembre 2023

canton de vaud

STATISTIQUE VAUD

Département des finances
et de l'agriculture (DFA)

BLOCKCHAIN, LES NOUVEAUX REGISTRES PARTAGÉS

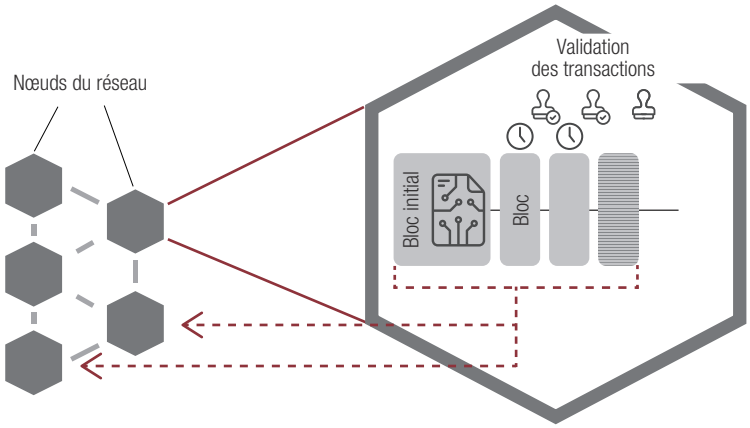
Depuis l'avènement du Web 2.0, l'utilisateur ne se limite plus à la simple consommation de pages web mais participe à la création et la diffusion de contenu. Ce Web 2.0 est également marqué par la concentration de ces outils entre les mains d'un nombre limité d'acteurs dominants (les GAFAM soit les géants du web que sont Google, Apple, Facebook, Amazon et Microsoft). Cette prépondérance des GAFAM est remise en cause avec l'arrivée du Web 3.0 qui se veut décentralisé et centré sur un autocontrôle des données personnelles. L'une des technologies structurantes de ce dernier est celle de la «blockchain» et des registres partagés. Cette note de veille vise à présenter les principes fondateurs de ce type de protocole informatique ainsi qu'à en illustrer les axes de développement possibles pour le canton de Vaud.

L'objectif de cette note de veille sur la blockchain, ou «chaînes de blocs», est de mieux faire connaître cette technologie émergente et de faire un premier état des lieux de ses usages possibles. En effet, cette technologie des «chaînes de blocs» est principalement connue pour être sous-jacente à de nombreuses cryptomonnaies. Néanmoins, ces protocoles informatiques peuvent être utilisés dans divers domaines et ne sont pas cantonnés à la finance. Les blockchains proposent ainsi un grand nombre d'applications émettrices de «contrats intelligents» ou *smart contracts* (voir p. 5) permettant de stocker et de transmettre des informations de façon immuable et transparente. Ces propriétés permettent une utilisation très variée de la technologie de la blockchain, de la traçabilité des marchandises à l'identité électronique des citoyens pour l'administration en passant par la cryptomonnaie, pour ne citer que ces domaines. Etant donné ce potentiel et le positionnement innovant du tissu économique et académique vaudois, cette technologie pourrait se développer de manière plus ou moins importante sur le territoire cantonal.

Sommaire

Après une description succincte des caractéristiques de cette nouvelle technologie, cette note présente des domaines économiques dans lesquels cette technologie pourrait se diffuser dans le canton. La dernière section est consacrée aux atouts du canton pour le développement des technologies des registres partagés ainsi qu'à l'impact environnemental de ces dernières.

[F1] REPRÉSENTATION D'UNE BLOCKCHAIN



Après la validation du nouveau bloc, ce dernier est ajouté à la blockchain. Cette nouvelle «version» de blockchain est dupliquée à chaque nœud.

Encadré 1 **Vocabulaire de blockchain**

Réseau blockchain
La technologie de la blockchain s'appuie sur une structuration du réseau non plus centralisé et linéaire mais sur un réseau décentralisé pair à pair, constitué de nœuds.

Nœud
Chaque nœud représente un utilisateur qui possède une copie actualisée de la chaîne.

Protocole de consensus
Le protocole de consensus définit les conditions d'entrée des acteurs sur la chaîne et les modalités de leur participation.
Il est définit par le code exécuté par les nœuds du réseau.

« Genesis Block »
Chaque blockchain commence avec un bloc initial, le « genesis block ».

Bloc
Chaque bloc est lié au précédent et contient la ou les nouvelle(s) transaction(s).

Horodatage
En horodatant chaque bloc et en répliquant l'intégralité de la blockchain à l'ensemble des nœuds du réseau, chacun peut vérifier la date des transactions et retrouver le nœud écrivain du bloc.

Validation / Minage
Le minage est une opération consistant à valider une transaction en cryptant les données et en les enregistrant sur la blockchain.
Dans le cadre des cryptomonnaies, ces « mineurs » sont rémunérés par des jetons constitutifs de la blockchain.

Clés publiques / Clés privées
Pour garantir les transactions, les utilisateurs de chaque blockchain « apposent » leur signature numérique. La clé privée de l'utilisateur permet d'effectuer des transactions ; et sa clé publique permet aux autres utilisateurs ou nœuds, de vérifier ces transactions. Cette signature numérique garantit l'immuabilité des données ainsi que l'identité de l'utilisateur.

