Diplôme national de master

Domaine - sciences humaines et sociales

Mention – sciences de l'information et des bibliothèques

Parcours – archives numériques

Mémoire de recherche / août 2023

La confiance dans les technologies blockchain : vers une solution pour l'archivage électronique ?

Céline Brems

Sous la direction de Laurent Duplouy
Maître de conférence associé – ENSSIB

Remerciements

Je n'aurais pas pu réaliser un tel travail seule. N'oublions donc pas toutes les personnes qui m'ont guidée, aidée et inspirée…

Je souhaite remercier mon directeur de mémoire, Laurent Duplouy, pour ses précieux conseils et son accompagnement tout au long de la rédaction de ce mémoire.

J'exprime toute ma gratitude aux personnes qui ont pris le temps d'échanger avec moi sur le sujet des blockchains : Arnaud Gaudinat, Christian Dubourg, Antoine Meissonnier, Hanane Wahibi et Stéphane Schoffit. Je vous remercie pour votre intérêt dans mon travail de recherche et pour le temps que vous m'avez accordé. Nos échanges furent particulièrement intéressants et ont apportés de nombreuses idées, qui ont permis de se positionner sur cette technologie, au cœur des débats.

Je te remercie Pierre-Olivier pour les relectures de mon mémoire. Merci pour le temps que tu m'as accordé.

J'adresse mes remerciements à ma famille pour leur accompagnement dans toutes mes années d'étude. Votre soutien fut essentiel.

Un grand merci à mes parents pour m'avoir donné l'opportunité de voyager en Suisse et en France pour poursuivre mes études.

Un tout grand merci à mon papa pour ses relectures plus techniques. Ce travail a pu naître grâce à toi, tu as participé à éveiller ma curiosité pour le numérique.

Merci à ma maman pour ses encouragements et les partages d'articles qui ont éveillé mon intérêt face aux technologies émergentes. Je te remercie aussi de m'avoir suggéré ces études, il y a cinq ans maintenant, j'ai fait le bon choix grâce à toi.

Gaël, merci pour ta force d'esprit et ton assurance qui furent mon inspiration tout au long de mes études.

Enfin, le mot de la fin s'adresse à mes fidèles amis belges, suisses et français. Je vous remercie pour votre gentillesse et votre accueil, vous avez rendu mes années d'études mémorables. Je peux à présent les clore et ouvrir un nouveau chapitre.

Résumé : Les technologies blockchain ont rencontré une popularité grandissante avec les cryptomonnaies. Grâce à cela, l'utilisation de la technologie a pu être pensée dans divers domaines. Celui qui nous intéresse étant le monde archivistique. Ces dernières années, la fraude documentaire se fait de plus en plus présente : arnaques, usurpation, vol de données, etc. Les blockchains pourraient aider les archivistes à solidifier les qualités de preuves exercées par les documents : traçabilité, garantie de non-modification et altération quelconque, intégrité, authenticité. Toutefois, l'utilisation des technologies est avant tout un rapport de confiance. Cette valeur est nécessaire pour s'assurer que la technologie soit utilisée. L'objectif de ce mémoire est d'analyser, au moyen d'entretiens avec des professionnels, notre rapport de confiance face à cette technologie souvent complexe et de ce fait, incomprise.

***Descripteurs** : Blockchains ; Confiance numérique ; Société numérique ; Protection de l'information (informatique) ; Traces numériques ; Gestion des documents ; Gestion électronique de documents ; Archivage électronique ; Systèmes d'information ; Technologie de l'information.*

Abstract : Blockchain technologies have seen a lot of fame due to the use of cryptocurrencies. As a result, the use of this technology has been thought in other fields. The one we are going to focus on is its application in the archival field. These last couple of years, documentary fraud has grown stronger : scams, usurpation, data theft, and so on. Blockchains could be put to use in order to help archivists solidify the quality of proof within records : traceability, guarantee of non-modification and alteration, authenticity and integrity. However, making use of any technology calls for a relationship of trust, above all else. This value is needed for the technology to be fully engaged. The aim of this paper is to analyze, through interviews with experts, our relationship of trust in the face of this often complex and therefore misunderstood technology.

***Keywords** : Blockchains, Digital trust ; Digital society ; Protection of information (computing) ; Digital traces; Document management ; Electronic management of documents ; Electronic archiving ; Information system ; Information technology.*

Droits d'auteurs

Sommaire

Sigles et abréviations

ACN : Alliance pour la Confiance Numérique

ADSN : Association pour le Développement du Service Notarial

ANSSI : Agence Nationale de la Sécurité des Systèmes d'information

BDD : Base de données

BC : Blockchain

BCs : Blockchains

Cryptos : Cryptomonnaies

DAO : Decentralized Autonomous Organizations ou Organisation Autonome Décentralisée

ETSI : European Telecommunications Standards Institute

GED : Gestion Electronique de Documents

KYC : Know Your Customer

OWASP : Open Worldwide Application Security Project

POS : Proof of Stake ou Preuve d'Enjeu

PoW : Proof of Work ou Preuve de Travail

RM : Records Management

SAE : Système d'Archivage Electronique

SI : Système Informationnel

SIAF : Service Interministériel des Archives de France

Techno : Technologie

TIC : Technologies de l'Information et de la Communication

INTRODUCTION

L'histoire est semée d'archives qui reflètent la mémoire d'une civilisation. Les guerres, les incidents tels que les inondations et les incendies, ont tous eu des conséquences désastreuses pour les documents d'archives, faisant disparaitre tout un pan de notre histoire. De la destruction de la bibliothèque impériale de Constantinople, à l'incendie de la Library of Congress, sans oublier la destruction massive d'ouvrages sous l'Empire Mongol. Voici quelques-uns des exemples qui furent responsables d'une perte considérable de données à valeur probante (Lafountain, 2022). Ces exemples mettent en avant que l'humanité produit de l'information depuis toujours, c'est pourquoi il est nécessaire de la conserver dans des conditions adéquates.

Par ailleurs, les données vont être exploitées avec les technologies de l'époque. Les supports transportant ces données vont évoluer : les tablettes d'argile en Mésopotamie, le codex à l'époque romaine, les chartriers au Moyen-Age, le célèbre papyrus inventé par les Égyptiens (Dhérent et al., 2009). Les moines copistes du XV^{ème} siècle ont permis d'augmenter la production du volume documentaire (Lumni, 2022). Mais c'est l'invention de l'imprimerie (Lumni, 2022) à Mayence en 1450 qui a permis de gagner du temps de manière considérable : nul besoin d'écrire à la main à présent. L'arrivée du XX^{ième} siècle a été marqué par l'informatique (Kennassiri, 2014). Notre rapport à l'information s'est vu modifié, notamment par rapport aux méthodes de traitement, de stockage et de préservation de celle-ci (Bouzeghoub & Mosseri, 2017). Le XXI^{ième} siècle est représenté par le Web, les technologies émergentes et les objets connectés (Ichbiah, 2023).

Aujourd'hui, les institutions patrimoniales, les entreprises et les organisations gouvernementales ont accès à de nombreuses solutions pour stocker leurs données et en garantir la préservation, cela permet aussi de limiter les risques d'accident. Les technologies ont changé notre manière de vivre et de travailler. Elles se sont insérées dans notre quotidien et dans des secteurs d'activité particuliers. Certains sont même présents dans des domaines où des vies humaines sont en jeu : les transports, la défense, le secteur médical (Caine, 2021). L'émergence du numérique offre des moyens et des méthodes supplémentaires de conservation de l'information. Mais en parallèle, elle engendre aussi un tournant dans la manière avec laquelle nous l'envisageons et la produisons (Bouzeghoub & Mosseri, 2017, p.21).

Une des conséquences est qu'il est à présent aisé d'en créer de nouvelles, ceci a pour effet d'augmenter en masse les données. Il y a de nouveaux besoins et donc de nouvelles demandes. Internet, les réseaux de télécommunication, les objets connectés sont toutes des technologies qui produisent constamment des nouvelles données pour communiquer entre elles ou extraire de l'information (Bouzeghoub & Mosseri, 2017, pp.26-27) : de la collecte de données, à sa transmission, jusqu'au traitement et enfin à son stockage (Cagle, 2015). Chacun de ces cycles va mobiliser certaines technologies capables de traiter les données de nature complexes, mal structurées et en large quantité (Calderan et al., 2015, p.101). Avec le temps, certaines technologies ont disparu comme les tubes à vide utilisés pour le traitement des données et d'autres se font plus rares comme les CD ROM utilisés pour stocker les données (Bouzeghoub & Mosseri, 2017, pp.26-27). Les progrès font aussi apparaitre de nouvelles technologies, avec des services innovants. L'industrie du numérique s'améliore continuellement (Calderan et al., 2015, p.101). Avant de nous

pencher sur l'actuel, revenons sur les progrès qui ont été réalisés par le passé, ceci permettra de comprendre comment nous en sommes arrivés à la modernisation des systèmes informatiques.

En 1971 débute la troisième révolution industrielle qui perdurera jusqu'en 2000 (Leloup, 2017, pp. 181-182). Il s'agit de l'âge de l'information et des télécommunications qui a débuté aux États-Unis. C'est l'emploi de l'informatique avec les télécommunications (Nabi Khan & Unesco, 1987, p.118). Le réseau ARPANET dans les années 1960 est créé par le département de La Défense américain; suivront ensuite le réseau Packet Radio Net qui connecte des ordinateurs mobiles et SATNET qui assure la connexion entre les ordinateurs européens et américains (Rajaraman, 2022). Ces trois réseaux vont être interconnectés en 1973 par le protocole TCP/IP, ceci marquera la naissance d'Internet, moyen de communication inédit (Ronfaut, 2019). L'intensité des échanges est propulsée au niveau mondial, grâce à cette interconnexion de réseaux informatiques (Leloup, 2017, p.181). De nouveaux matériaux révolutionnaires tels que la résine, la céramique et le silicone ont permis de créer cette infrastructure, ainsi que les câbles électriques (FuturaSciences, 2021) (Fanet & Duranton, 2017, pp. 26-27). Viennent ensuite les ordinateurs personnels ou PC, dans les années 70 (Leloup, 2017). Chaque individu peut à présent créer, stocker, diffuser et échanger des données aisément (Brasseur, 2016, p.7). A la fin des années 80, le World Wide Web est créé, il s'agit d'une des applications d'Internet. Par après, l'usage des réseaux sociaux fait un véritable boom au début des années 2000. C'est un tournant dans notre rapport à l'information qui est apparent. Le Web est responsable de la multiplication des données, les réseaux sociaux en sont le produit (Brasseur, 2016, p.8).

C'est un ensemble de fondements informatiques qui a rendu toutes ces évolutions possibles, et qui a fini par former une véritable révolution informatique. Par "révolution" nous entendons que c'est toute notre société et économie qui ont été bouleversées – mais surtout transformées (Bouzeghoub & Mosseri, 2017, pp.22-23). La création de nouvelles technologies nait de la satisfaction des besoins particuliers de cette déferlante de données. Elles sont attendues car elles permettent de répondre à des besoins particuliers (Fanet & Duranton, 2017, pp. 26-27) Par exemple : la sécurité informatique des données; la protection de la vie privée; une transmission plus rapide encore des données; le traitement de jeux de données importants; un stockage plus approprié et sûr; ou encore pour surfer sur la vague verte, une réduction de la consommation énergétique (Chouli et al., 2017, p. 5). Ces exemples mettent en lumière que si une technologie doit être adoptée, il faut avant tout qu'elle réponde à des enjeux précis. La technologie de la blockchain a su répondre à plusieurs de ces besoins. En outre, elle est la suite logique des révolutions technologiques qui ont eu lieu par le passé.

Nous nous situons aujourd'hui dans une transition vers le Web 3.0, c'est toute une émergence de technologies qui forment une sorte de "mise à jour" du Web : les blockchains, les NFTs, les transports autonomes (Azor, 2023). Mais le progrès instaure aussi la peur, le manque de confiance : la 5G est au cœur des débats, l'intelligence artificielle va nous détruire, l'internet des objets va dépasser l'Homme. Or, si nous comparons avec le passé, il est certain que la locomotive à vapeur engendrait aussi un scepticisme. Les citoyens ont certainement mis du temps avant d'oser franchir le pas : peur de la machinerie, perte d'emplois, bouleversements dans

la manière de se déplacer (Caine, 2021). Toutefois, le besoin de voyager plus facilement et rapidement a pris le dessus et a fini par convaincre.

Néanmoins, une myriade de questions vient se poser face aux incertitudes provoquées par ces technologies, comme l'a signalé David Baltimore (s.d.) :

> "*Serons-nous capables de choisir les éléments de la technologie qui améliorent la qualité de vie et d'éviter ceux qui la détériorent ?*"

Dans son ouvrage *Trust in modern societies*, l'autrice Barbara Misztal (1996) reprend que la transformation des sociétés, en se modernisant, engendre une complexification et une globalisation, qui est expliquée par cette caractéristique d'incertitude. Elle ajoute que l'ordre social est impératif à instaurer au sein d'une société ou d'un groupe d'individus. Pour y parvenir, la question de la confiance est nécessaire à instituer dans cet ordre, elle permet de créer des relations sociales entre les individus.

C'est dans cette suite logique de progrès que nous constatons que la blockchain à toute sa place dans la filiation historique technologique retracée plus haut, elle en est d'ailleurs la continuité. Elle a conquis de nombreux marchés, le plus rependu étant celui de la finance (Loignon, 2017, pp. 34-35). D'autres domaines ont aussi été impactés, comme les administrations, les assurances et le secteur médical. Elle a véritablement désarçonné notre économie mondiale en imposant son mode de fonctionnement. Cela va plus loin, car elle est parvenue à rentrer dans nos mœurs et dans nos modes de vie, les cryptomonnaies sont un bon exemple, elles ont prouvé que les citoyens pouvaient lui faire *confiance*. La blockchain, technologie "*trustless*" (De Filippi, 2018) implique plus que jamais cette notion de confiance. Autrement dit, tant que nous avons confiance en elle, nul besoin d'avoir confiance dans d'autres personnes. Alors même que cette confiance a été perdue dans le secteur bancaire, les politiques et les gouvernements. Nous pouvons constater que le facteur social fut donc impacté, tout comme Barbara Misztal (1996), dans son approche sociologique l'avait prédit. Pour reprendre les termes d'Arnaud Péchoux :

> "*La confiance s'appuie sur la technologie. La technologie crée la confiance*" (Leloup, 2017, p. 185)

Et pourtant son histoire reste méconnue, où en tout cas faussée. Qui est en mesure de revenir sur ses origines de création ? Nombreux sont ceux qui répondront en affirmant que la blockchain est née avec l'invention du Bitcoin par l'anonyme Satoshi Nakamoto[1], le 1er novembre 2008 (Bouzeghoub et Mosseri, 2017). D'ailleurs de nombreuses ressources consultées l'affirment, car elles considèrent l'application en pratique de la blockchain. Néanmoins, dans le cadre de ce mémoire, nous avons fait le choix de ne pas remettre tous les honneurs à Satoshi. Nous entendons par là qu'il est plutôt parvenu à utiliser les technologies blockchain pour mettre au point la cryptomonnaie Bitcoin, mais il n'est nullement le créateur de ce système décentralisé (Palop, 2017). Après avoir publié son livre blanc dans lequel il explique le réseau Bitcoin, la blockchain s'est popularisée de manière considérable et l'étendue de ses utilisations s'est développée au-delà des cryptomonnaies (Loignon, 2017, pp.37-39).

L'objectif de Satoshi – et des cryptomonnaies de manière générale – étant d'avoir :

[1] Ou les anonymes, il pourrait y avoir un groupe de personnes derrière ce nom.

"*une monnaie indépendante de toute forme d'autorité, permettant d'effectuer des paiements électroniques dans le monde entier sans le contrôle d'intermédiaires tels que les banques, de manière instantanée et anonyme*" (Pascal, 2022).

Il y a donc une certaine orientation politique libertarienne qui est ici affirmée au travers des monnaies virtuelles (Loignon, 2017, pp.32-33). Satoshi est parvenu à populariser la blockchain et de ce fait, à faire avancer le progrès, les implémentations et les innovations dans le domaine. Mais la technologie avait déjà été pensée et créée, elle a été conçue brique par brique au fil du temps. C'est pourquoi il est important de clarifier l'historicité de la blockchain. Revenir sur ses origines, permet de la démystifier et de comprendre les fondements de cette technologie relativement récente ; *mais l'est-elle seulement ?*

La technologie possède des caractéristiques bien particulières permettant de l'a constituer. Nous allons découper les composantes de la blockchain pour revenir sur l'histoire de chacune d'entre elles. Souvent définie comme étant un système décentralisé, un grand livre distribué, immuable, reposant sur le principe de consensus (Loignon, 2017). Toutes ces caractéristiques ne sont pas nées suite à l'apparition de la blockchain.

Le **chiffrement** prend place aux États-Unis avec le courant de pensée *cypherpunk* vers la fin des années 80. Les débuts d'Internet et la montée vers l'informatisation vont donner naissance à ce mouvement cryptoanarchiste (Quiniou, 2019, p.11). Ils ont avant tout une volonté de protéger leur vie privée, car ils sont conscients que les communications et informations échangées en ligne peuvent être interceptées par n'importe quel individu (Assange, 2016). La volonté du mouvement étant donc de chiffrer les contenus, dans le but d'assurer leur confidentialité. Ils avaient également des aspirations politiques de faire effondrer les gouvernements, c'est pourquoi ils sont aussi qualifiés de rebelles (Hoffman et al., 2020). L'ingénieur cryptographe Timothy C. May a rédigé un manifeste en 1988 au nom du groupe, dans lequel il y écrit :

"*Computer technology is on the verge of providing the ability for individuals […] to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols […] against any tampering. […] These developments will alter completely the nature of government regulation, the ability to […] control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation. […] The technology for this revolution […] has existed in theory for the past decade. The methods are based upon public-key encryption, […], and various software protocols for interaction, authentication, and verification. […]* " (May, 1988)

Nous ne pouvons pas parler de chiffrement, sans revenir sur la **cryptographie**. Celle-ci englobe le chiffrement. Ainsi, dans la cryptographie, nous pouvons également retrouver la fonction de hachage et la signature numérique. La cryptographie décrit donc l'ensemble des moyens permettant de dissimuler les données, autrement dit de les crypter (Commission Nationale de l'Informatique et des Libertés, 2016). Il faut remonter à l'Antiquité pour observer les premiers cas

d'usage de cryptographie (Chouli et al., 2017, p.30). A l'époque, le besoin de conserver des messages secrets était déjà une nécessité, le Code César échangeait des lettres de l'alphabet par d'autres pour camoufler les messages transmis (Babric, 2021). Auparavant décrite comme un art, pour lequel les individus se jouaient de l'écriture (CIGREF, 2013). Elle a ensuite été décrite comme une science suite à son utilisation au XX^{ième} siècle, lors de la Seconde Guerre Mondiale (Chouli et al., 2017, p.30). Le recours et le développement des ordinateurs à permis par la suite de faire progresser cette discipline.

Ensuite, la participation du réseau **en pair-à-pair** (peer-to-peer ou P2P) est également intéressante à analyser. Il s'agit d'un concept qui a été mis au point en 1999, il est donc relativement récent (Lafountain, 2022). Le logiciel Napster permettait d'échanger des fichiers musicaux au format MP3 (Maupu et al., 2019). Ce logiciel d'échange d'internaute vers internaute a rencontré un succès immédiat. Si le droit d'auteur a été violé, d'autres services reposant sur le peer-to-peer ont été déposés sur le marché plus tard (Audureau, 2016). Ce type de réseau aura rendu possible le piratage via le téléchargement de contenus de type films et musique de manière illégale. Les solutions légales de type Spotify, Apple (iTunes) et Netflix verront le jour plus tardivement.

L'utilisation du P2P en bibliothèque a permis d'avoir des copies de sauvegarde pour se prémunir des risques d'inondation, d'incendie, de vols, par exemple (Calderan et al., 2015, p.112). L'ensemble des utilisateurs du réseau sont au même niveau, il n'y a pas de distinction. Tout utilisateur peut être à la fois consommateur potentiel du produit ou du service, mais aussi fournisseur potentiel du service/produit en question (Findlay, 2017, pp. 178-179). Ces derniers ne sont plus dépendants d'une institution : tout un chacun peut avoir l'opportunité de devenir professionnel dans un domaine particulier. Le Bitcoin utilise la technologie du P2P, en outre, le manifeste édificateur de la cryptomonnaie qui a été publié en 2009 s'intitule : "*Bitcoin : a peer-to-peer electronic cash system"* (Quiniou, 2019, pp.3-4). Cette monnaie électronique a pu être en partie développée parce que le réseau en pair-à-pair avait été pensé auparavant.

Le **transfert d'argent** n'est pas né suite aux cryptomonnaies. L'idée avait déjà été pensée plus tôt. En 1976, Milton Friedman a remporté le prix Nobel d'économie, pour lequel il tenait le discours :

> "*Le seul élément manquant, mais qui sera bientôt développé, c'est un système de paiement en liquide fiable. Une méthode permettant de transférer d'une personne A à une personne B, sans que A connaisse forcément B ou que B connaisse A*" (Lewrick & Di Giorgio, 2019, p.21)

Friedman avait vu juste, ses propos résument ce qui est aujourd'hui le concept de cryptomonnaie. Friedman décrit le besoin d'avoir un système fiable, le vocabulaire employé est d'ailleurs intéressant. Nous retrouvons à nouveau une référence à la confiance qui est/doit être accordée dans le système. C'est un principe qui était considéré comme nécessaire en 1976. Et 32 ans après le discours de l'économiste, le Bitcoin venait au monde.

Le cas de l'entreprise Paypal, fondée en 1998 est un autre cas pour lequel il est intéressant de se pencher. Le principe étant de **transférer électroniquement des fonds** au moyen de la carte de crédit. Cette monnaie électronique existait bien avant le Bitcoin (Quiniou, 2019, p.4). Dans la même optique que les cryptomonnaies, Paypal se positionne en tant que concurrent face aux banques (Gentier, 2012). En

effet, Paypal offre une solution simple et moins coûteuse que les systèmes de paiement traditionnels, via sa stratégie "*Kill the Middleman*" (Gentier, 2012) visant à réduire au maximum le nombre d'intermédiaires, ce qui permet de diminuer les coûts de transactions. Paypal tire ses origines du câble transatlantique situé entre Terre Neuve et l'Irlande, en 1866 (Lacoursière, 2007, p.401). Ce câble a permis le transfert d'argent entre New York et Londres, afin de contrer les fluctuations du prix de l'or (p.402). À nouveau, nous constatons que ce sont les révolutions et innovations ayant eu lieu par le passé qui ont ensuite été constamment réinventées et améliorées. L'ensemble de ces innovations nous permet de donner naissance à de nouvelles technologies.