DÉFINITIONS

La blockchain est une technologie de stockage et de transmission d'informations et de transactions fonctionnant selon un principe de décentralisation. Elle agit, de manière schématisée, comme un registre papier permettant de suivre les transactions ayant lieu entre les différents participants à un réseau, par exemple pour consigner les emprunts de livres au sein d'une bibliothèque. Chaque mouvement de livre est noté, validé par un bibliothécaire et son parcours peut être suivi dans le temps par tous les membres. Dans le cas de la blockchain, les données de ces registres sont répliquées, distribuées, partagées (ou *distributed ledgers*), cryptées et structurées en blocs liés les uns aux autres, à intervalles de temps réguliers **[Encadré 1]**. Chaque bloc enregistre une ou plusieurs transactions, puis est validé par l'un des nœuds du réseau **[F1]** selon un protocole de consensus qui en définit le processus de preuve retenu dans la blockchain **[Encadré 4]**. L'intérêt premier de cette technologie réside dans l'immuabilité des données qu'elle contient. En effet, le fonctionnement même du cryptage, du hachage, ou « empreinte numérique », et de l'horodatage des blocs certifient l'authentification des données. Avec le partage à tous les utilisateurs de l'ensemble de la chaîne de blocs, soit la transparence des données, c'est la définition même de la confiance qui est au cœur de cette technologie.

Ce faisant, le « tiers de confiance », élément indispensable pour la mise en œuvre d'un contrat entre acteurs, n'existe plus en tant que tel mais se retrouve partagé par la validation de tous et la transparence de l'évolution de la chaîne de blocs. Cette immuabilité et cette transparence des données partagées permettent des utilisations très variées de cette technologie de la blockchain.

Nonobstant les qualités techniques de ces technologies, certains acteurs économiques soulignent souvent la **lourdeur du processus de mise en œuvre**. Pour répondre à cette difficulté, certaines sociétés notamment vaudoises développent des instruments informatiques ayant une base, appelée sous-couche, en blockchain sans pour autant que le registre partagé soit intégralement développé sous cette technologie unique. De tels produits permettent ainsi de maintenir les atouts majeurs de la blockchain sans pâtir de la lourdeur de sa mise en œuvre et ainsi favoriser son déploiement dans les divers domaines économiques.

DOMAINES DE DIFFUSION

L'utilisation la plus connue de la blockchain est aujourd'hui encore la création de **cryptomonnaies**. Pour autant, cette technologie trouve des applications dans de nombreux domaines, tels que l'e-administration, la santé, l'énergie ou encore de nombreux services. Cette partie présente des domaines de diffusion possibles dans le canton de Vaud, sans prétendre à l'exhaustivité, ou la priorisation de ces domaines.

CRYPTOMONNAIES

Le grand public assimile très souvent blockchain et cryptomonnaie. Ce raccourci trouve son origine dans la notoriété des monnaies virtuelles, telles que le Bitcoin ou l'Ether, qui s'appuient effectivement sur cette technologie.

L'une des caractéristiques de ce nouveau marché financier est que les **intermédiaires traditionnels** tels que les banques centrales et les banques commerciales sont des acteurs marginaux de ce système. Cet **écosystème particulièrement libéral** où la régulation se fait par le marché est extrêmement volatile [F2].

NE PAS CONFONDRE BLOCKCHAIN ET CRYPTOMONNAIES

Cette **volatilité, couplée à une croissance importante,** a incité les Etats à établir des règles. Tout en souhaitant limiter l'intervention étatique sur ce nouveau marché économique, la Suisse a également mis en place des mesures régulatrices et appréhende ces nouvelles monnaies virtuelles comme des « monnaies étrangères ». Le **Conseil fédéral et la FINMA**[1] ont ainsi fait le choix d'encadrer a minima la spéculation autour des cryptomonnaies avec **comme objectif principal d'éviter le blanchiment d'argent** et le financement des groupes délinquants. Fidèles à leurs principes libéraux, la Confédération, tout comme le canton de Vaud ont décidé de ne pas imposer les revenus liés aux cryptomonnaies, à partir du moment où ces derniers ne correspondent pas à une activité professionnelle indépendante.

En comparaison, la France voisine impose à 30% les plus-values réalisées sur les cryptomonnaies (on parle de « flat tax »). Au-delà d'un **cadre fiscal favorable**, la Suisse et plus encore certains cantons ont saisi l'opportunité de ces nouvelles technologies et de ces nouveaux domaines économiques. Le canton de Zoug offre ainsi, depuis 2016, la possibilité aux citoyens de payer les services publics ou encore leurs impôts (à hauteur maximale de 100 000 francs) en cryptomonnaies. Pour les autorités locales, il s'agissait principalement de soutenir ces innovations et de démontrer l'intérêt de leur territoire pour ces nouvelles activités économiques. Or, la couverture médiatique d'un tel choix politique est bien plus grande que l'utilisation effective de ce nouveau service à la population. En plus de ce soutien politique, l'arrivée dans la commune de la fondation Ethereum, qui est le protocole informatique de l'actuelle seconde cryptomonnaie mondiale, est venue structurer ce nouvel écosystème zougois.

[F2] COURS DU BITCOIN

E-ADMINISTRATION

L'Etat de Vaud peut également jouer le rôle d'exemple pour le développement de l'utilisation de la blockchain et des registres partagés. A titre illustratif, l'administration pourrait s'appuyer sur cette technologie pour la création d'une identité numérique pour chaque Vaudois·e contribuant ainsi au déploiement de l'e-administration. Un projet pilote pourrait consister à utiliser une identité numérique basée sur une technologie blockchain pour l'extrait de l'Office des poursuites. L'Etat de Vaud délivrerait toujours cet extrait au citoyen qui pourrait en donner l'accès de manière sécurisée et maîtrisée, par exemple, aux régies immobilières. L'utilisation de cet extrait par un tiers pourrait être ainsi limitée dans le temps par le citoyen lui-même afin de garantir la protection de ses données (Conseil d'Etat, 2023).

La mise en place d'une **identité numérique sécurisée** s'appuyant sur la blockchain apparaît comme l'un des axes prometteurs de diffusion. Une telle identité numérique offre non seulement aux citoyens un **accès facilité aux services administratifs** mais permet également un **gain de temps** pour les agents de l'Etat dans le **traitement des données**.

En partageant le même registre entre les différents services, l'administration peut accroître son efficacité dans la gestion des dossiers des administrés et **communiquer plus aisément entre les services**. En effet, l'usage de ces protocoles informatiques permettrait de réunir toutes les opérations concernant un même usager, de les partager entre les ayants droits, tout en garantissant la sécurité de ces données.

La population suisse semble favorable à ce type d'innovation. En effet, si le peuple a refusé la loi sur l'identité numérique en 2021 (Loi fédérale sur les services d'identification électronique (LSIE, FF 2019 6227), le 07.03.2021), pour de nombreux observateurs c'est principalement en raison de la création de cette identité numérique par des acteurs privés. A la suite de ces résultats, le Conseil fédéral propose une nouvelle loi sur l'e-ID dont la mise en consultation a eu lieu en 2022. Fin 2023, le Conseil fédéral devrait rédiger le message concernant la loi sur l'e-ID. La mise en place d'une telle identité numérique offre de nombreuses possibilités tant pour le citoyen avec une simplification des démarches que pour l'administration en termes notamment d'efficience, **voire d'économie, avec une diminution des coûts de traitement des dossiers**. De plus, la Suisse serait ainsi en accord avec ses voisins européens puisque la Commission Européenne cherche à modifier son règlement du e-IDAS et à créer un cadre juridique pour l'identité numérique européenne (EUid).

L'établissement d'une identité numérique sécurisée et auto-souveraine peut également apparaître comme une technologie d'**appui pour l'administration fiscale** notamment. Dans une optique de coordination, d'interopérabilité et de déploiement du numérique à l'ensemble de l'administration publique, le Conseil fédéral et les gouvernements cantonaux ont créés l'Administration numérique suisse qui est opérationnelle depuis le 1er janvier 2022.

Avec le déploiement de la blockchain comme support à l'e-administration, le citoyen ne renseignerait qu'une seule fois les informations liées à son identité numérique (principe du « once only »), les informations étant distribuées automatiquement entre les services.

Dès lors, la mise en place de cette identité numérique appellerait une réflexion de l'administration cantonale sur l'usage des données personnelles des citoyens récoltées, en se conformant au cadre légal (notamment la Loi sur la protection des données personnelles). Quelles données peuvent être transmises à quels services ?

Encadré 2 Blockchain publique versus blockchain privée

Dans une **blockchain publique**, tout un chacun peut y participer et devenir un nœud du réseau. Exemple: le Bitcoin. Très majoritairement, le processus de consentement s'appuie sur une **preuve de travail** ou *proof of work*.

Sur les **blockchains privées**, il existe un ou plusieurs régulateurs qui vérifient l'approbation des nouveaux membres et leur accordent des autorisations de lecture et d'écriture. Très majoritairement le processus de consentement ne demande plus des preuves de travail mais des **preuves d'engagement** (ou *proof of Stake*) voire des **preuves d'autorité** (ou *proof of Authority*).

Une telle identité numérique devrait aussi **répondre à des normes sécuritaires extrêmement fortes afin de garantir la protection des données personnelles** des citoyens.

Le canton du Jura a ainsi utilisé la technologie développée et éprouvée par l'Estonie, pour certifier une partie de ses documents officiels. En effet, à la suite d'une cyberattaque massive, ce pays a développé une blockchain robuste, la blockchain KSI, permettant le déploiement de son e-administration et offrant ainsi à ses citoyens leurs e-identités et des services facilités avec les différentes administrations.

Au-delà de l'identité numérique, le **registre foncier** peut également apparaître comme un **secteur favorable au déploiement de la blockchain**. La Suède a ainsi fait le choix d'organiser son registre foncier avec cette technologie permettant ainsi de partager un registre avec des données immuables et transparentes.

SERVICES ET CULTURE

Certains acteurs **du luxe** dans les branches de la maroquinerie ou encore de l'horlogerie ont également développé une blockchain garantissant la qualité de leurs produits et limitant de facto le risque de contrefaçon. Le **certificat numérique** lié au produit manufacturé garantit ainsi à l'acheteur la provenance du produit. Un tel procédé de garantie pourrait se déployer à l'ensemble des domaines économiques où la provenance des produits et la lutte contre les contrefaçons sont des enjeux centraux pour les acteurs des branches.