En 2013, la première plateforme en peer-to-peer basée sur la blockchain a été créée pour des applications financières (FuturTech, 2022). Par après, de nouveaux domaines ont adopté la technologie à leur activité tel que la Supply Chain, les smart-contract, les systèmes de paiement (Palop, 2017). Jusque là, les entreprises étaient particulièrement investies dans l'expérimentation et le développement de la blockchain. Mais c'est en 2018 (FuturTech, 2022), qu'il y eut un véritable tournant puisque l'Union Européenne à lancé un projet de recherche *Blockchain for social good* (European Innovation Council, 2018). Ce projet explore les possibilités de la blockchain en vue d'améliorer la transparence et la *confiance* dans le système public. Par la suite, d'autres projets avec les mêmes objectifs ont vu le jour : le vote en ligne, l'éducation, la santé. La blockchain est parvenue à réunir les secteurs publics et privés. Toutefois, ce premier secteur a-t-il réellement eu le choix ? N'a-t-il pas eu d'autres options que de se plier au mouvement afin de suivre le pas et garder la cadence ?

Pour conclure, certains affirment que les BCs, où pour reprendre les termes du journal The Economist (2015) : "*the trust machine*", sont comparables à Internet au niveau de leurs potentiels (Le Ven, 2017). D'autres auteurs (Pascal, 2022) avancent assez audacieusement que la BC est la *quatrième révolution industrielle* à venir. Pour la bonne et simple raison qu'elle répond aux besoins et aux exigences de la société, la variété d'applications qui en sont faites en constitue la preuve même.

Nous avons pu voir que la technologie n'est pas née soudainement, au contraire, elle a été pensée morceau par morceau, avant d'être mise en place. Même si elle n'est pas aussi récente que pensé, il faut tout de même garder à l'esprit que la blockchain reste avant tout une nouvelle technologie en termes d'application, de cas d'usages. Et comme toute (nouvelle) technologie, nous pensons souvent qu'elle sera la réponse à tous nos problèmes, cependant, elle ne guérira pas le cancer. C'est pourquoi si volonté y'a-t-il de l'implémenter dans un domaine particulier, il est crucial de bien l'étudier auparavant. Ceci permettra de définir son potentiel pour les cas d'applications envisagés, mais aussi des effets qu'elle va engendrer, ainsi que sa viabilité ; dans le but de connaitre le degré de confiance que nous avons actuellement dans cette "trust machine".

Ce mémoire s'inscrit dans cette longitude : **les archivistes peuvent-ils réellement avoir confiance dans les blockchains si elles sont utilisées dans un cadre de fortification de la preuve au sein des documents ? Le régime de confiance instauré dans les blockchains est-il seulement existant que pour assurer la fiabilité, la traçabilité et l'authenticité des archives ?**

Nous avons une approche basée sur la confiance, celle-ci étant nécessaire pour que les employés d'une institution puissent conduire leur activité en tirant

pleinement parti des documents. En l'absence de confiance, comment est-ce qu'un processus de travail peut être entrepris ? Il y'a donc un lien intéressant qui se forme entre la profession archivistique et les technologies blockchain, si nous prenons en considération les angles sociaux, politiques, historiques et légaux. Pour cela, nous allons constituer notre analyse sur base de cinq entretiens semi-directifs menés avec des professionnels dans des secteurs particuliers. La littérature de terrain étant cruellement manquante, ces entretiens ont permis d'ajouter une richesse d'informations sur cette technologie qui reste mystérieuse, afin de la démystifier.

Chaque entretien fut adapté à la fonction du professionnel que nous avions face à nous[2]. Chaque interviewé a donc eu des questions personnelles selon sa profession exercée, les projets réalisés, l'utilisation faite (ou non) de la technologie. Nous avons contacté les interviewés via LinkedIn ou le site internet de l'association pour laquelle ils travaillaient ou encore par mail. Nous avons également identifié les interviewés en faisant jouer notre réseau de connexion.

Nous avons inséré une dimension temporelle pour l'ensemble de ce mémoire. La présente introduction est un état des lieux des technologies blockchain, afin d'écouter son passé pour comprendre les rouages de la technologie et donc les raisons de son existence.

Le préambule, ainsi que les parties une et deux nous permettent d'intégrer son présent. Nous avons inséré un préambule, car nous considérons que l'ensemble de ce mémoire ne peut être pleinement assimilé tant que le fonctionnement des BCs (Blockchains) n'ait pas été compris, nous y expliquons l'architecture mécanique de la technologie. Dans la première partie, nous traitons du sujet complexe qu'est la confiance, afin de déterminer ce qu'elle est, comment elle s'instaure et ce qu'elle implique. Dans la seconde partie, nous réalisons un croisement entre la confiance et les BCs, dans le but de déterminer les facteurs qui entrent en compte pour créer un régime de confiance au sein de cette technologie.

Enfin, la troisième partie nous permet de décider de son futur. Nous observons le rapport de l'archiviste face à la technologie. Ainsi que la valeur déterminante qu'il doit détenir pour exercer son activité : la confiance.

[2] Voir Annexe 5 : exemple de la grille d'entretien pour les archivistes, p.88

FONCTIONNEMENT DES BLOCKCHAINS

Stéphane Tual, le fondateur de Slock.it a dit "*[…] tant que ça marche, on ne se pose pas la question sur le comment"* (Loignon, 2017, p.44). Nous allons pourtant procéder de manière opposée pour aborder notre sujet. Nous partons plutôt du principe que :

> "*Pour avoir confiance en quelqu'un, il faut bien entendu le connaître, il en va de même pour les innovations technologiques*" (Caine, 2021).

Les technologies blockchain sont réputées pour être complexes à comprendre à cause de leurs difficultés technique. C'est pourquoi la technologie est considérée comme relativement obscure. La compréhension du fonctionnement mécanique de la blockchain est essentielle pour bien assimiler les enjeux derrière cette technologie. Après tout, comment pouvons-nous accorder notre confiance dans une technologie si nous ne comprenons pas son fonctionnement ? Nous considérons que l'approche descriptive permet de démystifier la blockchain. Il sera par la suite plus aisé de comprendre les aboutissements, les enjeux et les éventuelles défaillances en procédant de la sorte.

C'est la raison pour laquelle nous allons débuter par la description des actions pour parvenir à la création d'un bloc, jusqu'à son rattachement à une chaîne constituée d'un ensemble d'autres blocs, afin d'avoir une première représentation de la technologie.

1. QU'EST-CE QUE LA BLOCKCHAIN ?

Nous allons d'abord reprendre les fondamentaux de la blockchain au moyen de définitions plus élémentaires, sans rentrer dans des détails techniques. Il est possible de définir de deux façons la blockchain.

D'une part, pour ses usages :

> " *[…] la blockchain est une manière sécurisée de faire et d'enregistrer des transactions numériques sans intermédiaire*." (Loignon, 2017, p.44)

Et d'autre part, pour ce qu'elle est :

> *"[…] une* ***base de données*** *distribuée, qui maintient une liste croissante d'enregistrements (blocs), qui sont protégés contre toute révision ou altération non autorisée. Chaque bloc a un lien vers un bloc précédent*." (Ndèla Marone et al., 2021)

Si nous prenons une définition plus courte et synthétique encore, nous obtenons :

> *"[…] un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible."* (Delahaye, [s.d.])

Enfin, la norme européenne NF en ISO 22739 se fait plus précise et déjà légèrement plus technique dans son vocabulaire, tout en restant compréhensible :

"*Registre distribué composé de blocs confirmés organisés en une chaîne séquentielle, à ajout seulement, utilisant des liens cryptographiques*." (Organisation internationale de normalisation (AFNOR), 2022, p.28).

1.1. Principes directeurs

La blockchain est complexe parce qu'elle allie un certain nombre de technologies et de terminologies : stockage au moyen d'algorithmes, partage sur un réseau fonctionnant en pair à pair (peer-to-peer ou P2P), système décentralisé, nœud, hachage, techniques de cryptographie (Mekki, 2020, p.10). C'est d'ailleurs la raison pour laquelle nous avons défini chacune d'entre-elles dans le glossaire[3]. Nous vous invitons à vous y référer avant de débuter la lecture de ce mémoire.

Le principe de sécurité est une notion importante, car elle ne fait plus intervenir une tierce personne ou un organisme (Mekki, 2020, p.10). L'intérêt de la BC réside dans le stockage et l'échange de données dans un environnement sécurisé. Par environnement sécurisé, nous entendons : un moyen de communiquer qui soit inaltérable, dans lequel les données ne pourront être interceptées par un individu non autorisé.

La blockchain, c'est aussi des ressources informatiques, tels que des ordinateurs, qui vont être connectés à la BC (Laurent, 2018). Ils agissent en tant que membres et ils sont mis en réseau via Internet. Ces membres vont être appelés nœuds (ou nodes). Les nœuds correspondent ainsi aux participants du réseau, ce sont eux qui vont contribuer à l'ensemble de sa maintenance et assurer sa sécurité.

Les données présentent dans la chaîne de blocs ne vont pas être stockées sur un serveur central, tel le schéma classique que nous avons l'habitude de croiser (Lewrick & Di Giorgio, 2019, p. 19). L'intérêt de la technologie va être le stockage sur ce réseau distribué d'ordinateurs décentralisés[4]. Tous les participants de ce réseau, c'est-à-dire, toutes les personnes qui vont interagir avec la blockchain, vont avoir la possibilité de copier des parties de la blockchain afin de les sauvegarder localement. C'est d'ailleurs ce qui assure la transparence de la blockchain (Fénéron Plisson, 2017). Les participants peuvent télécharger l'ensemble de la BC et donc en vérifier son intégrité.

Les BC sont souvent reliées aux cryptomonnaies, cette monnaie virtuelle que le Bitcoin à rendu populaire. Toutefois, il faut distinguer ces termes. Premièrement, la BC n'est pas une cryptomonnaie. Bitcoin va utiliser la technologie de la BC pour parvenir à faire des transactions d'argent. D'ailleurs, il serait préférable d'utiliser le terme de "protocole Bitcoin". Blockchain et cryptomonnaies sont donc à bien distinguer. Deuxièmement, l'utilisation de la BC ne se limite pas qu'au transfert d'argent (Lewrick & Di Giorgio, 2019, p.29). Il s'agit d'une application parmi d'autres. Nous reconnaissons trois cas d'usage (Fénéron Plisson, 2017) :

- Il est possible d'envoyer et de recevoir d'autres titres, appelés actifs numériques ou token. Il s'agit du transfert d'actifs comme les cryptomonnaies, des titres de propriété, des actions, etc.

[3] Voir Glossaire, p.91.

[4] Voir Annexe 1 : Système centralisé et décentralisé, p.86.

- Ensuite, la fonction de preuve va jouer un rôle prépondérant. Le fait de pouvoir assurer la traçabilité des actifs permet de prouver leur existence, leur origine de provenance au moyen de l'horodatage.
- Enfin, le smart-contract est le dernier cas. C'est un programme dit intelligent, car autonome dans l'exécution des actions, une fois qu'elles ont été validées par les diverses parties. Sans avoir besoin d'une intervention humaine pour se déclencher.

La blockchain n'est pas une GED (Meissonnier, 2019), elle peut être rapprochée à une BDD informatique, come cité précédemment. D'ailleurs, la blockchain *est* un document, tout comme un registre ou une BDD. Dès lors, il faut comprendre que nous n'allons pas stocker des documents dans les blockchains directement. Stocker tout un document dans la technologie serait même dangereux du fait des principes de droit à l'oubli, de confidentialité, de la destruction des documents, etc (Paltz, s. d.), car un bloc ne peut être modifié, nous reviendrons sur ce principe par après.

Il serait plus correct de dire que les BCs sont une façon de dématérialiser un document. C'est dans la BC que nous allons y stocker des empreintes. Ainsi, la blockchain n'est pas une solution permettant de conserver les documents. Son intérêt et ce sur quoi nous nous intéresserons, sont dans son utilisation pour chaîner, partager, horodater et sécuriser les transactions. Etant donné que la BC est dans son architecture, en mesure de préserver l'intégrité, la fiabilité, la traçabilité, l'authenticité des données. Les questions de traçabilité et d'horodatage sont particulièrement pertinentes avec les documents d'archives.

C'est pourquoi la blockchain peut être modulable pour correspondre à des besoins particuliers (Lewrick & Di Giorgio, 2019, p. 20). Ce qui lui permettra d'acquérir des fonctions spécifiques pour éventuellement atteindre un certain niveau d'automatisation. Comme cité plus haut, c'est le protocole informatique qui va rendre possible cette distinction. Chaque blockchain va ainsi acquérir une application différente. C'est la raison pour laquelle Arnaud Gaudinat (entretien le 07 juin 2023) préfère employer le pluriel. Nous devrions parler des technologies blockchain, car il n'y a pas une seule blockchain en particulier qui existe.

2. LE MECANISME BLOCKCHAIN

La compréhension de son fonctionnement sera plus facile à saisir si nous partons d'une transaction envoyée entre deux personnes[5] pour comprendre le fonctionnement général.

Dans un premier temps, il faut que les parties s'identifient. Ceci se fait au moyen du procédé cryptographique.

Puis, il faut **créer la transaction**, il s'agit d'un échange de valeurs. Prenons Alice qui doit envoyer la transaction à un certain Bob. Pour rappel, les données de la transaction sont des tokens. Ils peuvent représenter des contrats, des informations sur l'identité d'un individu, le hash d'une signature électronique.

Chaque **bloc** constituant la chaîne se compose de transactions qui ont été contrôlées, validées, puis figées par le dispositif (Palop 2017, p.5). Au sein d'un

[5] Voir Annexe 2 : Les blockchains pas à pas, p.86.

bloc, tous les membres peuvent consulter un certain nombre d'informations (agissant comme sorte de métadonnées) relatives à une transaction (Loignon, 2017, p.48) :

- Qui : les pseudonymes accessibles via les clés publiques utilisées (ici Alice et Bob) ;
- Quoi et combien : l'actif transféré, s'il s'agit d'un ether ou d'un bitcoin, alors le montant sera visible ;
- Quand : la date et l'heure précise de l'opération de transfert ;
- Et le bloc en question va, en plus des transactions, avoir un résumé cryptographique (le hash) du bloc précédent, c'est son ADN cryptographique.

La transaction d'Alice va dans un premier temps être inscrite dans un bloc (Palop 2017, p.5). Dans un second temps, ce même bloc va être ajouté à une **chaîne composée de blocs**, à la suite du précédent. Cette chaîne est immuable, incorruptible, ce qui signifie qu'il devient particulièrement difficile de modifier la transaction. Il est souvent repris dans la littérature que ce principe d'immuabilité est un vecteur permettant d'avoir confiance en la technologie. Une manière d'apporter un changement au sein d'un bloc serait que tous les nœuds du réseau s'accordent pour y arriver, autrement dit, la moitié des ressources informatiques doivent le modifier de manière simultanée (Fénéron Plisson, 2017). Ce qui est pratiquement impossible, il faudrait que l'ensemble des participants soient corrompus. De plus, le risque serait que l'ensemble de la chaîne soit invalidée, toute la chaîne en aval deviendrait caduque.

Le schéma ci-dessous représente les propos exprimés pour une meilleure visualisation :

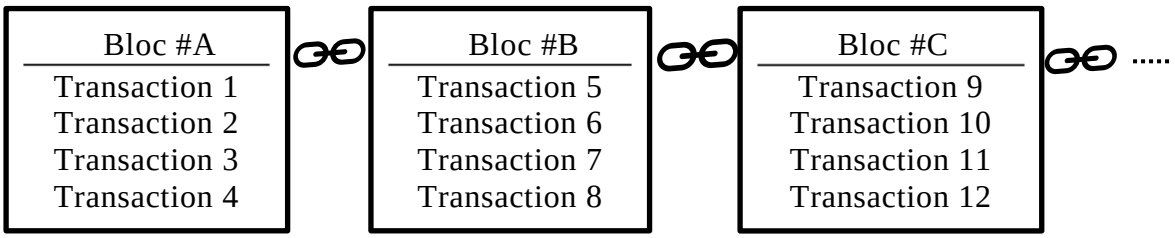


Figure 1 : Chaîne de blocs
Brems, 2023.

Chacune des transactions va utiliser la technologie de **cryptographie asymétrique**, de **fonction de hachage** et l'**arbre de Merkle** (Faure-Muntian et al., 2018), c'est d'ailleurs ce qui garantit l'intégrité et l'authenticité des données (Fénéron Plisson, 2017).

Dans la suite du processus, il y a la **fonction de hachage** qui intervient**.** Le **hash** va accompagner la transaction – tel un message - une fois qu'elle a été enregistrée (Loignon, 2017, pp.61-62). Ce qui permet de garder une trace dès qu'il y a une modification qui intervient. Dans la BC, ce message va être limité en nombre de caractères à 40. C'est pourquoi le document entier ne peut être stocké dans la transaction. D'autant plus qu'un document peut-être relativement volumineux selon son support : vidéo, photo. Alors, nous allons plutôt choisir une preuve de cette information, c'est-à-dire, le hash – l'empreinte digitale cryptée d'un document. C'est donc ce message, ce hash, qui va être stocké sur la BC.

Revenons à notre mise en situation : Alice désire signer électroniquement la transaction qu'elle veut envoyer à Bob[6]. Elle va utiliser sa clé privée qui est une combinaison aléatoire de chiffres (Faure-Muntian et al., 2018). Ceci va créer une deuxième combinaison : la clé publique. C'est la clé privée qui va signer le message. Les autres participants du réseau (ici Bob) peuvent vérifier qu'Alice est bien l'auteur de ce message, uniquement s'ils ont l'accès à la clé publique. En revanche, les participants ne peuvent retrouver l'origine de la clé privée, même s'ils ont connaissance de la clé publique. C'est d'ailleurs la raison pour laquelle elle peut être largement diffusée. En résumé, les membres du réseau sont en mesure de lire la transaction et de procéder à la vérification qu'Alice soit bien à l'origine de l'envoi et en possession de l'actif envoyé. Mais seul Bob, avec sa clé privée, pourra signer sa transaction pour prouver la possession.

La clé publique est donc diffusable, c'est elle qui permet de recevoir les transactions (Faure-Muntian et al., 2018), elle permet de coder le message (Fénéron Plisson, 2017). Tandis que la clé privée, gardée secrète, va permettre d'utiliser la transaction qui vient d'être reçue, elle va décoder le message. Il ne faut donc pas que Bob la perdre. Auquel cas, il ne pourra pas récupérer la transaction qu'Alice a effectuée au moyen de sa clé publique liée (2018).

Le bloc contenant la transaction d'Alice doit être validé. La transaction va donc être transmise au réseau. Il n'y a pas de responsabilité unique s'opérant sur le registre, tous les nœuds du réseau vont intervenir pour la valider ou la refuser (Fénéron Plisson, 2017), c'est le **mécanisme de consensus**, c'est second élément qui apporte toute l'innovation derrière le mécanisme blockchain (Meissonnier, 2019). Lors du processus de validation, les nœuds qui vérifient la transaction sont "les mineurs", cette vérification peut être motivée par une rémunération en crypto-monnaie, ils sont donc les uns contre les autres (Fénéron Plisson, 2017).

Les mineurs vont donc entrer en compétition. Ils vont résoudre un problème mathématique qui permet de valider la transaction. Evidemment, le mineur disposant de l'ordinateur le plus rapide sera avantagé, puisque ce sont les capacités de calcul de la machine des mineurs qui sont mobilisés (p.49). Les mécanismes de consensus[7] peuvent être la preuve de travail (Proof of Work) ou preuve d'enjeu (Proof of Stake), par exemple.

Il s'agit d'un consensus car le registre doit s'accorder avec celui de la majorité des nœuds du système. C'est justement ce consensus qui garantit l'intégrité du livre de comptes. Plus globalement, il s'agit d'une réflexion au moyen d'un consensus sur l'état de la blockchain. Le bloc que le réseau considère le plus légitime car il a une plus grande valeur computationnelle sera validé. En pratique, cette résolution de calcul n'a aucune utilité fondamentale, elle se limite à savoir quel mineur va inscrire le bloc dans la chaîne et à valider les transactions inscrites dans ce bloc (Meissonnier, 2019).

Le rôle des nœuds est de vérifier la véracité de toutes les transactions comprises dans le bloc : Alice possède-t-elle bien la monnaie suffisante, suite à toutes les transactions qu'elle a déjà pu réaliser depuis ? L'envoi à Bob est-il unique ? (Loignon, 2017, pp.48-49).

[6] Voir Annexe 3 : Cryptographie asymétrique, p.87.

[7] Pour notre exemple, nous utilisons le consensus PoW, car il est plus réputé que le PoS. Le fonctionnement de ce dernier est décrit dans le glossaire.

Une fois le problème résolu par un des mineurs, il va transmettre sa solution aux autres, qui vont l'accepter ou la refuser. Dans le cas où elle serait refusée, le processus de résolution se poursuit. Autrement dit, chaque ordinateur teste des solutions jusqu'à parvenir à la bonne. Dans le cas où elle serait acceptée, le bloc est validé, il peut être ajouté au reste de la chaîne, une fois que la majorité des nœuds ont voté pour accepter le nouveau bloc. Naturellement, toutes les transactions au sein de ce bloc doivent être valides.

Les mineurs vont inscrire le hash du bloc venant d'être validé. Une fois inscrit, il y a une garantie de la traçabilité de cette transaction puisqu'elle va être horodatée dans le bloc directement. Les blocs viennent donc confirmer l'heure et la séquence des transactions. Dès qu'un actif numérique se déplace d'un lieu à un autre ou dès qu'il y a changement de propriétaire (biens fonciers), une chaîne de données va se former (IBM, s.d.). L'ordinateur de chacun des participants va ensuite être mis à jour pour correspondre à la nouvelle BC. Les données sont répliquées à travers l'ensemble du réseau et tous les nœuds du réseau vont disposer d'une copie complète de la BC.

Les blocs formant la chaîne vont être reliés entre eux de manière sécurisée, via une empreinte – le hash. Cette mesure rend impossible la modification du bloc ou même une insertion en milieu de chaîne (IBM, s.d.).

Le bloc validé va être visible pour les détenteurs du registre (Faure-Muntian et al., 2018). Enfin, Bob reçoit la transaction d'Alice. Tandis que le mineur gagnant empoche sa récompense.

Notre parcours ne nous permet pas de comprendre l'entièreté du fonctionnement de la BC, ceci n'est pas notre objectif car il y a de trop nombreux algorithmes et solutions informatiques qui sont en jeu derrière la technique. Nous ne sommes pas informaticiens ou mathématiciens. Nous avons compris l'essentiel, c’est-à-dire les technologies qui entrent en compte et quels sont les mécanismes centraux derrière la BC. Nous avons compris le fonctionnement mécanique, ce qui nous permet de maintenir le dialogue sur le sujet lors des entretiens et de percevoir les enjeux derrière cette technologie complexe.

PARTIE 1 : UN REGIME TOURNE VERS LA CONFIANCE

Personne de confiance, société de confiance, tiers de confiance : l'ensemble de ces termes incluent la même notion. Et pourtant, chacun d'entre eux possède une signification différente. C'est pourquoi il est difficile de parvenir à définir la confiance avec une unique définition : "*Est-ce un sentiment, une qualité, une vertu ? Une relation, un choix, une attente ?*" (Laurent, 2009)

La littérature scientifique s'est approprié le sujet, étant donné que de nombreux articles ont été rédigés dans cette thématique. Toutefois, les disciplines scientifiques ne semblent pas adopter le même avis, elles se contredisent, les opinions divergent. Ce qui démontre la complexité de la notion de "confiance".