Les services d'offres culturelles peuvent également s'appuyer sur ces nouvelles technologies pour accroître leurs potentiels de vente. Le Paléo Festival Nyon a ainsi expérimenté la vente d'une partie de ses **billets numériques** en utilisant une interface basée sur la **blockchain privée et les contrats intelligents** [Encadrés 2 & 3]. Ce projet pilote a permis non seulement de limiter la fraude à la billetterie, mais également de limiter l'impact du marché de la revente des tickets d'entrée en offrant une vente plus tardive d'une partie de la billetterie grâce notamment à l'automatisation de la validation des transactions. La réussite de ce projet pilote réalisé par un festival international basé dans le canton peut servir de locomotive pour le déploiement de ce type de services par les autres fournisseurs locaux d'offres culturelles.

Une autre branche économique pourrait bénéficier de ces certifications et de la validation automatisée des transactions, celle du **recrutement**. En s'appuyant sur une technologie de type blockchain, des sociétés comme APPII **garantissent aux employeurs les informations transmises par les candidats**. La plateforme genevoise professionals.aero propose un service similaire de ressources humaines, spécialisé sur le marché de l'aérospatial. En garantissant la qualité des données transmises par les acteurs du domaine, la plateforme offre un gain de temps pour les professionnels quant à la vérification des différents documents des candidats-pilotes.

Encadré 3 Contrat intelligent

Un « contrat intelligent » (ou *smart contract*) est un programme informatique que l'on peut lier à une blockchain. Des lignes de scripts peuvent être échangées comme des transactions. **Ce ne sont pas des contrats au sens juridique, mais un code informatique qui facilite, vérifie et applique les contrats pendant les étapes de négociation ou d'exécution**. Par rapport aux programmes traditionnels, les contrats intelligents ont l'avantage de pouvoir profiter des propriétés particulières de la blockchain. Leur exécution est irrémédiable, immuable et leur code est librement vérifiable par les nœuds du réseau.

Sur le même modèle, les registres partagés pourraient être mobilisés pour la diffusion et la vérification des diplômes. Avec l'accroissement et l'encouragement des échanges universitaires, une telle technologie pourrait permettre aux institutions de vérifier facilement les diplômes des étudiants accueillis sur le territoire mais également de valider plus facilement les équivalences entre les institutions.

Le monde de l'art a également été impacté par l'apparition des jetons non fongibles (ou *non fongible token*, NFT). Ces jetons ne sont pas en soi une création artistique mais leur essor est lié aux créations d'art numérique. Ils en certifient la propriété à leur détenteur par l'octroi de jeton de propriété. En 2021, l'œuvre « Everydays: The First 5000 Days ! » de l'artiste américain Beeple, vendue chez Christie's pour 69,3 millions de dollars, est un collage numérique composé de 5000 NFT produits quotidiennement par l'artiste depuis 2007.

LOGISTIQUE ET OBJETS CONNECTÉS

A l'instar des domaines économiques précités, la logistique est également propice au déploiement des registres partagés.

En effet, les entreprises peuvent souhaiter garder une trace de la provenance de leurs fournitures et pour cela s'appuyer sur ces technologies. Migros a ainsi déployé une blockchain pour mieux suivre l'approvisionnement de ses fruits et légumes et ainsi limiter le gaspillage alimentaire (Martin et al., 2021).

De même, **certains négociants en matières premières** ont fait le choix de s'appuyer sur cette technologie, assurant la traçabilité de leurs marchandises à l'international et facilitant également la gestion documentaire de ces transferts, divisant par cinq ce temps de gestion. La plateforme genevoise Covantis regroupant des négociants en produits agricoles a ainsi vu son volume de tonnes métriques transférées bondir à 519 millions de tonnes en 2022, soit une progression de 246% sur une année, démontrant ainsi l'adhésion des acteurs du secteur pour ce type de technologie blockchain[2].

La transparence des données sur une blockchain et l'utilisation de contrats intelligents offrent à cette technologie des possibilités de déploiement importantes. L'utilisation des objets connectés couplés à une blockchain est également un **axe considérable de diffusion de ces registres partagés**. En effet, en s'appuyant sur les objets connectés pour inscrire directement les transactions sur la blockchain, la nécessaire confiance d'une relation économique avec des acteurs ne se connaissant pas est facilitée par ce triptyque: blockchain, objets connectés et contrats intelligents (*smart contracts*). Par exemple, la diffusion de la voiture électrique peut être accompagnée par la blockchain pour configurer les bornes de recharge permettant ainsi un paiement automatique entre le consommateur de la borne de recharge, sa banque et le fournisseur d'électricité. L'automatisation entre les informations transmises par l'objet connecté (ici la borne de recharge), les différents acteurs et les transactions financières en résultant sont réglés via un contrat intelligent.

Un second exemple est celui de la transmission d'informations concernant les conditions de transport d'une marchandise entre l'expéditeur et le consommateur final via un objet de traçage inclus dans le colis.

SANTÉ

Le domaine de la santé apparaît également comme un secteur propice au développement des registres partagés et notamment pour le suivi médical des patients.

En 2017, la Confédération a légiféré en faveur de la création d'un **dossier électronique du patient** (DEP), ayant pour objectif le partage et le suivi de la patientèle par l'ensemble des professionnels de santé. Actuellement, la création d'un tel dossier reste à l'initiative des patients. Pour garantir la maîtrise des données, les **patients ont le choix de déposer les informations concernant leurs parcours médicaux**, leurs traitements et autorisent le cas échéant les professionnels à y avoir accès. En cherchant à promouvoir le DEP et à harmoniser les données transmises et leurs formats, la Confédération a pour **objectif de permettre le partage de l'information médicale entre les différents professionnels de santé intra-, mais également intercantonaux**. Les données médicales sont cependant extrêmement sensibles et doivent être particulièrement protégées afin d'en assurer la confidentialité. Afin de limiter les risques de piratage de ces registres partagés, le DEP fonctionne avec des protocoles proches de ceux d'une blockchain privée **[Encadré 2]**, l'objectif étant de garantir la traçabilité de l'historique des données et de leurs consultations. Avec l'utilisation de clés cryptées, tant pour écrire dans le DEP que pour en lire les informations, ces données sensibles restent davantage protégées contre les cyberattaques.

Encadré 4 Protocoles de consensus et demandes de preuves

Preuve de travail ou *Proof of Work* (PoW)
Dans le cadre des principales cryptomonnaies, les mineurs, pour valider une transaction et ainsi être récompensés, doivent **résoudre une énigme informatique, on parle alors de minage**. Plusieurs mineurs tentent de résoudre l'énigme parallèlement pour obtenir la récompense ; dans le cadre du Bitcoin, un bitcoin (ou une part de ce dernier) est versé au mineur vainqueur. Au fil du temps, les énigmes se complexifient et la récompense attribuée se réduit.

Preuve d'engagement ou *Proof of Stake* (PoS)
La validation des transactions et donc des nouveaux blocs est effectuée par les nœuds pouvant **immobiliser des jetons**. Le nombre de validateurs est limité aux utilisateurs possédant le plus gros capital. Certaines blockchains ont développé des algorithmes permettant aux utilisateurs possédant un nombre de jetons minimal de participer à la validation des blocs et par conséquence d'être récompensés pour cela, via un « tirage au sort ».

Preuve d'autorité ou *Proof of Authority* (PoA)
Dans le cadre d'un consensus basé sur la preuve d'autorité, les transactions et les blocs sont **validés par des comptes (nœuds) approuvés** à l'avance. Un tel système repose donc sur la réputation des détenteurs de ces comptes.

En parallèle, la Confédération a dû accroître les garanties de sûreté de ces registres en proposant leur stockage crypté sur le territoire national. Or, le **territoire vaudois est particulièrement bien doté en datacenters** avec 7 centres de stockage de grande puissance (Avenches, Crissier, Gland, Lausanne, Nyon, Renens et Yverdon-les-Bains) et comprend des projets en développement.

Pour autant, le déploiement du dossier électronique du patient reste complexe. En effet, si les caractéristiques de la blockchain (immuabilité des données et rapidité de transmission, entre autres) sont soulignées par les services en charge de son déploiement, la transparence des données à chacun des nœuds du système apparaît comme un frein potentiel. Pour garantir la confidentialité des données transmises – et la « sélection » des différents nœuds autorisés sur le réseau - une des solutions possibles est la mise en place d'une blockchain privée avec un protocole de consensus appuyé sur une preuve d'autorité **[Encadré 4]**. Celle-ci fait par ailleurs partie des possibilités avancées par le service en charge du déploiement du DEP au niveau national, qui travaille au choix de la technologie numérique la plus efficiente pour cette diffusion.

Dans les faits, les Hôpitaux Universitaires de Genève (HUG) ont d'ores et déjà testé le déploiement d'une application s'appuyant sur une blockchain privée, notamment pour le partage de documents médicaux. A l'instar des objectifs avancés par la Confédération, ce centre hospitalier universitaire souhaite non seulement permettre une meilleure implication des patients dans le suivi de leur parcours médical mais également une communication facilitée entre les soignants.

En s'inspirant de l'expérience des HUG dans ce domaine, le canton de Vaud pourrait jouer un rôle de modèle pour le reste du pays, avec le déploiement précoce de l'identité numérique de ses citoyens, qui pourrait s'appliquer dans le domaine de la santé. Il peut également apparaître comme un incubateur de talents avec des start-ups développant ce type de produits.

Le développement des registres partagés de type blockchain peut également profiter à un autre volet de la santé: **celui de la traçabilité des médicaments.** Quelques start-ups vaudoises ont déjà développé des outils numériques garantissant la qualité des médicaments distribués et évitant ainsi les contrefaçons, dont les conséquences peuvent être dramatiques pour la santé des patients.

La cible de ces start-ups ne se limite pas au territoire national, ni même européen mais se situe principalement au continent africain, qui enregistre plus de 10% de médicaments frauduleux[3]. La mise en place d'un registre partagé offre ainsi aux organismes distributeurs de médicaments la certification de ces derniers, une traçabilité pouvant être immuable et un partage de ces données avec les différents acteurs de la chaîne.