Les articles ayant une approche *philosophique* adoptent le même point de vue concernant la définition de la confiance. Il s'agit d'un :

> " *[…] état mental dans lequel se trouve un agent A qui, lorsque confronté a un autre agent B sur le point d'accomplir une action, décide de croire que B accomplira l'action d'une manière qui maximisera les bénéfices pour A."* (Palus et al., 2022)

Par le terme *agent,* il est entendu que ce dernier peut être physique ou virtuel (Liothin & Riccio, 2015).

La définition met l'accent sur le fait de tirer quelque chose au moyen de la relation de confiance qui s'est créée entre deux individus. La confiance est donc perçue comme un outil permettant d'atteindre un but précis, un objectif.

Le point de vue *sociologique* inclut la notion de vulnérabilité (Schilke, 2021). Celui qui donne sa confiance, c'est-à-dire l'agent A, expose sa vulnérabilité en donnant sa confiance à l'agent B. L'agent B est en mesure de porter préjudice à A, il se situe en position de force. C'est la relation de confiance qui va laisser penser à A qu'aucun mal ne lui sera fait. La sociologie apprécie donc plutôt l'aspect relationnel qui peut être entretenu entre les individus, mais aussi des institutions (Granovetter, 1994).

Entre ces deux disciplines, la confiance est perçue différemment. Nous comprenons que la confiance n'est pas fixe, elle peut prendre différentes formes : morale, affective, professionnelle (Liothin & Riccio, 2015) ; physique ou morale (Laurent, 2019). La confiance s'exercera différemment dans chacune de ces conditions. Mais la confiance est avant tout un besoin, car elle permet "*[…] de se prémunir contre l'incertitude et la vulnérabilité*" (Fine, 2006). Il s'agit donc d'un moyen permettant de s'assurer qu'un acteur ne nous trompe pas.

La confiance est aussi symbolique : nous choisissons de faire confiance à autrui. Cornu (2003) définit cela comme étant un "*acte de reconnaissance*". Il prend l'exemple de la relation entretenue entre un parent et son enfant. Derrière cette relation, il n'y a pas d'obligation quelconque, l'enfant n'est pas contraint à faire confiance à son parent. L'auteur précise qu'il s'agit d'une forme de confiance, mais qu'il en existe beaucoup d'autres. La confiance ici décrite entre deux êtres institue

un sentiment de non-pouvoir (p.22). Ceci laisse penser que d'autres formes peuvent, à l'inverse, résulter d'une position hiérarchique en fonction de la puissance exercée d'une entité envers une autre.

> "*La confiance se signale par son absence et demeurerait insaisissable quand elle existe*." (Algan & Cahuc, 2007).

Cette citation tirée de l'ouvrage "*La société de défiance"*, décrit que la confiance lorsque, instaurée, n'est pas palpable. Nous ne pouvons donc jamais décrire avec certitude que nous nous situons bel et bien dans un régime de confiance. En revanche, elle se remarque plutôt par son absence. Nous pouvons comprendre par cette citation que nous n'atteignons jamais réellement une confiance absolue ou totale. Celle-ci pourrait être continuellement améliorée et travaillée. Si nous revenons à l'étymologie du mot, la confiance possède un lien avec la racine latine *fides*, autrement dit la *foi* (Cornu, 2003). La confiance fait partie de la foi : c'est un signe de promesse, de loyauté, d'engagement et de franchise (Le Robert, 2022). Cette référence avec la foi admet qu'il faut ajouter une part de croyance (Palus et al., 2022) et de crédulité (Cornu, 2003). Cornu (2003) entend par ces termes, le fait de croire quelqu'un sur parole, sans questionner la véracité des informations transmises. Autrement dit, s'en remettre totalement à quelqu'un d'autre, en fonction du statut hiérarchique supérieur qu'il possède, par exemple. La confiance, alimenterait-elle une amnésie de tout jugement de valeur qui nous est propre ?

Dès lors, il devient intéressant de se pencher sur la définition que le domaine *psychologique* donne à la confiance. En effet, un lien de confiance implique qu'aucun tort ne sera commis à partir d'une telle relation (Palus et al., 2022). La confiance est relative à la personnalité des individus, ainsi qu'à leur comportement (Deutsch, 1958).

Le point de vue *économique* a une approche des bénéfices contre les risques, l'Homme aura donc tendance à mesurer les avantages qui pourront être tirés de la relation (Evans et Krueger, 2009). Cette définition se rapproche de celle donnée pour le domaine *philosophique*.

Enfin, les domaines des *sciences politiques* (Karmis et Rocher, 2018) et des *sciences du management* (Rutter, 2001) présentent des similitudes dans leur approche. La confiance est synonyme de collectivité, de collaboration entre une communauté d'agents. Elle est fondée sur un ensemble de valeurs et de règles instaurées par une autre catégorie d'agents. La confiance repose plutôt sur un jugement collectif.

Revenons sur l'ensemble des définitions provenant des disciplines scientifiques citées précédemment. Selon plusieurs d'entre-elles, la confiance n'est pas établie innocemment, il y a une volonté d'arriver à une certaine fin – qui est connue de la part d'un des agents - en établissant ce contact.

Ensuite, de manière contradictoire, la confiance peut aussi être bienveillante, c'est une conséquence d'une relation qui vient d'être tissée entre des individus.

La confiance, c'est aussi le fait de se placer dans une posture de faiblesse, pour laquelle un des agents viendra se dévoiler. Il est en mesure de le faire, car ce principe de confiance est justement existant.

Enfin, la confiance est le fondement pour l'existence d'une collectivité, elle permet à tous les individus de vivre de manière commune et de parvenir à s'entendre. Elle fournit des normes et des règles permettant de coexister les uns avec les autres.

Chacune de ces disciplines a des opinions plus ou moins divergentes. Nous pouvons en tirer qu'il y a une part de confiance qui est rationnelle, tandis que l'autre tant à être plutôt d'ordre émotionnel (Rousseau *et al*., 1998).

La première est rattachée au fait de connaître la personne au moyen de ses qualifications et de ses compétences dans le but de s'assurer de sa crédibilité, avant d'être en mesure de donner sa confiance à l'autre agent.

La seconde catégorie de confiance est rattachée aux émotions et aux sentiments interpersonnels. La confiance est possible car il y a une croyance que l'autre ne nous trahira pas sur la durée. C'est une relation qui se créée entre une relation affectueuse entre des êtres humains, mais aussi avec des agents inanimés, comme une entreprise avec ses employés, par exemple.

Il existe d'autres définitions permettant de caractériser la confiance. Il est toutefois impossible de les adresser toutes. Nous avons ici une vision d'ensemble permettant de montrer l'étendue de possibilités derrière le terme "confiance". Elle est à la fois perçue comme positive et signe de sincérité. Mais également synonyme de protection des intérêts. La confiance est donc avant tout multidimensionnelle.

À présent que nous avons défini la confiance et délimité son périmètre, il nous reste à savoir : *comment pouvons-nous parvenir à instaurer un tel régime de confiance, finalement ?*

Selon Mucchielli (1995) et Watzlawick *et al.* (1972), la confiance c'est la somme d'échanges et de communication entre individus qui vont petit à petit établir un climat de confiance. Cependant, la confiance ne se limite pas aux Hommes. C'est pourquoi nous allons nous interroger sur la liaison de confiance entre les Hommes et des objets inanimés : les gouvernements, les entreprises, les machines, le numérique.

Ce cheminement nous permettra de comprendre comment nous pouvons avoir confiance dans la technologie de la blockchain, finalement. Ou alors, comment pouvons-nous parvenir à créer un régime de confiance dans le but de l'utiliser pour les documents d'archives.

Ensuite, un second questionnement intervient dans notre réflexion : *peut-on avoir sans cesse confiance ?* Nous avons précédemment vu que la confiance était le fruit d'un travail, elle ne se créée pas d'elle-même, il faut la provoquer. Ceci implique que tout doit, d'une certaine manière, être contrôlé et mesuré. Or, au plus de personnes sont impliquées dans un régime de confiance, au plus il pourrait y avoir des risques d'abus. Cette réflexion sera également placée dans la suite de notre réflexion.

1. LA CONFIANCE EST-ELLE FIABLE ?

Avant de poursuivre, il faut s'interroger sur la fiabilité derrière la confiance. Autrement dit : la "*fiabilité de la confiance"* (Akrout, 2005). Ceci permettra de comprendre les raisons derrière son importance vis à vis des technologies BC, ainsi que les raisons qui poussent à les confronter.

Le dictionnaire *Le Robert* (2023), indique que les synonymes de *fiabilité* sont : crédibilité, sécurité et sûreté. Le dictionnaire de l'Académie française (2019) ajoute que l'étymologie de ce mot est un dérivé de *fiable*, reprit de l'ancien français : *fiableté*, autrement dit : fidélité, confiance.

Fiabilité, confiance, crédibilité et sûreté forment un ensemble. Nous pouvons dès lors constater la proximité de ces termes.

Nous pouvons prendre pour exemple le fait de considérer une personne comme étant fiable (Marzano, 2010). Au fur et à mesure que nous passons du temps avec cette personne, nous allons constater ses qualités, ses compétences, ses valeurs. Ce sont des caractéristiques qui vont amener la confiance. C'est ce qui nous poussera à nous fier à cette personne, c'est-à-dire à compter sur elle. Lorsque le dialogue s'ouvre, l'autre individu se trouvera dans une position qui la motivera à s'engager dans ce processus de confiance réciproque.

Hardin (2006) souligne que confiance et fiabilité ne sont qu'une sorte de passage dans une relation : la confiance instaure la fiabilité. Quéré (2005) complète ces propos :

> "*Si faire confiance c'est croire que quelqu'un est digne de confiance et agir en conséquence, parce que l'on connaît ses intérêts et que l'on sait ce qui le motivera à se montrer digne de confiance ou à être loyal […] il faut pouvoir être en mesure d'évaluer la fiabilité (trustworthiness) et les chances de loyauté de la personne, de se faire une idée de sa manière habituelle de faire face à ses engagements, et de connaître ses motivations et ses intérêts*."

La confiance est un principe qui se forme de manière mutuelle entre des individus qui ont la volonté d'être fiable, grâce au lien qu'ils ont formé ensemble :

> "*La confiance est en réalité directement liée à la fiabilité, car faire confiance signifie estimer qu'une personne se conduira de la manière attendue."* (Frega, 2020)

Il y a une notion de mémoire qui est aussi rattachée à la fiabilité (Laurent, 2019). Nous nous souvenons des actions qu'un individu ou qu'une entité a exercé sur nous. Si une institution nous déçoit sur une décision qui a été prise, cela aura pour conséquence de développer un déclin dans notre fiabilité accordée envers cette institution. Il y aura une conséquence directe sur la confiance, puisqu'elle sera diminuée.

Enfin, dans le domaine des *sciences de l'information*, la notion de fiabilité est une caractéristique importante. Rattachée au domaine archivistique, elle fait référence à une des nombreuses règles archivistiques. Le SI utilisé par l'institution se doit d'avoir des documents authentiques et fiables et ce, dès leur création (Guyon, 2023).

La fiabilité se rapporte au discours du contenu, il peut prouver les faits qu'il rapporte dans l'exactitude des données énoncées (Bachimont, 2017). Pour lequel nous pouvons nous rapporter à une certaine opération, activité, ou autre (InterPARES 2, s. d.). Si le document est considéré comme fiable, alors nous pouvons lui faire confiance, car les informations transmises sont exactes, précises, justes (Guyon, 2023).

Ceci nous prouve donc que confiance et fiabilité sont intimement liés. Mais aussi que la fiabilité apporte la confiance.

2. UNE CONFIANCE OU DES CONFIANCES ?

Gary Alan Fine (2006) met en avant une réflexion pertinente : "*à qui, à quoi, où et quand apportons-nous notre confiance ?*"

Notre degré de confiance injecté dans un objet, dans une ressource matérielle ou immatérielle ne sera pas le même. Analysons cela.

2.1. Confiance entre les Hommes

Faire confiance à autrui est plus simple que de se faire confiance à soi-même. Lorsque la confiance est auto-portée, ceci exige un travail personnel sur soi. Il est parfois plus aisé d'avoir une reconnaissance dans un tiers (entretien avec C. Dubourg, 16 juin 2023).

Dès lors qu'il y a des interactions entre individus, leurs actions seront coordonnées pour avoir des réactions considérées comme acceptables par la société (Simmel, 2013).

Le facteur psychologique va intervenir pour permettre de contrôler son comportement dans une certaine situation. Watier (2019, p.141) utilise les termes de "*typifications sociales et psychologiques*". Ces comportements vont provoquer un sentiment de sûreté, nécessaire pour bâtir une confiance envers les uns et les autres. La confiance repose sur l'affectif porté entre deux individus, pour lequel le temps passé ensemble influera sur le degré de confiance. L'exemple présenté par le sociologue Simmel confirme nos propos :

> "*Tous les contacts physiques et psychiques, les échanges de plaisir et de douleur, les conversations et les silences, les manifestations d'intérêts communs ou opposés qui se produisent sans cesse - voilà d'abord ce qui fait la prodigieuse solidité du tissu social, sa vie fluctuante […]. Il s'agit de dévoiler les fils ténus, les relations minimales entre les êtres humains, dont la répétition continue fonde et porte toutes ces grandes formations, devenues objectives, dotées d'une véritable histoire*." (Simmel, 2013, pp.55-56).

Cette confiance ne peut être accordée telle qu'elle (Watier, 2019). Comme toute relation sociale, il faut connaitre la personne. Observer ses comportements, sa manière d'agir. C'est le système de confiance qui va permettre de comprendre les motivations d'une personne. Evidemment, il reste toujours une part d'incertitude, mais la confiance permet de réduire le doute, jusqu'à une certaine mesure.

Ensuite, la notion de "promesse" est importante, selon Hume (2010), il s'agit de tenir sa parole envers autrui. Si les engagements ne sont pas respectés, il y a une autorisation pour détruire la notoriété de la personne (Marzano, 2010). Promettre signifie, de manière implicite, que nous invitons une personne à nous faire confiance. Les manquements sont des vecteurs pouvant potentiellement être responsable d'une fragmentation de la société. Son existence même est donc cruciale. Sans confiance généralisée, c'est toute une société qui finira par se détruire (Macherey, 2004).

Dès lors que nous avons confiance en une autre personne, cela implique qu'il y aura une coopération qui peut être possible (Marzano, 2010). Cook, Hardin et Levi (2005), dans leur ouvrage, utilisent même les termes de "*cooperative relationships*", pour faire référence à des échanges sociaux perçus comme réussis.

Néanmoins, la confiance ne suffit pas à elle seule :

"*Trust is important in many interpersonal contexts, but it cannot carry the weight of making complex societies function productively and effectively*" (Cook, Hardin, et Levi, 2005, p.1).

Il est utopique de penser que nous pouvons accorder une confiance aveugle dans tous les individus (Fine, 2006). C'est un mélange entre crédibilité et plausibilité qui va nous permettre d'analyser la rumeur, les allégations. Fine définit la rumeur comme étant : "*une croyance liée à l'actualité et qui circule sans aucune preuve d'authenticité eu égard aux critères sociaux des croyances*". Ce sont les membres d'une communauté qui sont à mêmes de juger des propos, c'est à dire de les accepter et de provoquer une réaction quelconque. Les informations communiquées doivent donc être *fiables* (Watier, 2019). C'est aussi pourquoi notre société est régie par des codes, des règles et des valeurs à connaitre, et c'est dans celles-ci que nous placerons notre confiance. Certains métiers vont d'emblée instaurer un régime de confiance, de fiabilité : le militaire, le policier, l'ecclésiastique ; car leur profession suit les manières habituelles de groupe permettant de composer un ensemble. Ainsi, les règles provenant de l'Etat et d'autres institutions restent nécessaires pour faire respecter l'ordre (Cook, Hardin, et Levi, 2005). Mais nous l'avons signalé lors de notre exemple entre l'enfant et son parent, les relations de pouvoir ne sont pas les mêmes, le plus fort pourrait écraser celui disposant de moins de pouvoir, et ainsi détruire la fragile relation de confiance : la relation entre un manager et un collaborateur se déroulera bien s'il y a de la cordialité dans les échanges. Un moyen de la contrer est lorsqu'il y a une troisième partie prenante qui rentre en compte dans la relation pour éviter les formes d'abus, comme : le conseil d'administration d'un hôpital pour assurer la liaison entre le corps médical et le patient.

"*Third-party enforcers not only boost the probability of reliable behaviors but also create circumstances in wich trust within certain relationships over certain issues becomes more viable*". (Cook, Hardin, et Levi, 2005, p.4)

Poursuivons sur le régime de confiance et de fiabilité, qui sont deux notions proches, ainsi que la notion de jugement. En effet, c'est avant tout un *jugement social* qui va permettre de déterminer si l'un peut se fier à l'autre et inversement (Frega, 2020). Dans le monde politique, les politiciens partent du principe que tous les citoyens sont des acteurs responsables, de ce fait, fiables. La crise de Covid-19 a imposé des règles strictes à respecter pour l'ensemble des citoyens. Tout le monde ne les a pas suivies, il y a eu de nombreux abus. Ainsi, ce jugement peut s'avérer erroné. Ce dernier est donc prescrit par des stéréotypes et des valeurs faussées ; pour lesquels un individu peut attribuer une confiance, qui s'avérera par la suite mensongère. Nous nous situons ici dans un cas de "*confiance généralisée*" : nous traitons les autres en partant du principe qu'ils sont tous fiables (Uslaner, 2003). Pour cela, nous allons nous persuader qu'une majorité de la population va partager nos valeurs, il s'agit d'une confiance dans l'inconnu, en l'anonyme. Elle se crée par une acculturation. La société est considérée comme étant une seule et unique grande famille. C'est une notion qui est importante à garder à l'esprit car elle dispose d'un lien direct avec la blockchain, pour lequel nous reviendrons dans la seconde partie de ce mémoire[8].

[8] Voir 2.5. Le passé sulfureux des blockchains, p.52.

Nous sommes finalement dans une société qui reste régie par la confiance (Marzano, 2010). Les deux restent intimement liés : la société ne peut se passer de la confiance. Les Hommes aspirent à vivre dans un monde où ils peuvent compter les uns sur les autres, ceci est signe d'une société stable. C'est un ensemble social qui s'accorde et offre une sécurité.

2.2. Confiance dans les personnes morales

Nous n'allons pas rentrer dans des débats houleux d'économiste. Cependant, le schéma actuel de notre société est teinté par des crises financières, politiques et sociales (Algan & Cahuc, 2007). Pour laquelle la confiance est régulièrement remise en question : sentiment d'injustice et manque de dialogues, les relations se font plus méfiantes (Laurent, 2009).

La confiance envers une institution de type gouvernementale se fait plus difficilement que dans les années 50 (Savoie, 2014, p.9). Il y a une augmentation de la méfiance de la part de la société. Évidemment, l'auteur précise que celle-ci variera en fonction du pays, voire de la région. Les citoyens ne vont pas avoir le même degré de confiance par rapport à leur gouvernement. Ceci s'explique par la culture du pays, le régime politique exercé. C'est pourquoi il est particulièrement ardu de dessiner un seul et unique portrait. Dans ce cadre, nous allons essentiellement fonder notre analyse sur une société considérée comme démocratique, car la confiance se rapproche plutôt d'un gouvernent qui n'impose pas son pouvoir par la force, pour lequel, il n'y a pas d'autre choix que de se voir dans l'obligation de faire confiance.

Le gouvernement est représenté comme une figure d'autorité, nous ne pouvons pas à proprement parler de confiance. Il s'agit plutôt d'une soumission acceptée (Quéré, 2005). Nous choisissons de nous remettre à eux pour prendre des décisions qui nous espérons seront justes, car nous ne pouvons pas assister à tous les débats et problématiques publiques. Or, ce sont des jalons cruciaux à la mise en place et au respect de toute société désireuse d'être démocratique. Nous allons ainsi nous en remettre à des dispositifs de confiance : des personnes, des institutions, leurs agents qui vont aller, en notre nom, assister et participer à l'ensemble de ces activités. Ce qui est intéressant à noter, c'est qu'ils instaurent un climat de confiance, mais celui-ci ne peut être établi que si les citoyens acceptent de recevoir leur confiance. Nous sommes confrontés à un paradoxe, qui est provoqué par l'existence même du régime démocratique.

Le cadre de confiance des citoyens envers le gouvernement a un lien direct avec la gestion de l'information (Léveillé et Timms, 2015). En effet, les citoyens désirent avant tout que leur gouvernement communique avec eux, qu'il soit transparent dans la conduite des affaires et enfin, qu'ils aient accès aux informations produites par cette institution publique. L'ensemble de ces demandes peut être respecté avec une politique de Records Management. C'est l'ouverture des données à valeur probante pour que les citoyens puissent y avoir accès en tout temps. Dans cette optique, le projet InterPARES a pour objectif d'adresser un ensemble de solutions pour préserver les documents d'archives numériques. Ils établissent des modèles permettant de conserver, gérer et préserver les records. InterPARES intervient dans des projets d'actions envers des sociétés civiles. Ces projets de collaboration ont pour objectifs de :

> *"[…] generate theoretical and methodological frameworks to develop local, national and international policies, procedures, regulations, standards and legislation, in order to* ***ensure public trust*** *grounded on evidence of good*

governance, a strong digital economy, and a persistent digital memory." (InterPARES Trust, 2014).

Il existe de nombreuses méthodes pour répondre à ces besoins : des portails, des blogs, des sites internet, etc. Il importe peu la méthode choisie par le gouvernement, mais les données doivent provenir de sources sûres, elles doivent également être parlantes pour le citoyen qui en prendra connaissance. Le canal de diffusion est important, mais la nature de ces informations doit être pertinent et fiable. C'est pourquoi il est nécessaire de disposer d'une politique prenant en charge le document dès sa création, et ce, tout au long de son cycle de vie.

Ces types de projets permettent, entre autres, de créer une relation entre l'institution et la société. Plus largement, la diffusion des records s'intègre pleinement dans la création d'une démocratie plus solide et fiable dans laquelle le citoyen est impliqué et participatif. La confiance établie dans le gouvernement peut donc être facilitée par l'instauration d'une politique de RM.

Il faut distinguer la confiance portée aux autres, qui est interpersonnelle, de celle étant envers les institutions politiques (Pelletier & Couture, 2012). Nous ne pouvons pas avoir confiance envers un autre citoyen, de la même manière que dans une institution publique. Même si les auteurs précisent que derrière ces institutions, se trouvent des agents, des ministres, des politiciens. La confiance se trouve être plutôt diffuse (Savoie, 2014) : nous n'avons pas uniquement confiance envers l'institution en elle-même, mais plutôt son ensemble ; formant la confiance politique.

La confiance doit exister envers ce type d'institution, elle est l'élément crucial pour tout bon fonctionnement de régime démocratique (Pelletier & Couture, 2012). Sans elle, nous nous situons dans une impasse : les décideurs se retrouvent dans l'impossibilité de prendre une prise d'action. De plus, la fiabilité du gouvernement est nécessaire, il s'agit d'avoir un gouvernement correspondant à nos valeurs, normes et vision politique.

Les relations interbancaires sont un autre aspect à prendre en compte dans la confiance qui peut être développée entre les personnes physiques et morales. Ces relations font partie d'un ensemble plus large relatif à la relation de confiance entre les entreprises avec les salariés et les clients. Nous allons nous pencher sur le cas des banques, car elles sont particulièrement actives dans l'utilisation de la technologie de la BC et elles participent donc à son développement.

Lorsque nous parlons de confiance entre les relations bancaires et les consommateurs, les termes de "*crise de confiance"* sont utilisés (Gatfaoui, 2007). C'est une terminologie qui est assez forte et démontre un certain scepticisme de la part des consommateurs. Cette crise peut être expliquée par l'incertitude et les potentiels risques (ainsi que leurs impacts) qui pourront éventuellement intervenir dans la prestation du service, dû aux crises économiques qui ont eu lieu par le passé et qui ont joué un impact fort. La relation de confiance a été mise à mal (Antonin & Touzé, 2013). Il s'agit plutôt de *regagner,* de *restaurer* la confiance. Par le passé, les clients avaient confiance, mais celle-ci a été délaissée pour les raisons que nous avons évoquées. La confiance se travaille continuellement, elle n'est jamais réellement atteinte. Ce qui nous confirme la citation tirée de l'ouvrage "*La société de défiance"* de Algan et Cahuc (2007).

Pourtant, la relation de confiance est un point que les banques tendent à vouloir créer et développer dans les contacts avec leurs clients, comme nous le prouve cette citation :

> "*Le métier de la banque consiste fondamentalement à vendre de la confiance. Que 3 clients sur 10 expriment leur défiance mérite de l'attention, d'autant que le phénomène est résilient*" (Pion, étude Deloitte, 2012).

La compétitivité du marché impose de se démarquer, cela se fait en créant des relations durables et de qualité avec la clientèle, ce cas peut être appliqué plus largement à l'ensemble des entreprises (Hadj Khalifa & Kammoun, 2013). La confiance développée avec les banques repose sur la mise en place d'un marketing efficace, orienté sur le relationnel et la durabilité, il s'agit d' :

> "*Une politique et un ensemble d'outils destinés à établir des relations individualisées et interactives avec les clients, en vue de créer et d'entretenir chez eux des attitudes positives et durables à l'égard de l'entreprise et de la marque."* (Lendrevie et al., 2003, p. 904)

Les banques vont avoir tendance à créer deux typologies de confiance, la notion de *degré* de confiance, transparait bien ici. La première repose sur le développement de publicités permettant de diffuser la bonne image de la marque (Gatfaoui, 2007). C'est une confiance de premier niveau. Williamson (1993) l'appelle "*calculative trust".* Nous reviendrons sur ce terme plus loin dans notre réflexion. La seconde typologie - de deuxième niveau – est une confiance que nous considérons moins artificielle (Doney et Cannon, 1997). Il y a une volonté d'entretenir de solides relations avec le client, de par la prestation de service de qualité et de conseil, nous retrouvons donc la notion d'intensification du lien relationnel. Toutefois, aucune de ces typologies de confiance n'est synonyme de fidélisation du client. Il y a donc une nuance entre la confiance exercée et celle étant réellement perçue.

Il faut faire une distinction entre ces deux régimes de confiance explicités, car c'est le second qui permettra de rendre la relation stable, d'avoir une confiance plus accrue et qui engage une perspective sur du long terme (Hadj Khalifa & Kammoun, 2013).

Nous pouvons constater que la confiance entre les banques et les institutions publiques est totalement différente. Elles n'ont pas les mêmes objectifs et finalités. Les enjeux n'étant pas identiques, la confiance ne sera pas exercée, ni développée de la même manière. Ces deux cas démontrent toutefois la fragilité derrière le principe de confiance, ainsi que la difficulté à la mettre en place.

Elle s'établit dans un environnement particulier, la confiance est une notion qui se prépare et qui s'entretient si nous voulons la pérenniser dans le temps.

2.3. Confiance dans les machines

Les machines autonomes, les robots, les voitures intelligentes se manifestent de plus en plus dans notre quotidien.

La notion de *machine* fait ici référence aux machines dotées de systèmes autonomes, ainsi que les technologies pourvues d'une forme d'intelligence. Il est intéressant de se pencher sur la notion de confiance entre ces deux entités. En effet, cette relation est obligatoire. Il faut qu'il y ait une confiance dans la machine, autrement elle ne sera pas employée pour effectuer ses tâches (Desclaux, 2021).

La confiance développée entre l'Homme et une machine peut être comparée aux relations de confiance entre humains (Muir, 1988). Pour les relations humaines, avant qu'il y ait un contact établit avec la personne, il y a des éléments qui seront analysés chez l'autre individu : ses vêtements, son attitude, son langage corporel (Liothin & Riccio, 2015). Il en est de même avec un système. Nous aurons tendance à l'évaluer avant de l'utiliser, en étant vigilant à la marque, le nom des propriétaires, la charte éthique. Ceci peut même être étendu à l'ensemble du domaine numérique, d'ailleurs.

Une seconde comparaison peut être faite entre la relation d'Homme à Homme et d'Homme au Système. Les individus se font confiance s'il y a de l'honnêteté et de la bienveillance, ceci fait référence à la notion de la foi décrite plus haut. La confiance peut être perdue s'il y a une déception qui s'immisce. Muir (1988) indique qu'il en est de même pour les interactions homme-machine. La thèse de Victor Riley (1994) s'intéresse aux tests réalisés par des étudiants opérateurs sur des machines. Ces expériences avaient pour objectif de vérifier la confiance de l'opérateur dans le dispositif, la confiance que l'opérateur avait en ses capacités et son incertitude face aux risques de la machine et donc sa fiabilité. Certaines expériences menées ont subi des échecs, il y a eu un abus de confiance. Pourtant, ceci n'a pas eu d'influence dans le degré de confiance émis par l'opérateur sur la machine automatisée. Cela va même plus loin parce que les opérateurs ont continué à avoir confiance dans la machine, après l'échec. Le fait d'utiliser la machine va exercer une influence dans la confiance que nous avons dans l'automatisation. Cependant, une autre expérience réalisée par Parasuraman *et al.* (1993) précise que lors des tests, des stimulations ont été effectués. Elles ont démontré que l'automatisation de la machine provoquait des incidents graves. Malgré cela, les ingénieurs ont continué a avoir confiance dans le système, mais la relation de confiance a tout de même été impactée. D'autres expériences (Lee & Moray, 1992) ont montré que la confiance prenait du temps à se reconstruire si le dispositif avait présenté des échecs.

C'est pourquoi des facteurs vont permettre de comprendre la raison de ces divergences entre les expériences. Desclaux (2021) a mis en avant ceux qui lui paraissaient les plus importants pour tisser ce lien, à savoir : l'acceptabilité, la tolérance, la transparence et la bidirectionnalité entre la communication Homme et Système.

L'acceptabilité fait référence à la capacité d'une machine a effectuer une tâche plus ardue, ceci exercera une influence sur le degré de confiance entre l'humain et le système. Toutefois, si l'opérateur est fort occupé dans ses tâches et qu'il dispose de trop peu de temps dans sa journée, alors il aura tendance à se décharger sur la machine. Le degré de confiance n'exercera aucune influence, l'opérateur ne possède pas d'autre choix, il est devenu dépendant du système, voire même sur-dépendant. Ceci peut potentiellement résulter en un échec dans l'exécution d'une tâche par la machine. L'opérateur est alors insatisfait et il ne voudra plus autant dépendre sur sa machine, ce qui risque de créer une sous-dépendance.

La tolérance porte sur les facilités d'usage de la machine. En effet, si elle n'est pas complexe à utiliser, il y aura une certaine satisfaction qui sera ressentie de la part de l'humain.

Lorsqu'une situation complexe surgit, la machine sera ou non en mesure de fournir une réponse adaptée. Cela ne se limite pas à la simple restitution d'informations, mais également de préciser la source d'information, afin d'avoir une

transparence sur la qualité de cette dernière et donc sa fiabilité. En l'absence du critère de transparence, il est difficile de faire confiance au système.

Enfin, la communication humain et Système est cruciale. Elle permet d'avoir un partenariat entre ces deux entités. Pour reprendre l'exemple cité dans l'argument précédent, l'opérateur pourrait être en mesure d'ajouter des informations lorsque la machine n'est pas apte à fournir une réponse. De ce fait, l'opérateur propose des solutions qui seront ensuite jugées par le système automatisé. Il s'agit d'une résolution collaborative de problèmes.

Molloy et Parasuraman (1994), dans leur article, ont complété avec la fiabilité du dispositif d'automatisation de la machine. Si l'automatisation a su démontrer sa fiabilité par le passé, le fait qu'il y ait des incidents qui occurrent ne va pas avoir une influence directe sur celui-ci. Molloy et Parasuraman rejoignent l'argument de Desclaux (2021) puisque ce facteur de fiabilité aura, à nouveau, provoqué une dépendance pour l'opérateur dans la machine.

Il y a une confiance double qui entre en jeu et qui est énoncée au travers de ces facteurs (Kassaagi et al., 2006, pp.16-19). D'une part, la confiance émise dans le système. Et d'autre part, la confiance a *utiliser* ce système.

Desclaux (2021) et Kassaagi *et al.* apportent le même argument. Il s'agit de la *sur-confiance* ou de la *sous-confiance* que nous développons envers les machines. Se diriger vers une extrême ou une autre aura des conséquences plus ou moins néfastes. La notion de *degré de confiance* est un terme qui est intéressant à employer. Ces exemples montrent toute la complexité de la confiance. Nous l'avons prouvé : la confiance est essentielle et nécessaire, mais de manière mesurée[9].

Si nous ne nous dirigeons pas vers cette poussée à l'automatisation, alors le système n'est utilisé que passivement. Il n'aura plus de valeur ajoutée (Kassaagi et al., 2006).

Nous sommes surtout revenus sur la confiance entre l'opérateur et le système. Mais l'utilisateur de cette machine joue également un rôle prépondérant. Surtout au vu de ce que nous venons d'expliciter.

Concrètement, qu'est-ce que cela signifie pour nous, en tant que consommateur, développions un lien de confiance avec une machine ? Selon Gilles Desclaux (2021), c'est le *"degré auquel un utilisateur pense qu'un système se comportera comme prévu"*.

La notion de degré apparait à nouveau. L'utilisateur, tout comme l'opérateur, doit donc mesurer sa confiance. Un système avec un niveau d'automatisation relativement élevé pourrait être un véhicule capable de rouler à une vitesse relativement rapide, tel qu'une voiture (Calhoun, 2022). Le système est en mesure de détecter si l'humain perd connaissance et il peut donc agir en conséquence, dans le but d'éviter une éventuelle collision, par exemple. Le système informatique va réagir plus rapidement que n'importe quel humain. Nous sommes face à une situation de sécurité où des vies sont en jeu.

Tout un ensemble de technologies sophistiquées sont présentes sur les routes. Elles sont amenées à évoluer encore dans le temps. La sécurité routière n'en sera que fortement impactée, les métiers également. Mais n'oublions pas la fracture numérique : entre les consommateurs capables d'investir dans ce type de

[9] Voir Annexe 4 : Graphique : confiance et sur-confiance, p.87

technologie, et ceux pour qui il sera financièrement impossible de se le permettre. Nous dépassons ici le stade de confiance, car d'autres facteurs supplémentaires sont à considérer (Hautiere *et al.*, 2017). L'usage de cette technologie et la course à l'innovation par les groupes automobiles démontrent que les utilisateurs ont confiance dans le système et ils sont prêt à investir dans cette technologie.

Nous n'allons pas entrer plus amplement dans les détails relatifs à la confiance entre l'utilisateur et les dispositifs d'automatisation, nous considérons avoir ouvert le sujet.

Nous allons à présent nous concentrer sur le numérique, thème relativement proche des sciences de l'information. En effet, nos domaines sont continuellement impactés par les technologies numériques. La question de confiance est donc cruciale à soulever.

2.4. Confiance numérique

Nous évoluons dans une société où les entreprises et les administrations publiques sont désireuses de gagner en productivité et en performance. L'émergence des TIC offre des possibilités considérables (Rolland, 2022). L'échange d'informations peut être plus rapide et elles sont disponibles en temps réel (pp.12-13). Les relations internes et externes peuvent ainsi être développées.

Nous allons considérer la *confiance numérique* sous l'angle de la signature électronique. Ce n'est qu'une infime partie de la confiance que nous pouvons avoir dans les technologies numériques. La question peut aussi se poser pour les paiements en ligne ou l'identité numérique, par exemple.

La signature électronique est une thématique à haut potentiel pour les documents, elle sera plus loin analysée sous la perspective des blockchains.

Sa reconnaissance comme étant l'égale à son homologue papier remonte aux années 2000 (Tosi et al., 2015). Son utilisation reste toutefois timide.

En 2014, le règlement européen portant sur l'identification électronique et les services de confiance pour les transactions électroniques, communément appelé eIDAS est signé (Douville, 2017). C'est tout un régime juridique qui va être directement impacté. Auparavant, le papier disposait d'un avantage par rapport au format numérique (Girard, 2004). Toutefois, cette réglementation a eu pour effet d'annuler les intérêts dont le papier jouissait.

2024 sera l'année ou la réglementation eIDAS 2.0 devrait être appliquée (Electronic IDentification, 2022). eIDAS 2.0 vient ajouter la notion de "*digital identity wallet"* ou "*système d'identification digitale"*. Cette mise à jour du règlement européen vient corriger les défauts de la première version. L'un de ces défauts était le manque de coordination au sein même des pays.

Prenons pour exemple la Belgique, de nombreux citoyens ont l'application *Itsme* (Garnier *et al.*, 2023). Celle-ci est une carte d'identité numérique qui permet de s'authentifier sur diverses plateformes pour avoir accès à des services du gouvernement, des banques, etc. Des documents peuvent être directement signés au moyen de cette carte d'identité.

Au Luxembourg, l'identité numérique eID est multiapplicative puisqu'il est possible d'avoir plusieurs identités : l'une pouvant être privée, l'autre professionnelle ou encore institutionnelle. La carte se décline sous forme de certificats d'authentification et de signature électroniques. De nombreuses institutions utilisent

cette identité numérique, ainsi, bon nombre de services sont offerts aux citoyens : la poste, la banque, gestion administrative (Le gouvernement luxembourgeois, 2021). L'identité numérique est relativement forte et avancée (Garnier *et al.*, 2023).

En France, l'identité numérique est déclinée sous forme de certificat et donc de signature, ceci implique que pour chaque service, une identité doit être créée. Une application, France Identité, devrait voir le jour sous peu (Elina, 2023). L'application permettra de dématérialiser la carte d'identité physique pour ensuite authentifier l'identité d'une personne. Cette dernière pourra accéder à des services en ligne privés ou publics pour les démarches administratives (S, 2023).

Ces exemples démontrent que nous ne sommes pas tous et toutes au même niveau, il y a des disparités. eIDAS 2.0 a pour objectif principal d'acquérir une identité pour tous et qui soit valide sur l'ensemble du continent européen (Garnier et al., 2023). Il y a une volonté de se diriger vers une interopérabilité pour former une identité numérique européenne (Kassianides *et al.*, 2023). Cette mise à jour viserait également à rendre au citoyen un certain contrôle sur ses données personnelles.

Il s'agit donc d'accroître la confiance au sein des marchés intérieurs dans le but de construire un socle commun entre citoyens, entreprises, autorités publiques et les pays.

Revenons à présent à la signature électronique, car il s'agit d'un tournant dans la production de documents nativement numériques (Girard, 2004).

Signatures manuscrite et électronique sont dès lors placées sur un pied d'égalité, d'un point de vue juridique. Néanmoins, cela n'empêche pas que des limites viennent s'imposer. Tout comme le papier il faut, avec l'environnement numérique, s'assurer que le signataire a bien pris connaissance de l'ensemble du document, que le contenu de ce dernier n'ait pas été altéré ou modifié depuis la signature. Le législateur ajoute :

> *"[…] Sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité."* (Légifrance, 2000)

Pour nous assurer que les conditions dictées par la loi soient bien respectées, nous allons nous reposer sur la signature cryptographique et le principe du certificat de clé publique. Avec ces technologies, l'appel à un tiers de confiance devient inévitable. Le rôle de ce tiers "*est précisément de mettre en œuvre tous les moyens techniques afin de créer un contexte dans lequel les parties peuvent établir des échanges en toute sécurité*" (Gobert, 2004).

Prenons pour exemple l'entreprise Sogelink. Cette dernière se positionne comme étant un tiers de confiance (Mouton, 2012). Le président de Sogelink, Ignace Vantorre, a déclaré qu'il faut avoir une culture de la sécurité, sans faille (p.20).

À nouveau, nous avons cette notion de sécurité qui revient. La confiance numérique est donc ici synonyme de sécurité. Pour avoir confiance dans le système et donc l'utiliser, il faut avant tout créer un environnement sécuritaire, une "*culture de sécurité"*, pour reprendre les mots de Vantorre (Mouton, 2012, p.13).

L'exposition aux risques suite à d'éventuels échanges considérés comme non sécurisés pourrait être désastreuse pour les informations, pouvant engendrer une fuite et/ou un vol de données. C'est pourquoi la notion de sécurité ne s'applique pas qu'aux infrastructures techniques, tel que les réseaux (de Lamberterie & Blanchette,

s. d.). Il faut qu'elle soit élargie a engager du personnel compétent, mais également former les autres membres du personnel, pour qu'ils adoptent de bonnes pratiques en termes de sécurité. La sécurité ne peut se limiter à l'aspect informatique, elle doit prendre en compte l'humain pour le former et l'accompagner. La plus grande faille dans les systèmes d'information reste avant tout, l'humain.

Le numérique implique ici une notion de sécurité, synonyme de confiance. Pour l'instaurer, toutes les parties doivent être incluses. Il s'agit d'une sorte de "*chaine de sécurité*" (Mouton, 2012). La confiance est d'ordre collectif, tout le monde y participe. Mais elle est également multi-dimensionnelle puisqu'elle fait travailler objets inanimés avec des Hommes, ce qui forme une sorte de synergie.

Cette synergie peut être instaurée par les tiers de confiance : le prestataire de service de certification ou PSC. L'intérêt de ce prestataire est qu'il va instaurer un régime de confiance au moyen de règles fixées (audit de qualification ou de certification pour attester du respect des exigences réglementaires) et donc un certain cadre de sécurité (Merlin, 2021?).

La culture de sécurité peut être instaurée par les prestataires de confiance. Cet un label qui assure que:

> *"[…] l'ensemble des moyens techniques, humains et organisationnels a été mis en œuvre pour garantir un niveau de sécurité optimal."* (Merlin, 2021?, p.10)

L'article de l'Université de Namur (Gobert, 2004), ajoute que ce service de PSC ne peut se limiter qu'au champ de la signature électronique, ainsi que les certificats d'identité. Notons bien qu'ils ne peuvent pas s'élargir à un cadre électronique plus grand pour une application avec l'archivage électronique ou au recommandé électronique, par exemple. Ces domaines ne peuvent donc pas (encore?) bénéficier d'une couverture juridique et d'une certitude quant à la fiabilité du service presté.

Les conditions imposées par le Code Civil, repris ci-dessus, indiquent qu'il faut connaitre l'identité du producteur et signataire du document, ainsi que des conditions concernant la conservation et la préservation du document ; dans le but que la signature électronique soit considérée comme valable et l'ensemble du document valide. Nous pouvons traduire ces termes par les principes énoncés dans la norme 15489-1 relative à la gestion des documents d'activité. Celle-ci stipule que :

> "*La gestion des documents d'activités englobe les actions suivantes :*
>
> *a) […]*
>
> b) *Prendre des mesures appropriées pour protéger leur authenticité, leur fiabilité, leur intégrité et leur exploitabilité, le contexte opérationnel et les exigences de gestion évoluant dans le temps*"
>
> (Organisation internationale de normalisation (AFNOR), 2016, p. 9)

Un lien se fait entre le métier d'archiviste/records manager, qui transparait au travers de la norme ISO 15489-1 et l'article 1316-1 provenant du Code Civil. Dès lors, il apparait intéressant de faire un lien entre nos métiers et ce principe de confiance intervenant avec la gestion des documents.

Nous reviendrons sur cette analogie dans la seconde partie de ce mémoire.

3. LA BLOCKCHAIN, VECTEUR DE CONFIANCE ?

Jusqu'à présent nous avons pu voir que la confiance est une notion nécessaire à disposer si nous désirons évoluer dans un système – sociétaire ou informationnel - viable et fiable. L'ensemble des régimes de confiance s'intercalant entre les objets ou les individus est toutefois différent.

La confiance entre individus repose sur le principe de bienveillance, de connaissance de la personne et de promesse respectée.

Tandis que la confiance entre les Hommes et les personnes morales tant à se formaliser de deux manières selon que l'institution soit publique ou privée. La première utilisera la transparence et la circulation des informations, au moyen des TIC. Derrière ces institutions, il y a également des hommes et des femmes en charge de la faire fonctionner. Ces derniers sont à prendre en compte dans ce régime de confiance. Tandis que pour les institutions privées, telles que les banques, il y aura deux degrés de confiance. La première est une confiance artificielle axée sur la marque. La deuxième est axée sur la volonté de faire revenir le client et d'avoir son adhésion qui soit marquée sur le long terme, avec un service de qualité. La confiance est, dans ce cadre, nullement un signe de bonté puisqu'il s'agit d'un objet inanimé.

La confiance sert simplement les intérêts de l'entreprise/de l'institution à se démarquer face à la forte compétitivité du marché (pour le privé) ou à disposer d'une éventuelle réélection et d'une perte d'engagement civique (pour le public). À cela, le gage de confiance des institutions gouvernementales est aussi nécessaire, car il est vital pour le maintien d'une société démocratique (Laurent, 2009).

Ensuite, la confiance entre les Hommes et les Machines/Systèmes est caractérisée par une confiance mesurée : elle ne doit pas être excessive ou réduite, il faut un juste milieu. Pour l'instaurer, différents facteurs vont intervenir.

Enfin, nous nous sommes intéressés à la confiance numérique, sous l'angle de la signature électronique et nous avons ouvert le débat sur l'identité numérique. Un certain degré de confiance peut être atteint si la technologie est suffisamment sécurisée informatiquement. La notion de sécurité veut tout dire et paradoxalement pas assez, car si nous voulons que la technologie soit sécurisée, alors, il faut avoir confiance en elle. Nous sommes confrontés au cercle sans fin de l'Ouroboros, le serpent qui se mange la queue.

Dans ce cadre, l'existence d'un tiers de confiance est justement ce qui permet d'instaurer un régime de confiance dans la signature électronique. L'existence d'une personne physique et morale est un facteur de confiance. Or, l'intérêt de la blockchain étant l'absence de ce tiers. L'ensemble de l'architecture du réseau reposant sur un système décentralisé.

Comment pouvons-nous alors nous assurer de disposer d'une confiance : entre les utilisateurs du réseau, mais aussi les contenus présents et échangés de manière continue au travers des chaînes de blocs ? La notion de confiance est complexe à étudier, car elle n'est pas fixe à chaque fait ou domaine. Les exemples donnés jusqu'à présent nous le prouvent. La confiance va s'instaurer différemment, car elle est propre à chaque cas, en fonction des parties prenantes et de leurs intérêts en jeu.