ÉNERGIE

Le **domaine de l'énergie est également l'un des domaines économiques où l'utilisation de la blockchain pourra être importante** et apparaît comme un secteur potentiel de croissance. En effet, le développement des énergies renouvelables tout comme la réduction des émissions de gaz à effet de serre sont des leviers potentiels pour l'implantation de cette technologie dans ce domaine. Allant de l'ajustement des flux entre producteurs et consommateurs (comme pour le projet Quartierstrom dans la ville de Walenstadt à Saint-Gall), à la certification de l'énergie produite (Swytch sécurise et vérifie les données de production d'électricité verte pour les entreprises), en passant par la complémentarité des infrastructures de recharge pour les véhicules électriques (Oslo2Rome prend en compte les différents distributeurs européens), les registres partagés peuvent fluidifier les transactions entre les différents acteurs et limiter le nombre d'intermédiaires. Avec l'utilisation des contrats intelligents, l'automatisation des actions et/ou des transactions peut encore s'accroître. Par exemple, des acteurs

pourraient s'accorder pour limiter automatiquement le chauffage des bâtiments à 20°C.

NE PAS CONFONDRE «SMART CONTRACTS» ET CONTRATS JURIDIQUES

Les blockchains pourraient également être utilisées pour la mise en place de **réseaux intelligents** ou *smart grids*. Ces réseaux intelligents ont pour objectif d'**optimiser la gestion électrique du réseau**. En effet, ces outils permettent de connaître en temps réel la production et la consommation énergétique.

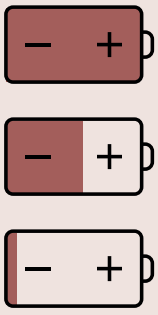
Alors que la transition énergétique passe par un développement massif des énergies renouvelables (Buri & Martin, 2023; Balthasar & Schalcher, 2020) entraînant le développement massif des « prosommateurs », c'est-à-dire les producteurs décentralisés consommant une partie de leur propre production, le réseau électrique risque d'être mis à mal. En effet, ce dernier construit il y a plus de 40 ans est peu adapté aux micromarchés induits par ces nouvelles unités de production électrique. Le développement des réseaux intelligents répond au besoin de gestion du nouveau profil de tension sur le réseau électrique ainsi qu'à la modification de ses flux de charge. Le déploiement de ce type de réseaux **facilite la prise en compte des petits producteurs et des besoins des consommateurs en fonctionnant** sur un système, non plus unidirectionnel, mais bidirectionnel.

Si les réseaux intelligents ne sont pas dépendants de la blockchain, cette dernière offre une rapidité d'exécution entre producteurs-vendeurs et consommateurs-acheteurs avec la mise en place notamment de contrats intelligents. De plus, la transparence sur les données, leur disponibilité ainsi que leur justesse en font l'un des axes de diffusion cantonal possible. Le développement de cette technologie dans le domaine énergétique favoriserait l'émergence des micromarchés. Pour autant, la mise en place de tels réseaux intelligents peut offrir au canton une meilleure lisibilité des besoins énergétiques des différents acteurs du territoire et lui permettre d'adapter sa politique énergétique.

Consommation électrique des blockchains

L'une des critiques les plus répandues concernant les blockchains est leur consommation électrique. S'il est vrai que le Bitcoin est extrêmement consommateur d'électricité avec ses 114 millions de détenteurs de Bitcoins en juin 2021 (*Les Echos*, 2021), on estime sa consommation d'électricité à environ 105 TWh, soit plus de 24 fois la consommation électrique du canton (4,3 TWh en 2021) [F3].

[F3] CONSOMMATION ÉLECTRIQUE DU BITCOIN, DE LA SUISSE ET DU CANTON DE VAUD EN 2021



BITCOIN
105 TWh d'électricité consommée en 2021

SUISSE
58,1 TWh d'électricité consommée en 2021

VAUD
4,3 TWh d'électricité consommée en 2021

Mais en ce qui concerne l'Ether, seconde cryptomonnaie mondiale, sa consommation électrique a diminué de 90%, selon ses fondateurs, en passant d'une preuve de travail (ou *proof of work*) à une preuve d'engagement (ou *proof of stake*).

C'est ainsi le protocole de consensus qui définit la consommation électrique de la blockchain.

La preuve de travail est hautement énergivore car elle impose la résolution d'algorithmes de plus en plus complexes ne pouvant s'effectuer qu'avec des outils informatiques très puissants et un temps de calcul long. C'est ainsi l'activité de minage qui génère une consommation électrique extrêmement importante.

Or la **rentabilité de l'activité de minage**, intimement **corrélée au coût du kWh, d'achat du matériel informatique** ainsi qu'au cours de la cryptomonnaie reste faible en Europe. Dès lors, avec un prix de l'électricité de plus en plus élevé en Europe et en Suisse, l'activité de minage y reste rare.

A l'inverse, les **blockchains privées**, majoritairement mises en place pour l'établissement d'une relation de confiance dans les données partagées, **ne sont pas plus consommatrices d'énergie que des transactions classiques d'autres formes de registres partagés**. C'est d'autant plus vrai dans le cadre d'un protocole de consensus dit de preuve d'autorité (ou *proof of authority*) **comme pour les blockchains mises en place notamment par les administrations**. Le déploiement de cette activité pourrait dès lors s'accroître sur le territoire cantonal, sans augmenter considérablement sa consommation électrique.