Cependant, la confiance est nécessaire dès qu'il y a des interactions. Sans elle, c'est tout un pan de la société ou sur une plus petite échelle, d'une activité qui ne pourra être durable dans le temps. En l'absence de confiance, des

dysfonctionnements émergeront, les cas étudiés nous l'ont démontré. Il y a une crainte qui émerge dans toutes les confiances que nous avons analysées : la peur de la voir se décliner (Laurent, 2009).

La confiance est aussi difficile à mesurer, car : "*personne n'a confiance dans tout le monde à propos de tout*" (Nannestad, 2008).

La confiance numérique a mis en avant plusieurs enjeux et défis que nous pouvons appliquer à la blockchain. La blockchain pourrait être solution. Mais avant d'être en mesure d'utiliser la technologie, encore faut-il déterminer si nous sommes prêts à lui faire confiance. Après tout, il s'agit de lui confier tout un pan du patrimoine documentaire d'une institution. Il faut déterminer si elle fournit une assurance suffisante.

PARTIE 2 : CONFIANCE DANS LES BLOCKCHAINS POUR UNE APPLICATION AVEC LES ARCHIVES

Notre société est de plus en plus façonnée et régie par les informations (International Business Machines Corporation (IBM), s. d.) A tel point, qu'elle en est devenue dépendante. L'entièreté des activités d'une entreprise repose sur ses capacités à produire, diffuser, retravailler, communiquer ses informations. Dès lors, des besoins vont naître pour être plus attractif sur le marché face à la rude concurrence. Il faut être productif et performant pour se démarquer dans un monde où l'urgence ajoute des contraintes supplémentaires. C'est pourquoi il y a une nécessité d'avoir une information qui circule rapidement et qu'elle atteigne sa cible visée pour éviter toute fuite de données, par exemple.

Selon la littérature scientifique, la BC est en mesure de répondre à ce besoin, car elle rend disponible les preuve relatives aux informations de manière quasi instantanée avec transparence. Selon la typologie de la blockchain qui est employée, l'environnement sécurisé permet de limiter les accès aux données pour les nœuds autorisés du réseau. La traçabilité des actifs numériques peut être effectuée en suivant l'ensemble du cycle de vie d'un record dans le détail.

Dans cette seconde partie, nous allons revenir sur le degré de confiance que nous pouvons injecter dans les technologies blockchains. Nous allons surtout fonder notre analyse sur base des cinq entretiens[10] qui ont été effectués, mais également de la littérature scientifique.

1. UTILISATION DE LA BLOCKCHAIN AVEC LES ARCHIVES

Avant de nous interroger sur la confiance en elle-même, il parait utile de revenir sur des projets qui sont en cours. Ces cas d'usage utilisent la blockchain pour la gestion de documents d'activité. Ceci permet dans un premier temps de vérifier la pertinence de son utilisation dans le domaine archivistique. Cette partie est donc plutôt descriptive, mais ce détour nous semble légitime d'être parcouru avant de revenir sur notre problématique.

La blockchain offre de nouvelles opportunités à nos métiers. Voici quelques exemples de cas d'usage, tels que décrits dans la littérature scientifique.

La supply chain est un domaine qui est particulièrement pertinent dans la traçabilité des documents (Bhatia et al., 2020). Par exemple, le projet "Blood Diamonds" par *De Beers Group* a développé une blockchain utilisant le protocole Tracr. Le projet consiste à tracer l'ensemble du circuit parcouru par les diamants, à partir des mines jusqu'à la vente en détail. D'autres matières premières doivent aussi avoir une traçabilité qui doit être suivie et prouvée, notamment : l'or, le tantale ou encore l'étain. Ce sont des ressources en forte demande, mais l'origine de provenance est questionnée, ainsi que l'ensemble du chemin parcouru, afin d'assurer l'acheteur de l'authenticité du matériau, notamment. Les blockchains privées et de consortium sont en mesure de garantir ce principe d'authenticité dans un réseau limité. Toute

[10] Description des entretiens dans les sources, p.73

altération, c'est-à-dire, une quelconque modification serait directement reprise dans le registre.

Le projet "ARCHANGEL" par la *Library of Congress* a été lancé en 2017 (Bhatia & Wright, 2019). Ce projet de type preuve de concept a pour but d'utiliser une blockchain parmi laquelle les nœuds du réseau sont les services d'archives et les organisations chargées de conserver des pans de mémoire. L'idée étant de créer un réseau d'archivage utilisant la BC[11]. Le protocole est celui d'Ethereum.

Ces dernières peuvent ainsi s'assurer que les archives publiques numériques n'ont pas été modifiées ou altérées dans le temps, une fois reçues par le service. Au sein de cette BC, les signatures électroniques des documents nativement numériques ou numérisés seront stockées (Collomosse et al., 2018).

L'utilisation de la BC spécifiquement pour ce projet sert à améliorer la confiance dans les archives publiques officielles[12], sans passer par le biais d'un système centralisé. La BC est donc ici perçue comme une solution pour assurer la confiance dans les archives :

> "*Document integrity is fundamental to public trust in archives. Yet currently that trust is built upon institutional reputation — trust at face value in a centralised authority, like a national government archive or University. ARCHANGEL proposes a shift to a technological underscoring of that trust, using distributed ledger technology (DLT) to cryptographically guarantee the provenance, immutability and so the integrity of archived documents."* (Collomosse et al., 2018)

Ensuite, l'association eFutura est un organisme actif dans la transition vers le numérique qui a été créé en 2015 (eFutura, s. d.). L'association est chargée de définir, mais aussi de certifier des normes françaises, européennes et internationales. Elle s'occupe de thématiques liées à la confiance numérique, l'archivage des data et des documents, la gestion documentaire, la capture de flux, notamment. En rapport avec ces thèmes, l'association va mettre en œuvre des groupes de réflexion et ainsi produire des livres blancs, des avis juridiques, des newsletters. Il y a également des échanges qui sont réalisés avec d'autres groupes ou associations qui ont la même activité à l'extérieur du territoire français.

Parmi les groupes de travail, l'un d'entre eux – "*la blockchain des archivistes*" - s'est consacré à la BC. Le projet vise à archiver des journaux en suivant la norme NF Z 42-013 (2020) qui porte sur l'archivage électronique (recommandations et exigences) sur une blockchain. Il s'agit du fruit de la collaboration entre le prestataire de SAE – Spark Archives – avec l'association eFutura.

Notre entretien avec Christian Dubourg (entretien le 15 juin) a permis de comprendre la relation que la norme entretient avec la technologie.

La norme NF Z42-013 revient sur la journalisation. C'est-à-dire les journaux qui sont produits dans les SAE. Ces journaux sont des éléments de preuves, ils intègrent le cycle de vie des archives, ainsi que tous les évènements qui ont pu intervenir sur le SAE. Autrement dit :

[11] Voir Annexe 6 : architecture du projet Archangel, p.89

[12] Voir Annexe 7 : nœuds du projet Archangel, p. 90

"*Il s'agit de documents structurés selon un format défini et exploitable consolidant un ensemble d'enregistrements relatifs aux événements du SAE. Les journaux sont gérés selon des procédés permettant de garantir leur* ***intégrité*** *et leur* ***exhaustivité*** *ainsi que* ***l'absence de modification*** *des enregistrements contenus*" (Organisation internationale de normalisation (AFNOR), 2020, p.31)

Les journaux de preuve reprennent toutes les opérations du jour. Et tous les soirs, ce journal est lui-même archivé. La norme précise en plus que l'empreinte du journal de J-1 va être consignée dans le journal J, nous allons "chaîner" les journaux. Il y a effectivement un risque de modification ou de suppression du journal – que ce soit intentionnel ou pas (p.34). Ce chainage va permettre de s'apercevoir si un journal est remplacé par un autre (entretien avec C. Dubourg, 15 juin). Dès lors que nous remplaçons un journal, un élément va être modifié, donc l'empreinte ne sera plus la même. Si nous remplaçons un fichier par un autre, alors le contenu sera changé, à nouveau, l'empreinte se voit être modifiée. Il est intéressant de savoir qu'en 2009, on parlait déjà du stockage de hash dans des journaux chainés, pour lequel on avait la restitution de l'heure et de la date à laquelle il avait été stocké.

Nous pouvons donc bien constater que derrière cette norme, se trouvent les mêmes aspirations que l'architecture des blockchains : journal de chaînage et chaîne de blocs.

Toutefois, en quoi est-ce que les BCs peuvent intervenir dans ce processus ?

Nous venons de voir que les empreintes des journaux étaient utilisées. Au départ, l'objectif de la norme était d'arriver à mettre en place un système dans lequel il était impossible de changer un élément par un autre sans s'en apercevoir, d'où l'utilisation des journaux chaînés (entretien avec C. Dubourg, 15 juin). Et finalement, la BC est arrivée un peu plus tard. Celle-ci repose sur des arbres de hash (arbre de Merkle) de telle manière à ce que si un des éléments de l'arbre est changé, nous pouvons casser la chaine et reprendre les empreintes des blocs précédents dans la blockchain.

De fait, ce sont ces mêmes empreintes qui vont pouvoir être chaînées sur la blockchain (entretien avec C. Dubourg, 15 juin). Cette dernière va donner des informations complémentaires sur l'horodatage, mais aussi attester que ce sont ces mêmes journaux qui ont été conservés dans le SAE et qu'ils ont bel et bien été créés par ce SAE en question, à la date/heure indiquée. La blockchain va jouer le rôle attendu par les tiers de confiance puisqu'elle est l'horodateur de confiance, tout en supprimant les intermédiaires pouvant intervenir dans ce processus. Néanmoins, la limite d'utilisation de la BC, réside dans le fait que si les contenus des journaux sont perdus, nous n'avons plus qu'accès aux empreintes des journaux chaînés, il y a donc une perte non moindre.

C'est la raison pour laquelle, dans un deuxième temps, il va falloir préserver les contenus indépendamment de la blockchain, puisqu'elle va garder les éléments de preuve que ces contenus existent quelque part (au moyen de l'empreinte). Les nœuds autorisés vont pouvoir vérifier qu'un certain contenu soit bien correspondant au hash intégré dans la BC, pour retrouver les informations de temps à laquelle les opérations se sont produites (typologie de l'opération, ce que c'est). Ce qui est important c'est que l'identifiant unique du contenu, ce soit bien ce hash. Et donc c'est cet hash là qu'il faut préserver de telle manière à ce qu'on puisse toujours avoir un

historique de ce qui a pu se passer sur un hash, quel que soit les opérations effectuées.

Nous allons revenir sur ce projet dans la partie ci-dessous en y intégrant l'angle de la confiance. Nous n'allons pas rentrer dans de plus amples détails, nous considérons qu'au travers de ces quelques cas d'usage, nous avons pu introduire qu'il existe bel et bien un potentiel d'utilisation à considérer. À présent, il nous faut interroger le régime de confiance que nous pouvons injecter.

2. LA CONFIANCE DECORTIQUEE SOUS L'ANGLE DES BLOCKCHAINS

La blockchain se place comme un véritable "*tiers de confiance numérique*" (Jost, Le Ven, & Texier, 2021). Le supplément gratuit au n°351 d'Archimag est nommé : *"Confiance numérique : quelles technologies pour la garantir ?"*. Au travers de ce numéro, il est mis en avant que la blockchain est une des technologies permettant d'avoir confiance dans le numérique. Nombre d'auteurs partent du principe que nous accordons *déjà* notre confiance envers cette technologie, elle est perçue comme un outil, une solution pour avoir confiance dans le numérique. C'est une sorte de réponse, finalement.

Selon Kevin Palop : "*[...] la confiance est établie de façon distribuée"* (Palop, 2017, p. 5). La question nous semble pourtant être posée dans le mauvais sens. La confiance existe au sein de la technologie parce que le système est distribué. Mais il est légitime de se demander : *à partir de quels critères peuvent-ils mettre en avant le fait que nous faisions bel et bien confiance dans cette technologie, aujourd'hui ?* Il nous semble effectivement limité de s'arrêter à sa simple architecture globale. Ceci ne nous permet pas de comprendre pourquoi nous devrions (ou non) lui faire confiance.

En l'état actuel des choses, la littérature assume que nous considérons la technologie comme responsable d'un vecteur de confiance. Cependant, il est difficile d'en trouver les véritables causes qui génèrent un tel régime.

Sur base de cette constatation, nous allons donc réfléchir dans le sens inverse en nous penchant sur les raisons, mais aussi l'échelle avec laquelle nous parvenons à lui accorder une telle confiance. *Et qu'en est-il de la méfiance et de la défiance ? Quelles sont-elles ? Existent-elles seulement ?*

La littérature se limite à présenter des cas d'usage possibles et les opportunités offertes, sans rentrer dans de plus amples détails. La BC est citée de manière excessivement positive, sans qu'il y ait de réelles prises de recul. Nous considérons que la réponse à notre problématique ne se trouve pas dans cette littérature, car elle reste trop vague, optimiste et théorique.

C'est la raison pour laquelle nous avons posé la question à des professionnels directement[13]. Les corps de métiers nous permettent de rentrer dans le cœur de l'activité : quelles sont les personnes qui utilisent, envisagent d'utiliser, attendent le moment opportun ou encore se refusent, à utiliser les BC ? Tout en mettant en vis-à-vis ces professionnels avec leur rapport de confiance dans la technologie.

[13] Voir Annexe 5 : exemple de la grille d'entretien pour les archivistes, p.88

2.1. Blockchain et sécurité

Dans la première partie de ce mémoire dédiée à la confiance, nous avons conclu qu'une prérogative permettant d'instaurer un certain degré de confiance était la *sécurité* derrière la technologie. Nous allons donc allier cette notion avec la blockchain : *comment pouvons-nous savoir si la blockchain est suffisamment sécurisée ?*

Pour cela, nous nous sommes penchés sur les organismes de recherche, les institutions représentatives de la défense des intérêts et/ou de l'innovation de la blockchain. Ils agissent plutôt en tant que porte-parole des technologies BCs.

Il existe des organismes de manière générale pour le numérique, notamment avec la cybersécurité, sujet qui est actuellement en vogue, dont l'ANSSI :

> "*Les formidables applications que permet le numérique ne seront durables que si elles recueillent la confiance de leurs utilisateurs. […]*
>
> *[…] dans un monde où la cybercriminalité est en forte croissance et où il est de plus en plus difficile d'assurer la protection de ses données […]"* (Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), s. d.)

L'ANSSI se positionne comme l'acteur majeur en termes d'écosystème numérique, en menant des actions de recherche, de sensibilisation, afin de contrer les menaces causées par le numérique, mais également jouir de cette dernière pour innover et développer de nouveaux cas d'usage.

Sur le site internet de l'ANSSI figure un de ses Webdocumentaire consacré à la cryptographie :

> *"[…] Et paradoxalement, la cryptologie est passée d'une science du secret à une* ***science de confiance****."* (Stern & Agence nationale de la sécurité des systèmes d'information (ANSSI), s. d.)

Le Groupe Goldman Sachs Inc. est une institution financière qui délivre des services financiers à leurs clients. Une partie de leur site internet est réservé à la BC. Il y figure une citation qui rejoint celle de l'ANSSI :

> "*It [la blockchain] combines the openness of the internet with the* ***security of cryptography*** *to give everyone a faster, safer way to verify key information and* ***establish trust****."* (Goldman Sachs, s. d.)

Ces deux citations mettent en avant que la blockchain est sécurisée, car elle utilise la cryptographie, ce qui permet d'établir la confiance.

Pourtant, lors du webinaire organisé par Archimag le 23 mai 2023 sur la confiance numérique. Pascal Agosti et Eric Caprioli, tous deux docteurs en droit, ont énoncé que l'utilisation de la cryptographie ne permettait pas de s'assurer pour autant que nous ayons confiance dans la BC. D'après les intervenants, confiance et cryptographie n'ont pas de lien.

De plus, lors des entretiens menés, deux interviewés (entretien avec H. Wahibi, 03 juillet et A. Gaudinat, le 07 juin) nous ont signalé un problème similaire relatif au futur des BCs et qui impacterait la sécurité directement de la technologie : il s'agit des ordinateurs quantiques. Ils ont une puissance tellement considérable qu'ils seraient en mesure de casser toutes les clés publiques et privées. Toutefois, le

quantique a encore du chemin à parcourir avant d'être prêt. Et la BC reste, à date d'aujourd'hui, une bonne option en termes de sécurité. C'est d'ailleurs la raison pour laquelle la cryptomonnaie s'est intéressée à cette technologie. Mais, nous avons vu que la sécurité n'apporte pas la confiance, pour autant dans la première partie.

Il existe de nombreux protocoles BC (bitcoin, ether, monero, etc.). La course à l'innovation oblige les BCs à se réinventer pour se démarquer (entretien avec A. Gaudinat, le 07 juin). Dans ce cas, l'innovation passe par l'ajout d'applications. C'est un réel marché, si une nouvelle BC se crée, mais qu'elle a les mêmes applications qu'une autre – déjà existante – elle n'aura pas de longévité, car elle n'a pas de valeur ajoutée. Bitcoin n'évolue pas, car dans sa gouvernance interne, il est de nature conservateur. En revanche, Ethereum se doit d'innover, car il est fortement concurrencé.

Il est effectivement possible de rajouter des couches logicielles à la BC, tel que les smart-contracts, par exemple (entretien avec A. Meissonnier, le 28 juin). Dans l'architecture "brute", les BCs ne possèdent pas de failles en matière de sécurité, il n'est pas possible d'accéder aux informations inscrites sur la BC, autrement dit, de l'a craquer. Ces failles sont plutôt apparues suite à l'ajout d'applications autour de la BC. Et c'est un des problèmes aujourd'hui avec les BCs, il y a une pléthore d'applications possible qui permettent d'avoir de nombreux usages (entretien avec C. Dubourg, le 15 juin). Pour lesquels il a été possible de détourner le code, ou alors des bugs sont apparus (entretien avec A. Meissonnier, le 28 juin). Derrière les smart-contracts se cache avant tout une couche de code, il ne s'agit pas d'un contrat à proprement parler. Finalement, il ne s'agit pas de réelles failles en matière de sécurité, mais plutôt de détournements autour des technologies qui sont ajoutées. Souvent, nous allons jouer avec le code, dans le but de voler de l'argent, c'est d'ailleurs ce qui a pu se passer en détournant des millions d'euros en cryptomonnaie. Il nous semble légitime d'interroger cette interopérabilité entre les BCs et ces applications. Si nous désirons instaurer un régime de confiance, ne devrait-elle pas être limitée, isolée ? En tant qu'être humain, nous n'accordons pas notre confiance à une grande échelle d'individus, c'est justement ceci qui apporte à la confiance sa valeur, parce qu'elle est limitée. Dès lors que nous faisons parler les BCs entre-elles ou avec d'autres outils qui sont extérieurs à la BC, il y a des risques de rendre l'ensemble du système défectueux (entretien A. Gaudinat, le 07 juin). Nous voulons une seule infrastructure qui fasse tout, mais le revers de la médaille étant que nous augmentons de manière drastique la complexité du système. L'idée étant de garder la confiance au sein de la BC – que nous savons sécurisée – pour l'isoler au maximum.

Par ailleurs, les BCs ont été écartées de eIDAS 2.0. En 2021, il y a eu une proposition de texte pour mettre à jour la première version de eIDAS de 2014 (entretien avec C. Dubourg 15 juin 2023). Dans ce texte, il y a un volet concernant la confiance numérique, avec les nouveaux services de confiance ; dont la partie sur l'archivage électronique, la préservation des éléments de preuves de la signature et un service de registre partagé. En mars 2023, il y a eu un ensemble d'amendements qui ont été produits par trois universités européennes. Ces entités ont revu le texte qui avait été proposé en 2021. Et parmi ces amendements proposés, il semblerait que le service de registre partagé ait disparu. Avant cette suppression du service de registre partagé, il y avait une volonté d'ancrer une confiance numérique via les institutions européennes ; qui elles-mêmes étaient partagées par l'ensemble des États européens sur lesquels chaque nœud, de chacun des pays, retombait sur le nœud des

autres états. Au départ, l'idée était de passer sur plusieurs identifications numériques et ils s'imaginaient pouvoir utiliser ce service dans le cadre de service d'archivage électronique qualifié ; dans le but d'ancrer la confiance au travers de la traçabilité des hash de la blockchain. Toutefois, l'idée fut mise de côté faute de temps à disposition et de moyens de financements. Il n'est pas impossible qu'elles soient rajoutées, mais cette information est encore inconnue à ce jour.

Selon Pascal Agosti et Eric Caprioli (2023), il serait intéressant que la BC figure dans eIDAS 2.0 afin de nous informer sur la sécurité de la technologie, notamment. Actuellement, il n'existe pas de référentiel incluant les technologies BC. Cette absence implique que toute personne physique ou morale est en mesure de vanter ou discréditer la BC, c'est la raison pour laquelle nous avons cité quelques institutions plus haut. Mais où sont les certitudes ? Où sont les prérogatives ? De même pour les exigences minimales dont il faut disposer. Ceci ajoute un certain degré d'incertitude, pouvant dévaloriser toutes les blockchains.

2.2. Blockchain et SAE

Il y a tout un questionnement quant à la pérennité de l'information, au sens purement archivistique : faire survire les informations sur le très long terme. Nous l'avons dit, nous ne sommes pas face à une GED, ni un SAE. Nous savons que la blockchain peut nous signaler si nous sommes face à une copie fidèle et fiable, même s'il y a 10 ans d'écart entre la période où il a été créé et vérifié. En revanche, nous ne savons pas en quoi le contenu a été modifié (Meissonnier, 2019). Or, le SAE garantit que le document ne bougera pas, ou, que s'il y a action de modification, ce sera uniquement dans le code à des fins de préservation ou de lisibilité sur le long terme. Si nous changeons le format pour une meilleure préservation, cela va modifier l'empreinte. Or, le contenu en lui-même du document est resté le même. Comment sommes-nous capables d'assurer la pérennité et l'invariabilité du document, dont nous avons l'empreinte dans la chaîne de blocs ? (entretien avec A. Meissonnier, le 28 juin). Ceci nous laisse supposer que nous ne pourrions pas garantir notre confiance dans ces BCs, car nous considérons que la technologie présente des limites non-négligeables dans notre domaine.

En parallèle à cette problématique, il y a aussi l'arrêt de la BC et donc l'archivage de la BC en elle-même (Bhatia et Wright, 2019). Lorsqu'elle n'est plus utilisée pour une certaine raison et qu'elle devient dormante. Il faut alors archiver cette BC pour s'assurer de pérenniser les informations qui y sont stockées et l'ensemble du système en lui-même. Trois solutions s'offrent à nous. La première consiste à extraire les informations qui y sont stockées, afin de les stocker ailleurs en vue de les pérenniser. La seconde étant de s'assurer que la BC continue à tourner en injectant des requêtes pour ne pas qu'elle se mette en mode dormante, nous considérons cette méthode comme étant un moyen pour retarder le problème, mais ce dernier perdure toutefois. La troisième, qui selon nous est la plus complexe, puisqu'il s'agit d'archiver la BC. Cette technologie étant utilisée depuis peu, il s'agit d'une réflexion qui n'a pas encore atteint une maturité suffisante. Néanmoins, il semble urgent de lancer les recherches, car au plus longtemps le système est délaissé avec des participants inactifs, au plus les données qui y sont stockées deviennent périmées. En effet, le système repose sur un système décentralisé, avec des nœuds dans lesquels l'ensemble du réseau est censé avoir confiance pour que le système

soit utilisé, nous allons le voir dans la partie suivante[14]. Cela va dépendre du type de BC utilisé, car la BC publique sera bien plus exposée à ce risque qu'une BC de consortium. Mais à nouveau, nous considérons que le risque zéro n'existe pas, il faut donc y inclure toutes les typologies de BC. Dès lors qu'il n'y a plus suffisamment de participants actifs, le nombre de nœuds malveillants peut alors grandir et risquer de corrompre l'ensemble de la chaîne. Les données stockées ne seraient plus valides et elles ne pourraient donc pas être utilisées, bref, la confiance dans le système serait en danger.