CONCLUSION

S'il est difficile aujourd'hui de se prononcer sur la diffusion future de la technologie de la blockchain, **l'intérêt des registres partagés, de l'immuabilité des données transmises, ainsi que la rapidité d'exécution sont des caractéristiques recherchées tant par les entreprises, les administrations[5] que les citoyens**. Avec « 600 start-ups suisses basées sur la technologie blockchain en 2018, soit deux fois plus qu'en 2017, [l'emploi de] 3000 personnes » et un chiffre d'affaires de 44 milliards USD pour les 50 premières entreprises suisses de la blockchain (Innovaud, 2020), le domaine des registres partagés et distribués est un domaine porteur.

Or le canton de Vaud possède un écosystème favorable à ces technologies, notamment au niveau académique avec plusieurs institutions tournées vers les nouvelles technologies et le numérique (EPFL, HES-SO, UNIL). Si des formations spécifiques à la blockchain, notamment des **Certificate of Advanced Studies, dispensées par les HES et soutenues par Crypto Valley Association, commencent à émerger**, celles consacrées à la technologie des registres partagés, à la cryptographie (authentification numérique), ou encore aux outils connectés, sont déjà bien implantées dans le canton. De plus, la transition numérique en cours incite fortement les entreprises, les acteurs parapublics et publics à évoluer dans leurs pratiques professionnelles et à s'appuyer de plus en plus sur des outils numériques (Martin et al., 2021) où ces registres partagés pourraient jouer un rôle important.

Au-delà de favoriser les emplois dans l'accompagnement numérique des entreprises et administrations, la diffusion de cette nouvelle technologie peut également transformer profondément certaines professions bien installées historiquement et n'appartenant pas au domaine du numérique. En effet, au-delà du strict gain de temps proposé par la rapidité d'exécution des contrats intelligents, le déplacement du rôle de « **tiers de confiance** » d'une profession à une technologie informatique pourrait impacter fortement certaines professions, par exemple les notaires et les avocats. Pour autant, **l'arrivée de cette technologie ne signifie pas la disparition de ces professions** mais risque d'entraîner une **réorientation de leurs pratiques** vers leur cœur de métier. Dans le cas des notaires, si aujourd'hui un pan important de leur métier est la validation des transactions entre des tiers, avec la mise en place d'une blockchain et de contrats intelligents, cette délégation de validation est transférée du notaire à la technologie. Néanmoins, l'intégralité des autres aspects de cette profession ne peut pas être déléguée à la technologie, tel que le conseil aux particuliers ou aux entreprises. De même, si la profession d'avocat peut se voir transformée par l'avènement des registres partagés, l'intervention de ces professionnels reste indispensable en cas de litige, les contrats intelligents définissant uniquement les situations fonctionnelles entre les acteurs.

Afin d'anticiper de telles **transformations/évolutions, les autorités et institutions publiques gagneraient à accompagner la mise en place** de formations supérieures initiales et continues ainsi que de l'information citoyenne autour de ces nouvelles technologies, voire en devenir un acteur porteur en l'utilisant dans le cadre de son e-administration.

L'autorité publique **peut d'ores et déjà s'appuyer sur des outils politico-législatifs offrant un cadre favorable au développement de ce type de nouvelles technologies numériques**. Avec une couverture de plus en plus importante en datacenters, le canton de Vaud possède sur son territoire des lieux de stockage de données sensibles des citoyens et entreprises pouvant ainsi garantir aux différents acteurs demandeurs un stockage de proximité et aux mains d'acteurs vaudois ou suisses. De plus, l'adoption d'une Stratégie numérique en 2018, en passant par des outils de promotion économique, notamment via le Service de la promotion de l'économie et de l'innovation (SPEI) facilitent l'essor des start-ups et des PME dans ce secteur. L'agence Innovaud, l'association Crypto Valley ou encore le collectif Trust Valley sont également des leviers importants pour la diffusion de cette technologie, tant par les formations proposées que par leurs connaissances dans ces domaines et leur soutien à cet écosystème émergent.

[1] La FINMA est un organe de surveillance indépendant du marché financier et des assurances. Elle autorise et surveille l'activité des établissements sur ces deux marchés. Elle possède également un rôle de réglementation.

[2] http://covantis.io/covantis-substantially-increases-volume-in-2022/.

[3] Selon l'Organisation mondiale de la santé, au moins 1 médicament sur 10 est une contrefaçon et ce chiffre passe à 1 sur 2 pour les médicaments achetés via Internet.

[4] Aujourd'hui, on ne connaît pas l'identité de Satoshi Nakamoto dont le nom pourrait désigner non pas une seule personne mais un collectif.

[5] Actuellement, la blockchain est en phase de test au sein de l'administration cantonale vaudoise et sera mise en œuvre lorsque les conditions pour son déploiement optimal seront réunies (Conseil d'Etat, 2023).

Un peu d'histoire

En 1991, Stuart Haber et W. Scott Stornetta publient plusieurs articles structurant les bases de la blockchain avec comme problématique centrale, l'horodatage des documents numériques et l'immuabilité des données. En 1994, ces deux acteurs de la cryptographie fondent la société Surety qui sera la première à développer une blockchain. Pour garantir l'immuabilité des données, Haber et Stornetta choisissent de publier la valeur de hachage de leur registre toutes les semaines dans le « New York Times » garantissant ainsi l'immuabilité de cette valeur et la transparence de cette dernière à tous les clients. Cette publication a toujours lieu à l'heure actuelle.