Ensuite, le SAE est un service de confiance à proprement parler (Caprioli & Agosti, 2023). Il a acquis ce statut suite à son ajout dans eIDAS.

La "blockchain des archivistes" que nous avons explicité plus haut, a travaillé sur le sujet du point de vue des side-chain.

Ils sont partis du principe qu'aujourd'hui, les services d'archives stockent seulement les contenus pour une durée indéterminée et ils stockent également leurs journaux. Nous pouvons faire confiance à un service d'archive pour réaliser ce processus. Ceci veut dire qu'un service d'archive peut y arriver, dès lors qu'il y a un mécanisme de chaînage. Le projet "la blockchain des archivistes" a considéré qu'ils pouvaient aller plus loin en venant partager la confiance. Et qu'est-ce que la confiance d'après le groupe de travail ? C'est avant tout un *partage de contenu*. Il s'agit de diviser la confiance via un système de partage d'empreinte dans lequel chaque service d'archives ne peut plus apporter de modification. Le principe étant de créer une blockchain pour les services d'archives, dans lequel ces services n'auront plus leur propre système de confiance - qui est donc propre à eux, avec leurs journaux chaînés, conformément à la norme NF Z42-013. Mais ils vont pouvoir utiliser une blockchain qui est partagée entre les services d'archives (les nœuds du réseau) et qui sera gérée par cette communauté formée.

Ce côté partagé de la preuve est particulièrement intéressant (entretien avec C. Dubourg, 15 juin). Une personne remettant en cause le SAE et/ou la blockchain, va de ce fait, remettre en question; d'une part, le système de chainage interne au système de SAE; d'autre part, le système des empreintes qui elles ont été validées de manière partagée par les nœuds (les services d'archives). En résumé, il serait particulièrement compliqué de remettre en doute la confiance dans le système dû au nombre de couches de vérifications existantes.

Un autre entretien effectué avec Antoine Meissonnier, chef du service des archives du Ministère de la Justice, nous a permis de revenir sur ce projet (entretien le 28 juin). Il a effectivement porté un intérêt sur les BCs, ce qui lui a permis de comprendre son intérêt dans notre domaine. Le premier point sur lequel nous nous heurtons sera dans les fonctionnalités même des SAE. Si les prestataires ont choisi d'être certifiés, ils sont dans l'obligation d'intégrer la fonctionnalité de chaînage des journaux, étant donné que c'est une spécificité dictée dans la norme NF Z42-013. La BC va ajouter un *partage de preuve*. Selon lui, il est déjà difficile de convaincre une institution d'adopter un SAE qui soit conforme à nos normes. Alors, il serait plus difficile encore de convaincre l'institution d'ajouter une couche de sécurité supplémentaire. Couche, qu'il considère ne pas être nécessaire, car elle n'apporte pas de valeur ajoutée. C'est pourquoi il ne s'est d'ailleurs jamais plus intéressé à la question de la confiance dans la technologie, dans le sens où, il n'est à ce jour pas persuadé que la BC soit utile dans le domaine archivistique. Argument, pour lequel

[14] Voir 2.3. Blockchain et souveraineté des données, p.48.

Archipels confirme qu'il faille toujours disposer d'une GED et d'un SAE (entretien avec H. Wahibi, 03 juillet). Là où la BC va ajouter une couche de sécurité en plus, c'est pour avoir *confiance en ces données* : je peux lui faire confiance parce que je suis en mesure de vérifier cette donnée. Lors de l'entretien, l'exemple a été rapproché avec la data visualisation. L'outil permettant de générer des tableaux de bord et des graphiques peut être excellent. Mais nous n'avons pas confiance dans les données affichées – pour quelconque raison - alors il n'y aura pas d'utilisation qui en sera faite. Antoine Meissonnier rejoint cet argument (entretien le 28 juin). La problématique de la confiance est tout à fait pertinente à questionner, car elle joue un rôle central. Les BCs qui vont jouer un rôle au sein de la "confiance documentaire" soulèvent l'interrogation que nous ne sommes pas en mesure de savoir avec certitude que ce qui est dans la BC est bien vrai. Il n y a pas de problème de sécurité derrière la BC, moyennant les couches logicielles qui sont ajoutées, la complication réside dans le fait que nous avons toutes nos raisons de douter de la sécurité, véracité et de la fiabilité des informations qui sont dans les blocs. Nous pouvons compléter avec les propos énoncés de Arnaud Gaudinat (entretien le 07 juin). Les BCs se sont des sortes de boîtes noires, dans lesquelles nous ne savons pas exactement si l'information présente au sein de la BC n'a pas été transformée d'une certaine manière. Le fait de ne pas disposer de la cuisine interne – son fonctionnement interne – nous permet de remettre en doute ces données. Ce qui est paradoxal puisque les BCs sont réputées pour être de nature transparente : la possibilité de partager les informations entre les nœuds. Ce qui est accessible ce sont les données et les smart-contracts inscrites sur les BCs. Nous ne pouvons pas analyser ceci plus loin, car il y a un manque de métrique commune, nous reviendrons sur ce sujet dans la partie suivante. Mais ceci implique qu'il est difficile de comparer les évènements. C'est pourquoi il faut avant tout gérer la qualité des données et la BC va pouvoir exercer un rôle à ce niveau grâce à la vérification de la donnée (entretien avec H. Wahibi, le 03 juillet).

Stéphane Schoffit (entretien le 19 juillet) apporte une comparaison intéressante avec le sceau de cire utilisé pour sceller les lettres au Moyen Âge. Cette technique garantit que le document qui a été envoyé n'a pas été trafiqué au moyen d'une ouverture par un individu malveillant ou par incident et donc garantir l'intégrité des données. Par contre, ce n'est pas le sceau de cire qui garantit le contenu de la lettre, mais la personne qui a rédigé le contenu.

Nous pouvons constater que nous nous retrouvons avec des moyens technologiques qui vont *moderniser* la confiance, avec une volonté de moderniser aussi les services d'archives, en particulier ceux qui font de l'archivage qualifié et de la préservation de la preuve (entretien avec C. Dubourg, le 15 juin). L'objectif est de donner une valeur légale avec la protection de cette preuve, dès lors que nous faisons appel à un service d'archivage qualifié, ce qui est un enjeu pour les entreprises.

Le principe du service d'archivage qualifié est actuellement en cours de discussion. Il y a une collaboration entre eFutura et la norme européenne sur ce sujet-là. Un rapport est en cours de rédaction afin de revenir sur la manière avec laquelle chaque pays européen a mis en place l'archivage électronique. Il y a un retour sur les grandes différences, l'usage fait entre les pays; de telle manière à produire, pour la révision des aspects de eIDAS 2.0, une norme. Cette dernière prendrait en référence des textes nationaux et viendrait compléter l'ensemble de ces textes pour avoir une **approche commune sur l'Europe**, ce qui pose justement

problème aujourd'hui. Et c'est le sujet sur lequel nous allons revenir dans la partie ci-dessous.

2.3. Blockchain et souveraineté des données

Archipels est une entreprise qui vend ses services par le biais de leur solution de BC de consortium. L'architecture décentralisée est majoritairement construite par des actionnaires à connotation publique : la Caisse des Dépôts, EDF, Engie, la Poste. Parmi ces derniers, le seul étant privé est Engie. Les autres organismes restent des acteurs avec des fonds publics. Ils ne se limitent pas à être actionnaires, ils sont également opérateurs de la blockchain, autrement dit : la BC dispose actuellement de 24 nœuds venant de ses actionnaires. Pour rajouter un nouveau nœud à la chaîne, il faut disposer de l'accord des institutions citées, puisqu'elles agissent en tant qu'opérateur. D'après Hanane Wahibi, commerciale pour Archipels (entretien le 03 juillet), le fait d'être porté par ces acteurs-là instaure déjà de la confiance, car ils sont identifiés. Ils vont agir comme étant les tiers de confiance. Christian Dubourg (entretien avec C. Dubourg, le 15 juin) rejoint cette pensée, il faut que la BC soit répartie avec des acteurs qui ont des enjeux de confiance partagée tous ensemble (BC privée, BC de consortium), dans ce cas-ci l'usage de la technologie fait sens. Il y a la création d'un système partagé, dans lequel les nœuds et les participants se mettent d'accord sur la manière de gouverner la BC et la façon avec laquelle elle sera technologiquement mise en œuvre. Donc s'il y a un désir de créer une BC afin de stocker des empreintes. Mais il faut tout de même qu'il y ait une confiance partagée. Or, ces BC présentent un risque : le défaut de gouvernance. Il faut la cadrer et vérifier que l'ensemble des risques potentiels soient pensés et couverts ; c'est ce qui permettra de créer un environnement dans lequel nous avons confiance les uns dans les autres. Et c'est l'objectif de l'Europe de demain.

Un second aspect qui apporte de la confiance est que chacun de ces actionnaires est d'origine française. Archipels émet la volonté de s'ouvrir pour bénéficier d'une dimension qui soit élargie à l'Europe. L'entreprise n'est donc pas fermée à avoir une ouverture vers une entité européenne. Mais, il faut s'assurer que l'interopérabilité entre les États soit faisable. C'est pourquoi aujourd'hui, il y a une dimension exclusivement française, mais que demain il y a de fortes chances qu'elle devienne européenne. Ceci rejoint l'argument de Stéphane Schoffit (entretien le 19 juillet), il y a actuellement un manque d'encadrement. Si volonté y a-t-il de développer plus d'applications au sein des BCs et donc des cas d'usage, alors il faut être vigilant aux impacts que cela aura sur le droit national et/ou européen. D'après lui, il y a deux conditions qu'il faut prendre compte :

- Si la BC reste une technologie qui est utilisée au même titre qu'un langage de programmation ou un disque dur, par exemple, alors il n'est pas nécessaire de s'armer d'une réglementation particulière.
- En revanche, si la BC devient un élément qui juridiquement peut avoir du poids, tel que garantir l'intégrité d'un document ou encore son authenticité[15] notariale;

[15] L'authenticité a un sens particulier dans le notariat qui diffère de celui que nous percevons dans le domaine archivistique. D'une part, il s'agit de l'intégrité du contenu du document (tout comme en archivistique), mais c'est aussi la garantie de l'identité des personnes qui ont signé et de leur bonne compréhension du contenu du document, ainsi que leur consentement à signer ce contrat. Il s'agit de l'engagement de la responsabilité du notaire. Tout le processus de signature (constitution du contrat à son explication, sa lecture ou son recueil des signatures, le consentement des signataires) a bien été fait dans les règles de l'art. Les signataires doivent avoir toutes ces facultés pour signer. Et c'est cet ensemble qui crée l'authenticité de l'acte.

alors oui, le cadre réglementaire actuel n'est pas suffisant. Il rejoint donc l'argument précédemment cité par Pascal Agosti et Eric Caprioli (2023) : la BC doit être encadrée au niveau de eIDAS 2.0., au même titre que la signature électronique.

D'après nous, il y a deux arguments qui sont ici soulevés par ces professionnels. Dans un premier temps et nous l'avons déjà abordé : l'incertitude quant à la sécurité derrière les BCs, dû au fait de son absence (actuellement) dans un référentiel certifié. Et d'autre part, l'absence de socle commun – une interopérabilité – nous permettant de jouir d'un socle de sécurité qui soit partagé par tous les Européens.

Arnaud Gaudinat (entretien le 07 juin) soulève un point dans la mécanique interne des BCs. Elle est une sorte de puits sans fond, il est possible de creuser toujours plus profondément, cependant, il est difficile d'avoir une personne qui maîtrise ces technologies. Le majeur problème avec les BCs ce sont les personnes qui sont derrière. Il s'agit d'un monde d'ingénieurs, plutôt que de chercheurs. D'ailleurs, chez Archipels, c'est une équipe d'ingénieurs qui est chargée de déployer la BC (entretien avec H. Wahibi, le 03 juillet). Nous autres pouvons comprendre le fonctionnement tel qu'expliqué dans le préambule de ce mémoire, mais nous ne serions pas aptes à mettre la "main dans le cambouis". D'ailleurs, le terme d' "ingénieurs blockchain" est relativement nouveau.

D'après Arnaud Gaudinat (entretien le 07 juin), les informaticiens ont plus de facilités à la comprendre. Cependant, lors des cours donnés à la filière *Informatique de Gestion* à la Haute Ecole de Gestion de Genève, il a constaté qu'il y a un manque d'esprit blockchain. Les étudiants ont tendance a rester dans le modèle de pensée classique. Développer les BCs requiert de penser autrement, penser différemment. Ceci implique que ce sont ces ingénieurs qui dirigent le marché, de ce fait, nous avons un manque de recul, nous ne savons pas exactement ce qui s'y passe. À nouveau, le même problème surgit : le manque de métrique commune définie, de standard, qui semble être intimement lié à l'immaturité de cette technologie ; il faut se remettre constamment à jour sur les innovations et les changements dans le domaine.

Face à ce constat, il y a aussi un manque de protocoles standardisés et qui ont atteint un degré de maturité suffisant (entretien avec A. Gaudinat, le 07 juin). Nous savons que ces protocoles fonctionnent, mais il y a un problème d'interopérabilité, puisque toutes les BCs n'utilisent pas les mêmes.

Ce sont des difficultés directement liées à la scalabilité et à la sécurité. Elles rejoignent également notre constatation émise sur le manque d'adoption commune dans un référentiel. A ce stade, il s'agit surtout de compétitions autour des BCs.

Si nous nous plaçons en tant qu'utilisateur final, désireux d'implémenter un service BC, nous voulons nous assurer que la technologie utilisée est connue. Ainsi, nous pouvons affirmer avec certitude que l'outil est qualifié au niveau européen, de ce fait, il y a tel degré de sécurité qui s'y applique : tel degré d'exigence, avec tel degré de sécurité juridique. Stéphane Schoffit, ajoute toutefois que le risque nul n'existera jamais. Le tampon eIDAS ne peut, par exemple, garantir que la signature électronique ne soit pas sans faille. Cependant, derrière un règlement comme eIDAS, il y a une multitude d'experts qui travaillent de manière collaborative pour fournir

un socle commun de sécurité. Nous rejoignons ce point soulevé, car la confiance n'est jamais garantie[16].

Selon Christian Dubourg (entretien le 15 juin), les référentiels de sécurité montent en puissance, ils vont permettre de vérifier qu'une entreprise de type tiers de confiance challenge son niveau de sécurité, que les sécurités informatiques sont remises à niveau en fonction de ces challenges (définis par l'OWASP, notamment). L'Europe a défini des standards à appliquer, pour chaque service européen et elle laisse l'initiative à chaque agence nationale de définir le référentiel et les acteurs qui vont vérifier que les sociétés qui souhaitent exercer ce service peuvent le faire, mais dans les conditions exigées. L'ETSI est, par exemple, en charge de définir les référentiels eIDAS. L'entreprise doit prouver que le service qu'elle preste a travaillé sur la sécurité. Certifier les tiers de confiance permet de vérifier que les exigences dictées par le référentiel soient bien respectées et appliquées. La notion de confiance va être utilisée dès lors que nous sommes aptes à faire confiance à un tiers, donc la confiance passe par l'usage d'un tiers. La confiance doit être validée. Pour cela, elle doit être reconnue par une entité qui va analyser que le service proposé est bien un tiers de confiance. Et cette confiance numérique, c'est eIDAS qui est aujourd'hui en mesure de l'accorder. Il s'agit d'une confiance qui certifie les tiers de confiance (comme les organismes de l'État), elle repose sur un référentiel de certification fondé sur les bonnes pratiques proposées par l'Europe. Le gage de sécurité est le standard européen, il est donc garant de cette confiance.

eIDAS 2.0 va aller plus loin que son prédécesseur (entretien avec C. Dubourg, le 15 juin). La confiance s'élargit envers une reconnaissance au niveau européen et par l'innovation de la preuve. Pour y arriver, il faut disposer d'informations législatives sur les pays de la preuve partagée. Par exemple, si nous utilisons un service de confiance de type SAE, les retombées ne seront pas les mêmes que si nous utilisons un service d'archivage français. La confiance passe par une "européanisation" : une reconnaissance des services de confiance européens, nommés dans eIDAS 2.0 : "trust service". Le service de confiance doit être transverse sur l'échelle européenne au moyen d'une validation des usages de ce service, peu importe qu'il ait été validé par l'agence nationale du pays dans lequel ce service est. Ainsi, les entreprises pourront utiliser le service d'un autre pays. À la condition que la législation soit mise en œuvre afin de la rendre indépendante de eIDAS 2.0. et d'instaurer un *partage de confiance*.

Toutefois, selon Arnaud Gaudinat (entretien le 07 juin), il faut aussi un équilibre entre la régulation et le "trop plein" de régulation, qui va empêcher et contraindre de manière excessive. En précisant toutefois qu'elle est nécessaire. L'entreprise Archipels (entretien avec H. Wahibi, le 03 juillet) suit également cette constatation. Le président du Board était auparavant directeur de l'ANSSI. Or, à date d'aujourd'hui, Archipels a fait le choix de ne pas avoir une certification ANSSI. Pour la raison qu'une certification les empêcherait d'innover dans leurs services, car ils viennent de se lancer dans de nouveaux projets : Digital Identity Wallet, smart-contacts, notamment. Se certifier provoquerait une limite pour eux, ils attendent donc de développer ces projets. La certification viendra d'ici une, voire deux années. Naturellement, la BC a été vérifiée en jurisprudence. En revanche, Archipels attend que la réglementation autorise des sujets BCs et que cette même réglementation accepte aussi des outils de BCs – ce qui pour le moment, semble être sur la bonne voie avec eIDAS 2.0. En somme toute, nous rejoignons l'argument de Arnaud

[16] Voir Partie 1) 2.1. Confiance entre les Hommes, p.25

Gaudinat : il faut trouver un juste équilibre dans cet univers de certifications et de réglementations. Mais il est indéniable que nous en avons besoin, tant qu'il n'y a pas de véritable standard technique, il y aura toujours des failles derrière les BCs (entretien avec A. Meissonnier, le 28 juin).

Un second obstacle a été émis par Stéphane Schoffit (entretien le 19 juillet) : l'éloignement géographique et temporel. Ceci a un rapprochement avec l'aspect purement technique des signatures. La signature électronique qualifiée permet au notaire de sceller les documents, une fois qu'ils ont été clôturés et validés au moyen d'une signature par le client. Mais qu'est-ce que la BC pourrait ajouter au sein de ce processus ? Aujourd'hui, peu ; demain, sans doute. Si nous avons la possibilité réglementaire et juridique de réaliser des signatures avec, d'une part, le notaire qui se trouve dans son bureau, et d'autre part, l'un de ses clients à Tokyo, l'autre à Bruxelles, et l'autre encore à New York. Dans ce cas, l'usage d'une technologie telle que la BC pourrait garantir l'intégrité des recueils de signatures et de la signature électronique en elle-même, entre ces différentes parties, dans un laps de temps défini. Que ce soit en même temps ou à quelques jours voire quelques heures près. Cependant, l'ADSN ne s'est pas lancée plus amplement sur le sujet. Les réflexions ne sont pas encore lancées parce que d'un point de vue réglementaire, c'est impossible aujourd'hui. Pour la raison que le client doit être face à son notaire pour procéder à la signature. Il n'y a pas d'intérêt à fait usage d'une quelconque technologie tierce. L'authenticité notariale est conférée par le fait que le notaire est présent, qu'il a un contact visuel avec son client et qu'il y a des échanges entre eux. À nouveau, nous pouvons constater que la réglementation n'est pas encore adaptée à la technologie et forme ainsi un frein face à son usage de manière plus courante dans nos pratiques.

Le dispositif commence toutefois à s'insérer pour certains actes de procuration. Il serait prochainement possible de faire signer directement les clients sur l'acte de procuration : le client étant à son domicile et le notaire dans son bureau, par exemple. Néanmoins, c'est encore restreint, puisque limité aux actes de procuration. L'acte final avec des vendeurs, des acquéreurs ou plusieurs personnes qui sont héritières d'un défunt n'est pas concerné. Cependant, Stéphane Schoffit pense qu'il faudra étudier cela demain, car la transaction pourrait être exécutée : plusieurs personnes sont en même temps en train de donner leur consentement à un même contrat et elles sont géographiquement et dans un temps dispersé. Dans ce cas, la blockchain pourrait éventuellement nous apporter une garantie supplémentaire qui prêterait son concours à l'authenticité. Mais aujourd'hui, nous n'y sommes pas encore.

2.4. Blockchain et modèle économique

Notre modèle économique repose essentiellement sur la création de gains, il faut qu'il y ait des rendements pour être rentable.

Les entreprises font face à une rude concurrence, c'est la raison pour laquelle il y a une course à l'innovation (entretien avec A. Gaudinat, le 07 juin). Les entreprises vont sortir des nouveautés afin de se réinventer. D'une part, il y a la question de la volatilité de ces entreprises/start-ups. Antoine Meissonnier (entretien le 28 juin) a constaté que d'une année à l'autre les entreprises qui développent des solutions BC ne survivaient pas. Il y a donc toute une part de notre confiance qui est fragilisée, car cela constitue un risque énorme. Nous pouvons rapprocher cela à une problématique que nous rencontrons dans le domaine archiviste : les formats de fichier. En effet, nous allons privilégier un format qui soit ouvert, avec une garantie

de stabilité sur le long terme, une interopérabilité, ainsi qu'une utilisation par un grand nombre de logiciels et un standard ouvert. Plutôt qu'un format fermé qui soit créé par une seule entreprise, dont nous sommes entièrement dépendants : si l'entreprise ferme ses portes, nous n'avons pas de garantie que le format soit encore lisible. Nous sommes face à un risque de perte de données. Dans le cas des start-ups qui développent des solutions BC, leur durée de vie ne dépasse pas une année parfois. Le problème majeur étant le manque de financement sur les activités proposées et les services rendus. Mais il est relativement difficile de survivre uniquement par ce facteur-ci, il faudra qu'elle mine pour être plus rentable et donc qu'elle utilise une cryptomonnaie.

Ensuite, il y a les institutions publiques : l'État. Nombreux sont les citoyens qui expriment un défaut de confiance – ou avec modération - envers cette institution. Toutefois, selon Antoine Meissonnier (entretien le 28 juin), il semble plus aisé d'accorder sa confiance envers cette institution, car elle présente une organisation sociale pluriséculaire, en d'autres termes : elle est faite pour perdurer. Nous reviendrons sur le rôle de l'État avec la BC au point suivant.

Notre modèle économique fonctionne à partir du moment où nous lui fournissons une valeur (entretien avec A. Meissonnier, le 28 juin). Dans le domaine archivistique, cette valeur est la confiance dans les records et les archives pour qu'elles puissent être utilisées. Mais comment pouvons-nous *fournir* cette confiance ? Une entreprise qui n'est pas renommée, qui ne s'est pas encore fait un nom sur le marché va être confrontée à cette défaillance de confiance. Cette dernière s'est bâtie à partir d'une construction juridique et sociale. Elle peut effectivement être attribuée par des institutions privées qui sont en charge d'une mission pour le service public, les notaires en sont un bon exemple. Pour finir, donner sa confiance à la technique (la BC) via des entreprises privées qui existent depuis peu, nous prouve que c'est particulièrement ardu.

Arnaud Gaudinat (entretien le 07 juin) complète cet argument avec un autre fondement de notre modèle économique qui est lié à la monétisation : la publicité et donc le marketing. Et derrière cette technologie, il y a beaucoup de marketing, c'est avant tout des incitatifs économiques. Nous vendons, nous voulons faire parler, c'est la raison pour laquelle nous entendons parler de la BC comme étant révolutionnaire, d'après Antoine Meissonnier (entretien le 28 juin). Il ajoute que cet enjeu économique est la raison pour laquelle la technologie n'est pas tant adoptée dans d'autres domaines. Les BCs de notarisation présentent des dysfonctionnements, car ce ne sont pas des modèles crypto, il s'agit d'un problème purement économique. Et ceci pourrait expliquer pourquoi la crypto est le seul cas d'usage qui fonctionne réellement à large échelle. Tout ceci étant virtuel et donc sans rapport avec le réel.

2.5. Le passé sulfureux des blockchains

> "*En 2008, les blockchains sont émergentes en informatique, avec l'article de Satoshi Nakamoto, mais quinze ans plus tard, cette technologie est déjà bien plus éprouvée, et critiquée*." (Di Pretoro, échange par mails le 14 juin).

Pendant les entretiens, l'histoire de la BC fut évoquée à plusieurs reprises. Dans notre état de l'art, nous sommes revenus dans le détail de son passé, qui nous l'avons vu, n'est pas des plus "carré".

Nous allons à présent confronter son historique avec la confiance. Dans ses fondements, la BC a été créée par un courant anarchiste : ni Dieu, ni Maître, nous sommes responsables de ce que nous faisons. Or, les gouvernements ne sont pas pro-anarchistes, bien au contraire, ce qui amenuise la crédibilité que nous avons envers cette technologie (entretien avec A. Gaudinat, le 07 juin). Sur le papier, le gouvernement existe, car il n'y a pas d'anarchie. La BC est teintée par l'histoire des cryptomonnaies qui est sombre. Et les BCs qui font parler d'elles sont celles qui gèrent les cryptomonnaies. Le problème est que l'objectif même des cryptomonnaies est d'être opposé à l'État, d'être libre (entretien avec C. Dubourg 15 juin).

Au vu de ce passé, il pourrait donc être difficile pour le gouvernement d'adopter la technologie, ceci pourrait véhiculer un message, c'est ce côté de gouvernance générale de la technologie qui pose problème à l'État. D'ailleurs, il n'est pas le seul à exprimer une appréhension envers la technologie. Les citoyens également (entretien avec H. Wahibi, le 03 juillet). Archipels le constate lorsqu'elle propose ses services. Les cryptomonnaies ont donné une mauvaise publicité aux BCs, c'est pourquoi ils doivent expliquer son fonctionnement au moyen d'un vocabulaire généraliste, car les BCs font peur. Cependant, il est possible d'utiliser la BC sans pour autant tokeniser ou miner. D'autant plus que si la crypto s'est intéressée à la BC, c'est parce que c'est un système particulièrement sécurisé dans son architecture.

Mais à nouveau, nous réutilisons cette notion de valeur : qui peut créer de la valeur ? Les gouvernements, les académies, les chercheurs aussi (entretien avec A. Gaudinat, le 07 juin). C'est pourquoi ils vont faire usage des technologies. Par exemple Chat GPT est de plus en plus utilisé dans ces domaines. La conclusion pour Arnaud Gaudinat, c'est l'aspect de la confiance qui se cache derrière l'accès à des données soient transparentes, que ce soit : pour les chercheurs ou les citoyens. Ce qui vient confirmer nos propos énoncés dans la première partie[17]. Et c'est aux gouvernements à travailler pour améliorer les technologies BCs. Une solution pour y parvenir est de favoriser le côté entrepreneurial. En somme, notre économie est fondée sur cet aspect-ci, autant l'utiliser pour que les gouvernements tirent, eux aussi, leur épingle du jeu.

Or, l'État refuse d'utiliser des moyens qui vont lui échapper (entretien avec C. Dubourg 15 juin). Pour y répondre, elle va apposer des réglementations sur une échelle nationale. Donc, l'État ne fait pas confiance aux technologies BCs. Mais si nous voulons parvenir à un degré de confiance au niveau européen, il faut que les États puissent avoir leur mot à dire et qu'ils travaillent ensemble. Les pays européens doivent reconnaitre ce moyen technologique. Au travers de l'Europe, chaque État dispose de registre partagé, mais il n'y a pas de partage de la confiance. Or c'est ce que promulgue eIDAS 2.0. En tant que citoyens, nous devons faire confiance à l'État, nous avons confiance, car l'État nous dit qu'il faut. Les actes notariés en sont un bon exemple : rédigés par le notaire, ce tiers de confiance au service de l'authenticité. Ils assurent leur autorité, car l'État le leur a délégué. D'après Christian Debourg, le seul moyen qui permette d'avoir une valeur de confiance, c'est d'avoir une BC partagée et elle n'est pas spécialement publique. Pour cela, l'État européen doit se mettre d'accord pour appréhender la BC, mais le chemin vers le registre partagé européen semble encore long. Nous l'avons dit plus haut, le partage de confiance est un élément, mais encore faut-il qu'il y ait des coalitions. Sans harmonisation, sans partage : nous ne pouvons pas nous faire confiance. L'Europe doit jouer son rôle

[17] Voir Partie 1) 2.2. Confiance dans les personnes morales, p. 27.

pour disposer d'une BC partagée qui soit abritée dans chaque pays. L'État européen aurait confiance dans la BC, tous les États se feraient confiance, donc nous aurions confiance dans la BC. Ceci avait été promulgué dans la version eIDAS de 2021, mais elle a été mise à mal et laissée en stand-by, sans que nous sachions les réelles raisons…

L'Europe de demain semble encore loin.

3. UNE BLOCKCHAIN REELLEMENT "DISRUPTIVE" ?

La littérature qu'elle soit professionnelle, scientifique ou généraliste relate que les blockchains vont révolutionner notre société. Cependant, la théorie semble bien loin de la réalité de terrain. En effet, secteurs privés et publics ne semblent pas l'accueillir avec autant d'entrain.

D'après Christian Dubourg, le domaine public est assez prêt, car il est en avance sur les idées, contrairement à ce que nous pourrions imaginer. En France, les participants aux normes et organismes de certification sont des acteurs privés, mais aussi des acteurs publics. Beaucoup d'initiatives sont faites, elles démontrent que le domaine public a pris confiance dans le numérique. Par exemple, la norme NF Z 42-013 a été co-révisée avec le SIAF. Mais cela est-il suffisant ? Notre étude de terrain nous prouve qu'il y a des intérêts forts à se tourner vers le numérique et les technologies. Cependant, la BC en elle-même reste difficile à s'implémenter, il y a une sorte de blocage. Néanmoins, ce blocage n'est pas mental, il y a une ouverture d'esprit vers la technologie, une curiosité, une volonté qui nous semble positif.

Antoine Meissonnier (entretien le 28 juin), reste interrogatif, il avait réfléchi pour l'utilisation de la BC avec l'État civil, car c'est un cas d'usage qui avait failli être imposé au Ministère de la Justice. Il a présenté un intérêt dans le domaine, car, du point de vue des projets de loi, il y a un amendement qui avait été déposé (mais qui n'est pas passé) par l'Assemblée Nationale. Il visait à obliger le gouvernement à faire une expérimentation BC sur l'État Civil. La mission qui s'occupe d'identité numérique au Ministère de l'Intérieur devait être associée au Ministère de la Justice pour faire une expérimentation. Antoine Meissonnier n'a plus eu de nouvelles concernant le cahier des charges qu'il avait dressé. Dans tous les cas, dans le POC, il transparaissait un manque de compréhension de ce qu'était la technologie et de ce qu'il pouvait en être fait. Or, selon l'archiviste, l'intérêt de la blockchain est quasiment nul par rapport aux SAE que nous avons aujourd'hui, comme cité précédemment. Le Ministère des Affaires étrangères a pris la décision que l'état civil des Français de l'étranger serait dématérialisé. Il s'agit du premier parti de l'état civil qui sera dématérialisé dans un SAE conforme à la norme NF 42-013, l'intérêt d'utiliser une BC comme couche de sécurité supplémentaire ne semble pas intéresser. Toutefois, nous considérons cet exemple positif : il y a eu des recherches dans le domaine, même si elles ne semblent pas avoir abouties. Un amendement a failli être instauré dans la loi pour réaliser des expérimentations au sein du gouvernement. Ce sont tous des exemples qui démontrent qu'il y a bel et bien une confiance qui existe dans la technologie, même s'il résulte en une suite d'échecs : la valeur de confiance est bien présente. Christian Dubourg (entretien le 15 juin) nous a prouvé d'ailleurs que l'État s'auto-fait confiance par défaut. Lorsqu'il s'agit d'une entreprise privée, il n'y a pas de confiance, sauf si elle est capable de démontrer sa capacité à faire confiance via une certification. Donc nous pouvons constater qu'au sein des certifications, il y a des journaux chaînés qui forment les prémices d'une

BC[18]. Ainsi, l'État fait confiance – autrement ils n'auraient pas mis ce que nous venons de citer en place - à la journalisation chaînée des empreintes. Nous pouvons conclure que l'État est déjà dans la confiance numérique de la BC. En revanche, son adoption, pour qu'elle sorte de la pensée strictement théorique, reste encore à prouver. Ces derniers propos viennent donc confirmer ce que nous avons énoncé dans la partie précédente.

L'entretien avec Stéphane Schoffit (entretien le 19 juillet) a permis de constater que le notariat est ouvert à aider la profession au moyen des technologies. Les notaires sont avant tout présents pour répondre à la loi et aux citoyens, c'est pourquoi il y a de réelles recherches pour déterminer comment les technos peuvent les aider. Nous trouvons également intéressant qu'il y ait un intérêt envers ces dernières afin de s'assurer qu'elles vont servir le droit et non pas le contraindre. De fait, il y a une volonté d'être le plus en avance possible sur une nouvelle technologie : anticiper pour mieux appréhender, afin de ne pas être surpris, d'avoir à s'y plier et que le droit se retrouve désavantagé d'une quelconque manière. La volonté de la profession est d'investir, de réaliser une veille et d'éventuellement être acteur de nouvelles technologies. Le début des années 2000 fut le vecteur d'un réel tournant pour le notariat qui a subi depuis cette date de nombreuses transformations technologiques. L'acte authentique a été privilégié sur support numérique et plus papier. Au départ, il y a eu des mouvements de méfiance. Mais avec du recul, nous ne pouvons que constater qu'aujourd'hui, c'est plus de 90% des actes qui sont dématérialisés et qui facilitent réellement le quotidien de la profession, sans pour autant remettre en cause le cadre juridique des actes. Stéphane Schoffit explique que c'est justement parce qu'ils ont investi dans la technologie : faire en sorte qu'il n'y ait pas de risque juridique, qu'il n'y ait pas de violation du droit et en retour une technologie qui leur vienne en aide. Les technologies sont venues apporter un changement de paradigme fort à la profession, donc.

Nous pensons qu'il s'agit là d'un vecteur de confiance non moindre. Le fait d'étudier la technologie pour la connaître, mieux l'appréhender, se placer dans une position qui permette de ne pas la craindre et d'imaginer des possibilités d'utilisation dans ce cadre. L'ADSN n'est pas (encore) convaincue par l'utilisation de la BC, pour la même raison qu'Antoine Meissonnier : quels usages leur apporterait-elle ?

C'est d'ailleurs la raison pour laquelle Archipels (entretien avec H. Wahibi, le 03 juillet) est actuellement bloqué dans l'évangélisation de la techno pour le secteur public, c'est un processus qui prend du temps. Pourtant, de notre point de vue, après avoir écouté chacun des entretiens, nous comprenons les raisons de cette avancée à tâtons. La technologie a été réfléchie et imaginée pour des cas d'utilisation précis dans le domaine archivistique et notarial, elle n'a pas été refoulée, bien au contraire. Il s'agit surtout d'une absence de poursuite pour les raisons que nous avons évoquées jusqu'à présent.

Le secteur privé, quant à lui, s'y intéresse fortement, surtout le domaine bancaire avec la partie cryptomonnaies et KYC (entretien avec H. Wahibi, 03 juillet). Plusieurs BCs ont d'ailleurs vu le jour, notamment de consortium pour le luxe. Le système bancaire s'y intéresse parce qu'il y'a la partie crypto et KYC. Il y a quelques blockchains qui ont vu le jour, avec des consortiums de blockchain de luxe, tel que l'Oréal, pour la traçabilité des produits. 80% des personnes qui viennent sur le site internet d'Archipels proviennent du secteur privé, tandis que très peu du

[18] Voir Blockchain et SAE

public. Ce dernier vient surtout par curiosité, "*ils sont au courant du sujet, mais **ils attendent de voir**, je ne sais pas quoi, mais ils attendent de voir"*.

Mais qu'attendent-ils de voir ?

Selon Antoine Meissonnier, les BCs ne fonctionneraient que dans le domaine des cryptos, c'est le cas d'usage qui a le mieux fonctionné. Il ajoute que derrière cette monnaie virtuelle nous ne pouvons pas à proprement parler de révolution, elle existait déjà bien avant l'apparition des BCs.

Arnaud Gaudinat (entretien le 07 juin) rejoint l'argument que derrière les BCs, il y a de nombreuses promesses et d'idées d'utilisation qui semblent pertinentes, de nombreux projets sont aussi créés ; mais sur le terrain, rien ne semble réellement adopté. Ceci peut être expliqué par le fait qu'il soit ardu d'en faire usage, car les BCs créent une réalité à elles-mêmes (entretien avec A. Meissonnier, le 28 juin).

En effet, la simple écriture dans la BC va avoir un effet sur le "réel", dans le sens où elle va transférer de la valeur (entretien avec A. Meissonnier, le 28 juin). Et justement, les BCs forment un système qui fonctionne parfaitement parce qu'il n'y a pas besoin d'avoir une référence au réel. C'est un circuit qui reste fermé, chacun s'échange de la monnaie – de la valeur – éventuellement des biens et des services, tout ceci peut être inclus dans les BCs. L'échange de valeurs est possible mais dès le moment où les individus désirent faire une action dans le réel, en s'échangeant de l'argent "palpable", des services, des biens ; alors c'est à ces individus qu'il incombe de réaliser cela dans le réel. Et s'ils n'ont pas ce qu'ils désirent en échange, la faute ne peut être portée que sur eux. Cependant, dans notre métier d'archiviste et pour l'usage que nous désirons faire des BCs, nous n'avons pas d'autres choix que de travailler avec ce rapport au réel : un document, un contrat, un bien immobilier. Et le monde notarial peut être directement rapproché à cet obstacle.

Nous sommes auparavant revenus sur l'authenticité notariale. Stéphane Schoffit (entretien le 19 juillet) rejoint la pensée d'Antoine Meissonnier, sur le principe qu'à elle seule, la technologie ne peut pas donner une équivalence à cette authenticité archivistique. En revanche, elle pourrait se limiter à y rajouter des éléments.

Arnaud Gaudinat avance qu'en interne, dans les institutions, il y a un manque de formations ou un manque de volonté d'être formé. Mais malgré qu'il y ait de nombreuses idées d'innovation, la technologie se met difficilement en place. D'un point de vue technologique (entretien avec C. Dubourg, 15 juin), la BC est très intéressante, mais elle n'a pas été faite pour l'usage que nous souhaitons mettre en place. Une autre explication pourrait être que nous avons un système actuel qui fonctionne et qui nous suffit (entretien avec A. Gaudinat, le 07 juin). Cela signifie-t-il que nous accordons uniquement notre confiance dans nos systèmes actuels ? La réponse se trouve dans les corps de métiers directement.

Selon Stéphane Schoffit (entretien le 19 juillet), le Groupe ADSN n'a pas trouvé d'avantages particulier à utiliser la BC par rapport à leurs "*bons vieux stockage très classiques*" qui sont actuellement utilisés afin de stocker les informations. Le Groupe n'a pas perçu la plus-value que cela pourrait leur procurer de disposer de cette double couche en plus de leurs serveurs. Il précise toutefois, qu'il ne reproche rien à la technologie en son fond, en revanche, il n'y a pas tellement d'avantages par rapport à leurs besoins. Nous pouvons résumer ceci par *: quelle est son utilité ? que peut-on en faire ?*

Cet argument est rejoint par Antoine Meissonnier (entretien le 28 juin). Au sein du Ministère de la Justice, il n'est pas le seul qui soit dubitatif en termes d'utilisation dans le domaine. Les informaticiens le sont également. Les problèmes que cette technologie pourrait résoudre sont assez flou : pour quels usages ? Il y a eu une telle vague de publicité autour des BCs, à tel point qu'il est pensé qu'elle peut être utilisée pour tout et donc nous essayons d'y voir des usages. Mais si nous réfléchissons dans le sens inverse, lorsque le Ministère de la Justice est confronté à des problèmes précis, la solution qui leur vient n'est pas la BC. L'aspect disruptif derrière les BCs proviendrait du fait que ça ait été imaginé par des personnes qui n'ont pas pensé ou fait le lien avec le rapport au réel que nous avons cité plus haut.

Archiviste et notaire interrogés n'ont rien contre la technologie, ils n'y sont pas fermés ou opposés. Tous deux n'ont, aujourd'hui, pas trouvé de cas d'usage particulier pour leur activité.

Les BCs sont aussi populaires pour leur immuabilité : impossible de changer les données une fois inscrites dans les blocs (entretien avec A. Gaudinat, le 07 juin). Mais en parallèle, nous demandons à cette technologie de pouvoir effacer des données pour quelconque raison. L'une d'entre-elles pourrait être le RGPD, par exemple, avec le principe de droit à l'oubli, de droit à l'effacement de nos données personnelles. Il faudrait creuser plus amplement la question. Mais, il semblerait possible d'effacer le document de l'endroit où il est stocké ou encore de simplement modifier l'empreinte pour qu'il n'y ait plus de lien entre les deux. Ces attentes peuvent obstruer la confiance que nous injectons dans le système. Mais Arnaud Gaudinat soulève un point : ceci ne serait-il pas artificiel ? Nous ne pouvons pas être à la fois effaçable et dans le même temps être immuable, c'est totalement contradictoire. Dans ce cadre, il faudrait éviter de saturer la blockchain de demandes et de besoins qui ne peuvent avoir une réponse, car nous considérons qu'il ne s'agit pas de remettre en question l'idéologie derrière le fonctionnement *mécanique* de la BC[19].

Un second raisonnement a aussi été mis en avant. Les BCs sont des systèmes qui s'auto-alimentent avec des incitatifs économiques (entretien avec A. Gaudinat, le 07 juin). Et ceci va changer le modèle, car aujourd'hui tout est économique et repose là-dessus. Or, selon Arnaud Gaudinat, il y a des opportunités pour rendre ce système plus durable. La durabilité, mot qui prend également tout son sens dans le domaine archivistique : être dans le temps, longévité, pérennité. Un argument permettant de s'interroger sur la confiance est évidemment sa durabilité dans le temps. La BC l'est-elle seulement ? Nous sommes revenus sur une partie de cette réflexion dans la section relative au modèle économique. Cependant, il nous semble légitime d'adresser ce sujet sous un autre angle encore : l'obsolescence technologique.

Dans le fond même, la blockchain bouge très peu en termes de niveau d'évolution. D'un point de vue purement technologique[20], les BCs sont relativement pérennes, car nous sommes en mesure de les entretenir. Le fait que les BCs reposent sur des incitatifs économiques, fait en sorte qu'elles ont été suffisamment bien conçues, car elles s'autoalimentent et deviennent autonomes (entretien avec A.

[19] Nous ne mettons pas ici en avant l'idéologie au sens de son passé historique, mais bien le fonctionnement interne.

[20] Dans ce paragraphe, nous omettons les risques liés au marché : si une BC se ferme suite à une trop grosse compétitivité. Nous désirons analyser la techno au sens purement mécanique.

Gaudinat, le 07 juin). Et ceci est justement une opportunité permettant de rendre ce système durable. Si nous nous intéressons aux BCs à elles seules (en omettant les couches applicatives qui sont ajoutées), nous sommes face à un fonctionnement qui est stable et qui procure un sentiment de confiance. Arnaud Gaudinat donne l'exemple du Bitcoin. Si un jour une partie des jetons veut continuer à être émis et l'autre partie non, d'autres intéressés viendront s'ajouter, parmi lesquels certains resteront sur le Bitcoin original et d'autres feront un nouveau Bitcoin. Mais tant qu'il y a de l'intérêt, il y a des usages.

Toutefois, nous considérons que la techno a été l'objet de réflexions et de recherches qui démontrent la confiance qui est injectée dans la technologie et que nous percevons encourageante pour tracer un avenir dans lequel les technologies BCs pourraient – éventuellement – intervenir.

PARTIE 3 : L'ARCHIVISTE COMME TIERS DE CONFIANCE

Des corps de métiers peuvent agir en temps que tiers de confiance. Ils peuvent ainsi gagner la confiance des utilisateurs du logiciel, programme : horodateur, labellisateur, prestataire de confiance.

Les BCs font sauter les tiers de confiance. Mais est-ce réellement le cas ? Ou est-ce que nous nous situons dans une situation qui soit – à nouveau – pour objectif de vendre la technologie et lui donner une bonne publicité ? Pour analyser cela, nous avons été chercher la réponse auprès des notaires directement. Notaires, huissiers de justice, greffiers, horodateur, prestataire de confiance agissent comme tiers de confiance. Ces professions réglementées exercent un poids dans notre société. Elles définissent les engagements à respecter entre des personnes, notamment. Ces professions possèdent une haute fiabilité qui les rend garants de la confiance, elles apposent un régime de confiance grâce à leur assentiment.

Pourrions-nous imaginer un futur qui se passe d'eux, pour exercer cela au sein des BCs ? Avons-nous suffisamment confiance en la technologie ? Pour cela, nous sommes partis d'exemples de terrain afin de nous positionner sur des cas concrets.

Selon Antoine Meissonnier (entretien le 28 juin), si nous enlevons les greffiers des tribunaux de commerce, par exemple, nous nous retrouvons rapidement face à des problèmes, car la mission des tribunaux ne se limite pas à enregistrer les actes, ce n'est effectivement pas un processus qui peut être réalisé de manière automatique. Derrière cet acte, le greffier va vérifier la légalité de l'entreprise, car ils ont avant tout un rôle de police administrative. Il est interdit de créer des entreprises qui ont des vocations illégales (proxénétisme, blanchiment, par exemple); des individus vont tenter de tout de même créer des institutions de la sorte. C'est le greffier qui va contrôler, il va analyser ce réel pour poser un regard analytique sur les activités de l'entreprise. C'est une action qui doit être réalisée par un humain et qui peut être dématérialisée ou automatisée sur une BC, uniquement.