A cette première étape de la conception et mise en œuvre de la blockchain, Adam Back va ajouter l'un des éléments structurant des blockchains publiques, la notion de coût. En mars 1997, il publie son travail sur le hashcash ayant pour objectif la limitation des spams dans les courriels. Son « système d'affranchissement basé sur une collision de hachage partielle » a pour objectif de rendre « coûteux » l'envoi de courriels. Ce programme hashcash a ainsi pour impératif de devoir effectuer un calcul pour pouvoir envoyer un courriel. Ce faisant, cet algorithme qui reste peu coûteux notamment en matière de puissance de calcul, le devient en cas d'envoi massif de courriels. L'objectif d'Adam Back était la lutte contre les courriels indésirables.

Alors que ces avancées datent des années nonantes, il faut attendre 2008 et l'article de Satoshi Nakamoto[4] pour que les dernières difficultés techniques soient levées pour sa mise en œuvre d'une blockchain avec une preuve de travail. Son article décrit le fonctionnement d'un protocole infalsifiable utilisant un réseau pair à pair comme couche technologique d'une nouvelle cryptomonnaie, le Bitcoin, qui sera opérationnel une année après, en 2009.

En 2015, les fondateurs de la plateforme informatique décentralisée Ethereum, parmi lesquels Vitalik Buterin, proposent des applications émettrices de contrats intelligents appuyées sur la technologie de la blockchain. C'est ainsi la confiance entre acteurs basée sur la transparence et l'immuabilité des informations transmises qui est au cœur de cette proposition. Les applications développées sur cette blockchain Ethereum sont de nature variée : « bourses décentralisées », jeux onlines multi-utilisateurs ou encore échange de NFT, de terres virtuelles, vérification d'un marché pour de nouvelles applications numériques avant la levée de fonds, etc.

BIBLIOGRAPHIE

Aït-Kacimi, N. (2021, 31 juillet). Le nombre d'utilisateurs a doublé en six mois. *Les Echos*.

Balthasar, A. & Schalcher, H.R. (2020). Recherche pour l'avenir énergétique de la Suisse. Résumé du Programme national de recherche « Energie ». Comités de direction des Programmes nationaux de recherche « Virage énergétique » (PNR 70) et « Gérer la consommation d'énergie » (PNR 71), Fonds national suisse. URL : https://nfp-energie.ch/fr/projects/1000/

Buri, A. & Martin, M.-J. (2023). *Transition énergétique dans le canton de Vaud à l'horizon 2050*. Lausanne: Statistique Vaud. URL : https://www.vd.ch/themes/etat-droit-finances/transition-energetique-a-lhorizon-2050

Braun-Dubler, N. Gier, H-P. Bulatnikova, T. Langhart, M. Merki, M. Roth, F. Burret, A & Perdrisat, S. (2020). *Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment*. 73/2020. Bern: TA-SWISS.

Colombo L. (2022, 10 mars). Première vente aux enchères de NFT en France. *Les Echos*.

Conseil d'Etat. (2023). *Blockchain: le web 3.0 peut changer les rapports entre l'administration et les administrés.* Rapport du Conseil d'Etat au Grand Conseil sur le Postulat Vassilis Venizelos et consorts (17_POS_017), Adopté par le Conseil d'Etat, Lausanne, 5 avril 2023.

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99-111. URL : https://link.springer.com/article/10.1007/bf00196791

Hug, M. (2017). Un nouvel outil numérique pour la fiabilisation des supply chains: la blockchain. *Annales des Mines - Réalités industrielles*, 3, 106-108. URL : https://doi.org/10.3917/rindu1.173.0106

Innovaud (2020). *Blockchain. Un domaine d'innovation du canton de Vaud*.

Le Figaro. (2021, 12 mars). L'acheteur de l'œuvre numérique à 69,3 millions de dollars se cache derrière le pseudonyme Metakovan. Le Figaro.

Martin, C. Martin, M.-J. Guye, O. & Both J.-F. (2021). *Emploi et transition numérique dans le canton de Vaud*. Lausanne: Statistique Vaud.

OPECST – Office parlementaire d'évaluation des choix scientifiques et technologiques. (Avril 2018). Comprendre les blockchains (chaînes de blocs), Note n° 4, *Les Notes scientifiques de l'Office*: Paris.

Rao A. (2020, 11 février). Accélération de la transition énergétique grâce à la technologie des blockchains. (s. d.). *IFPEN*. URL : https://www.ifpenergiesnouvelles.fr/article/acceleration-transition-energetique-grace-technologie-des-blockchains.

Cette note de veille est publiée sous la responsabilité éditoriale de Statistique Vaud (fin de récolte des données et informations : octobre 2023). Les éventuelles opinions exprimées engagent son auteure et n'ont pas vocation à refléter la position de l'Etat de Vaud.

© Statistique Vaud | Rue de la Paix 6 | 1014 Lausanne | T +41 21 316 29 99 | info.stat@vd.ch | **www.vd.ch/statvd**
Rédaction : Adeline Cherqui, Statistique Vaud | Responsable de publication : Carole Martin, Statistique Vaud | Mise en page : Statistique Vaud