Un second exemple donné par Stéphane Schoffit (entretien le 19 juillet) est relatif à la vente/achat de terrains. Une des applications qui est vendue avec les BCs est le stockage de morceaux des titres fonciers – via les smart-contract.

Nous pourrions imaginer que l'Etat détienne dans des registres basés sur la technologie blockchain toutes les transactions qui disent qu'effectivement Alice a bien vendu un terrain à Bob à telle date. Ceci pourrait être vérifiable et opposable juridiquement au moment où la transaction a été effectuée. Donc, si nous avons un contentieux devant le tribunal demain, nous pourrions aller chercher l'information dans cette blockchain. En revanche, nous ne pourrions pas imaginer effectuer un processus d'achat/vente reposant uniquement sur la BC, en enlevant les tiers de confiance. Il s'agit plutôt de l'inverse, l'utilisation de la BC en supplément, pour ajouter une sécurité technique complémentaire, mais nous pourrions nous passer de cette technologie. Pourquoi ?

Il y a tout un aspect humain qui intervient derrière une telle transaction. C'est la partie visible de l'iceberg : disposer des preuves nécessaires de la transaction au moyen d'un registre tracé. Mais la partie immergée de cet iceberg relève de l'expertise des métiers et elle est indispensable. Le notaire et d'autres métiers dans le domaine vont s'assurer que la vente aie été faite dans des bonnes conditions, que

la cliente Alice n'était pas sous la menace, qu'elle désirait réellement vendre sont terrain et que Bob exprime une volonté de le lui acheter. Ensuite, sur le terrain, il peut aussi y avoir des conditions qui s'appliquent : être averti que le voisin a un droit de passage, que la société EDF va prochainement placer un pylône sur le terrain, etc. Donc, lorsque l'information est inscrite au sein de la BC, elle est vraie, il ne faut pas plus. En revanche, si Alice dit à Bob "*Je te vends ma maison*", rien ne prouve que cela a réellement été exécuté dans le réel. La blockchain va se limiter à inclure une suite de chaînes de caractères qui l'indique (entretien avec A. Meissonnier, le 28 juin). Mais le fait d'exprimer que c'est bel et bien vrai, nous n'en savons rien. Nous n'avons rien qui nous prouve qu'Alice était bien détentrice d'une maison au départ, d'ailleurs. Toutes ces dispositions qui peuvent arriver donc physiquement, dans le réel, une BC ne peut pas nous l'apporter. Il faut un professionnel du droit qui accompagne les clients, le vendeur, l'acheteur qui vont s'assurer que le contenu de la transaction soit faite avec le maximum de sécurité juridique possible. Les BCs ne peuvent donc pas remplacer les tiers de confiance, car elles ne peuvent pas nous apporter toutes les actions qui vont intervenir de façon physique, au quotidien (entretien avec S. Schoffit, le 19 juillet). De plus, les BCs ne peuvent remplacer l'expertise humaine. Lorsqu'un terrain est acheté/vendu, il y a une masse d'informations qui sont à traiter. Les acheteurs/vendeurs seraient seuls et responsables d'aller chercher les informations, pour lesquels ils devraient se porter garant. Nous voyons dans notre exemple que la confiance ne peut être placée en ces individus, car ils ne possèdent pas les connaissances nécessaires dans le domaine, tout comme les BCs, finalement.

Dans ce cadre-là, si nous imaginons utiliser la BC dans le domaine archivistique, il y a besoin des archivistes pour attester que le document aie bien suivi le bon process et donc que les utilisateurs des documents puissent s'y fier et donc avoir confiance dans le contenu.

Le problème du rapport au réel qui a été énoncé pourrait être résolu en faisant intervenir les Oracles qui viendraient ajouter ce rapport au réel, de manière automatique, ce qui permet d'activer les smart-contracts. Antoine Meissonnier (entretien le 28 juin) ajoute toutefois qu'à l'heure actuelle, ceux qui agissent le mieux comme un Oracle, restent les humains - en qui nous avons confiance pour diverses raisons sociales, juridiques ; c'est-à-dire : les notaires, les greffiers, les archivistes. Sauf qu'Antoine Meissonnier n'imagine pas un univers qui ne repose que sur une automatisation via la BC. Premièrement, nos sociétés accueilleraient ceci de manière peu désirable. Deuxièmement, la soutenabilité environnementale que cela impliquerait serait désastreuse.

Par ces arguments, nous comprenons qu'il s'agisse d'une confiance qui s'établisse entre individus – en dehors du système des BCs. Si la confiance pouvait être exercée à 100% entre les Hommes, nous n'aurions pas de crainte quant à ce facteur de rapprochement au réel. Mais il est légitime de se demander si nous pouvons réellement avoir une confiance "aveugle" en tout un chacun ? La première partie de ce mémoire nous a démontré que nous ne pouvions pas agir comme tel. La question ne repose donc pas sur une remise en question de la technologie, mais bien de l'Homme. Nous pensons qu'il est effectivement ardu de confier notre part de confiance de la sorte, c'est d'ailleurs la raison pour laquelle nous mettons en place un ensemble de dispositifs, systèmes, technologies ; car les exemples du passé nous prouvent constamment qu'il est difficile d'avoir confiance entre individus que nous ne connaissons pas personnellement.

C'est pourquoi nous avons plus que jamais besoin des différentes professions qui agissent en tant que tiers de confiance. Elles existent car elles attestent que telles ou telles informations, si elles arrivent dans un système automatisé, elles n'y sont pas présentes de manière hasardeuse. Par exemple, les archivistes doivent être en mesure d'affirmer que dès lors qu'un document se retrouve dans le SAE, ceci implique qu'il est fiable, car il a fait l'objet d'une étude avant d'être versé, comme cité dans la seconde partie de ce mémoire[21]. Ceci confère aux utilisateurs des documents une confiance dans le système informationnel, mais aussi envers les archivistes.

Les arguments que nous venons d'exposer démontrent que nous avons plus que jamais besoin des tiers de confiance. Il semble même utopiste de vouloir s'en passer. Nous ne pouvons pas nous permettre d'accorder notre confiance sans avoir une quelconque assurance ou promesse en retour, comme cité dans les deux premières parties de ce mémoire.

Un second point qu'Antoine Meissonnier a soulevé, c'est qu'au sein des institutions publiques et dans le domaine de la notarisation, les personnes qui vont utiliser les BCs sont les greffiers, les tribunaux de commerce, les huissiers ; autrement dit, tous les intermédiaires de confiance. Et justement, il y a un enjeu de confiance qui se créée mais via ces intermédiaires de confiance, pas les BCs. En effet, nous avons confiance en ces intermédiaires. Et ces derniers utilisent la BC pour faire le lien entre le réel et la technologie. C'est la raison pour laquelle nous avons besoin de ces intermédiaires, sans eux, pas de confiance, car elle n'est pas créée au sein de la BC.

1. L'ARCHIVISTE, GARDIEN DE LA VALEUR PROBANTE

L'argument apposé dans la partie précédente, nous amène à penser que nous considérons les archivistes comme intermédiaire de confiance. De fait, l'archiviste fait partie des corps de métier agissant comme des tiers de confiance (Gobert, 2004). Notre intervention permet de créer "*un contexte dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée.*" (p.34)

Nos responsabilités sont élargies selon les évolutions technologiques, juridiques, économiques et organisationnelles :

> " *[…]. Ceci demande que les professionnels de la gestion documentaire appréhendent et répondent à un ensemble diversifié de besoins émanant de parties prenantes internes et externes. Ces besoins peuvent englober des attentes plus grandes en matière de transparence […] exprimées par des entreprises et des gouvernements, des citoyens, des consommateurs, des utilisateurs de services, des personnes visées dans les documents d'activité et d'autres parties intéressées […]*" (Organisation internationale de normalisation (AFNOR), 2016, p. 9)

Ainsi, en tant qu'archivistes/records manager, nous faisons aujourd'hui partie de la catégorie nommée les "*nouveaux métiers de la confiance*." (Poullet, 2009, p.186). Nous sommes un service de confiance, nous intervenons pour assurer la sécurité des opérations, dans le but d'assurer la conduite des activités et d'être en

[21] Voir Partie 2) 2.2. Blockchain et SAE, p.43

mesure de rendre compte à d'éventuels prestataires commerciaux ou administratifs, ainsi que des possible auditeurs (p. 197).

L'enjeu de nos professions en tant qu'archivistes sont d'assurer la conservation *pérenne* des documents d'archives numériques, quel que soit leur support, leur format, pour l'entièreté du cycle de vie qui a été défini pour cette typologie de document (Organisation internationale de normalisation (AFNOR), 2020, p. 22).

En tant que records manager, il s'agit de conserver les documents d'activité – les records – qui serviront de preuve pour la conduite des activités de l'entreprise dans le temps strictement nécessaire (Organisation internationale de normalisation (AFNOR, 2016, p. 9).

Ces deux domaines d'activité sont touchés par les mêmes attendus. En effet, pour qu'un document soit conservé dans le SI, il doit respecter certaines qualités. Le document doit être :

- **Authentique** : le document est le même que celui produit à l'origine, il est fidèle à l'identité qui lui est propre (Guyon, 2023, pp.13-14).
- **Intègre** : le contenu du document n'a pas été modifié par rapport au support original, il est considéré comme complet, il ne manque pas de parties. Ce critère se rapporte à l'aspect physique du document (p.20).
- **Fiable** : le document est en mesure d'attester la réalité de ce qu'il véhicule comme information (p.32).
- **Traçable** : il faut être capable de retracer l'ensemble du cycle de vie des documents (Leibenguth, 2019). Ceci permet de savoir : le ou les endroits où il a été stocké, qui l'a modifié, à quelle date.
- **Exploitable** : le document peut être localisé, interprété, récupéré, communiqué, et accessible pour une éventuelle utilisation (Makhlouf Shabou, 2019).

Ce sont autant de caractéristiques qui sont des notions présentent avec les BCs[22].

Cependant, nous connaissons un foisonnement dans le développement des technologies numériques depuis plusieurs années (Dubois, 2019), qui portent préjudice aux cinq caractéristiques que nous venons d'évoquer. Aujourd'hui, de plus en plus d'informations sont créées sous forme numérique. Ceci s'explique par l'augmentation radicale de la puissance des ordinateurs, des logiciels, des réseaux, des systèmes de stockage. Tout ceci est possible par la démocratisation des matériaux. Toutefois, l'ensemble de ces innovations auront des effets sur la longévité des technologies numériques. La concurrence économique des marchés déclenche un remplacement rapide des produits ce qui provoque leur obsolescence. C'est une réelle course à l'innovation qui est en marche. Cela entraîne une conséquence sur la conservation et l'exploitation des documents électroniques. Lorsqu'un dispositif de lecture devient obsolète, les données qu'il devrait interpréter deviennent alors inutilisables. L'instantanéité des systèmes d'information provoque un risque de non-disponibilité des preuves des ressources informationnelles (Poullet, 2009, p.198). Un courriel peut aisément se perdre dans la quantité de données présentes dans la boite mail. Le contenu d'un document électronique peut être modifié et falsifié en

[22] Voir la partie relative au fonctionnement des blockchains, p.16

peu de temps. Les sanctions d'un point de vue légal existent, mais elles sont souvent insignifiantes.

C'est dans ce contexte, que le terme de "*tiers-archiveur*" prend tout son sens (Girard, 2004). L'archiviste en tant que gardien de la sécurité et de la fiabilité (Poullet, 2009, p.17), reste toutefois limité par le manque de couverture juridique et l'archivage électronique est souvent délaissé. Dès lors, il y a une absence de critères minimaux à respecter. L'offre de services dans le domaine est insuffisant d'un point de vue légal et technique. Or, certaines questions s'avèrent tellement précises qu'il devient ardu d'y répondre en se référant au droit commun uniquement. Nous pouvons alors nous référer aux obligations minimales qui sont à respecter, en tant que tiers de confiance :

> "*Conserver l'intégralité des éléments électroniques reçus, […] prendre toutes les dispositions pour assurer la sécurité de l'archivage des éléments électroniques qui lui ont été confiés, […] n'adresser les éléments électroniques qu'aux seuls destinataires indiqués dans le contrat, sauf obligations légales, […] restituer les éléments électroniques sous une forme convenue, […] en fin de contrat ou en cas de cessation d'activité […] mettre à la disposition du donneur d'ordre les éléments électroniques qui lui avaient été confiés [ou] détruire les éléments électroniques sur demande écrite du donneur d'ordre et fournir à celui-ci une attestation de destruction."* (EDIFICAS & IALTA, 2000)

Ces besoins à respecter sont une partie du métier d'archiviste, notre profession nous impose déjà toutes ces règles. Remplacer le terme "*élément électronique"*, par "*document"* permet d'avoir la perspective de nouveauté du point du vue du support employé (Girard, 2004). Le tiers de confiance n'a donc rien de novateur, les archivistes font cela depuis toujours.

L'archiviste n'est pas face à un nouveau défi. Il est cependant indéniable que nos métiers tendent à se complexifier en fonction des innovations technologiques et des nouveaux matériaux utilisés (Belin & Rietsch, 2016). Les exigences citées par EDIFICAS & IALTA ne sont pas nouvelles. En revanche, les systèmes d'informations et les moyens techniques sont et vont continuer à être en perpétuelle évolution.

Si nous prenons l'exemple de la signature électronique, il y a un ensemble d'enjeux derrière la pérennisation de ces types de contenus. Les systèmes d'information et les SAE doivent assurer la préservation et la conservation des données sur un temps plus ou moins long. Mais encore faut-il avoir confiance dans le document qui est conservé dans l'outil[23] (Belin & Rietsch, 2016). Les enjeux de pérennisation sont secondaires, tant que la confiance dans le document n'a pas été attestée.

Tiers de confiance et archivistes disposent de nombreuses similitudes (Girard, 2004). Pourtant ils ignorent leur proximité, alors qu'ils ont les mêmes buts. Tous deux travaillent du point du vue de la valeur du document, condition fondamentale permettant d'avoir confiance en ce dernier (Belin & Rietsch, 2016). Les deux professions sont les témoins officiels de cette confiance accordée ou non au document. Le contenu de ce dernier, à savoir : son contexte de production et son intégrité permettent d'avoir confiance en lui. Nous sommes formés à garder ces

[23] Voir Partie 2) 2.2. Blockchain et SAE, p.43

notions à l'esprit et à les appliquer. Depuis toujours, le principe de confiance se situe dans le cœur de notre travail.

Or, nous devons maintenir l'accessibilité, la fiabilité, l'intégrité, l'authenticité et la traçabilité des informations numériques, sur une durée suffisamment longue, mais pour le temps strictement nécessaire. Dans une perspective de Records Management, les documents sont conservés pour leur valeur de preuve, qu'il faut garantir dans le temps. C'est ce qui va donner la légitimité de conserver les documents dans le SI.

Il faut penser à l'avance, c'est-à-dire maintenant, aux possibilités de changements technologiques, tels que l'arrivée de nouveaux supports, des formats de données ou des modifications dans la communauté d'utilisateurs; ce mémoire s'inscrit dans cette optique. Ceci permet de ne pas être surpris face aux évolutions à venir dans le spectre technologique. Il faut être dans l'optique d'anticipation, afin de prévoir, puis de minimiser les éventuels risques et leurs impacts. Même si nous avons adopté une analyse orientée BC, nous ne pensons pas qu'il y ait, à ce jour, une solution miracle, le numérique étant de nature instable. Ceci s'est d'ailleurs ressenti au travers des entretiens. Il s'agit de trouver des *compromis*. Cependant, nous pouvons considérer celles disposant d'un impact négatif moins important pour les records et les archives. En l'attente d'une autre solution qui puisse répondre différemment à nos problématiques causées par le numérique.

2. L'ARCHIVISTE DU FUTUR

Lorsque les effets d'une technologie se font ressentir, il y a des transformations au sein du métier qui surgissent :

> "*Comme dans tous les domaines - et en particulier dans le domaine de l'information - l'administration des archives ressent pleinement les effets des nouvelles technologies*." (Couture & Rouseau, 1987, p. 229)

Si la technologie se voit un jour être adoptée de façon plus courante, l'archiviste devra être préparé à subir bon nombre de changements. Nous sommes revenus sur la confiance qui pouvait être injectée dans les BCs, mais qu'en est-il du point de vue de la profession sur cette technologie ?

Nous n'avons pas pu interroger en masse des archivistes pour disposer de leur avis sur le sujet, il est donc difficile de parler au nom de tous. Les arguments ci-dessous se limitent à être des réflexions théoriques.

De manière générale, peu d'archivistes savent que les BCs peuvent jouer un rôle. La technologie est connue, mais de par son utilisation au travers des cryptos. Il existe aussi peu de "spécialistes" dans le rapport entre les BCs et nos métiers. Disposer d'entretiens pour répondre à notre problématique ne fut donc pas aisé.

Selon Antoine Meissonnier (entretien le 28 juin), ceci peut s'expliquer par le fait que nous sommes peut-être meilleurs pour utiliser des outils numériques, au sens de la valorisation, de la diffusion de nos données, il y a de plus grands intérêts.

Nous avançons également l'argument que nous allons rechercher les potentiels d'une technologie si nous savons qu'elle pourrait jouer en notre faveur, tant qu'il n y a pas de plus-value derrière celle-ci, l'intérêt semble être moindre. Emmanuel Di Pretoro (échange de mails le 14 juin), chargé de projet numérisation pour la commune d'Uccle, les technologies doivent être une "*proposition de solution à un problème*", ceci s'est d'ailleurs ressenti au travers des entretiens.

De fait, Antoine Meissonnier a fait des recherches car il travaille pour le droit de la preuve électronique au Ministère de la Justice. Les BCs ont été promulguées comme étant une technologie permettant d'agir sur la preuve des actifs numériques, il considérait qu'il pouvait donc y avoir un potentiel intérêt. Il s'est formé pour être en mesure d'évaluer en quoi la technologie viendrait en aide dans son domaine, mais également de *peser les risques.* Ceci rejoint l'argument de Stéphane Schoffit que nous avons cité dans la deuxième partie. Le notariat et le domaine archivistique se rejoignent car il y a une approche technico-juridique : il faut être en mesure de mélanger le droit avec la technique. De plus, en tant qu'archiviste, nous considérons qu'il faut disposer d'un minimum de connaissances. En effet, cela permet de conseiller l'institution - pour laquelle nous travaillons - sur la mise en place d'un système/dispositif permettant de témoigner de la valeur probante.

Les archivistes doivent avoir une appétence, une ouverture d'esprit pour des sujets plus techniques et comprendre la technicité d'un système rapidement. Il n'y a pas de formations spécialisées, c'est un enseignement qui se fait au fil des échanges, des discussions avec d'autres corps de métiers ou d'autres archivistes plus avancés sur le sujet. Ce mémoire en est d'ailleurs la preuve. Et ce sont toutes ces conditions qui vont, finalement, donner aux archivistes les armes permettant de comprendre les implications derrière les outils technologiques. Mais aussi de l'a décrypter afin de comprendre au minimum l'outil pour parvenir à se positionner et prendre une décision qui soit la plus judicieuse possible pour l'organisme.

Antoine Meissonnier (entretien le 28 juin) prend l'exemple des vracs bureautiques et le classement d'un fonds d'archives papier. Nous devons comprendre le contexte de production, le(s) producteur(s), son organisation, l'activité du(des) producteur(s), etc. Ce sont autant de compétences qui mettent en avant que nous avons les aptitudes pour comprendre une matière qui nous est inconnue, le cadre juridique qui intervient, les contraintes techniques, etc. Pour à terme, proposer une solution. Notre métier est aussi régi par des normes et des standards, c'est un métier particulièrement contraint, mais qui nous donne les clés pour comprendre un système et la documentation technique s'y appliquant.

Mais ceci demande un investissement personnel relativement fort et nous sommes avant tout une profession qui, d'après Antoine Meissonnier (entretien le 28 juin), se situe plutôt dans les sciences humaines, avec une part scientifique plus minime, mais qui doit transparaître.

Selon Arnaud Gaudinat (entretien le 07 juin), la technologie est encore en mouvement, ce qui ajoute une forte complexité, que le monde archivistique et du records management n'a pas encore pris en main. Ceci est peut-être un désintérêt dû à la difficulté de compréhension de son fonctionnement ? Un manque de temps à disposition pour creuser plus en détail le sujet ? Un ensemble d'hypothèses qu'il serait intéressant à creuser pour comprendre cette timidité face aux BCs.

Emmaunel Di Pretoro (échange par mails le 14 juin) ajoute que les BCs sont souvent qualifiées de "technologies émergentes" et de "technologies de rupture". Mais ces termes en eux-mêmes sont trompeurs, car les résultats se trouvent être souvent moindres par rapport à ce qui est espéré ou attendu de la technologie. Nous l'avons d'ailleurs prouvé dans la seconde partie du mémoire. Or, chacune d'entre elles va se développer à un rythme différent, selon les disciplines. Peut-être qu'il s'agit donc d'une question de temporalité et de patience, avant que les BCs trouvent une utilité supérieure dans notre domaine ?

3. VERS UNE SPECIALISATION DU METIER DANS LES TECHNOLOGIES ?

Nous avons un pressentiment que la technologie pourrait être poussée plus amplement car le sujet ne semble pas être clos.

Nous avons adopté une analyse orientée BCs, nous avons considéré un seul système, mais il faut peser nos mots. En effet, Emmanuel Di Pretoro (échange par mails le 14 juin) avance qu'il faut maîtriser plusieurs technologies, pour résoudre une plus grande variété de problèmes, car une technologie est avant tout un outil spécifique. Se tourner vers un seul outil est un biais de jugement, qu'Emmanuel Di Pretoro qualifie ceci de "*loi de l'instrument*", terme inventé par Abraham Maslow[24]. Il s'agit d'assurer un régime de confiance excessif dans un seul outil, ce qui implique que nous allons résoudre tous les problèmes en se limitant à l'utilisation d'un unique outil. Nous suivons cet argument, car nous ne pensons pas qu'il y ait, à ce jour, une solution miracle unique. Le numérique est de nature instable, il faut trouver des compromis. Il faut considérer les technos qui disposent d'un impact négatif moins important pour les records et les archives. En l'attente d'une autre solution qui puisse répondre différemment à nos problématiques causées par le numérique, en évitant de mettre toutes nos chances dans une seule techno. Précisons que nous avons évoqué dans la seconde partie[25] qu'il pourrait y avoir des problématiques de sécurité, si la BC était externalisée, il faudrait donc mener une étude plus approfondie sur le sujet, il s'agit ici de trouver une solution pour remédier aux manques qui ont été évoqués au cours des entretiens.

Nous pensons que le rôle des archivistes est de déceler des solutions, au moyen de groupes de travail et de POC, face aux problématiques que le numérique engendre. Le numérique nous impacte tous et toutes à de nombreux niveaux, les archivistes disposent de connaissances et compétences non négligeables, qu'il faut mettre en commun en favorisant l'intelligence collective avec d'autres corps de métiers. A ce jour, il manque cruellement d'archivistes orientés BCs, pour les éventuelles raisons énoncées tout au long de ce mémoire. Mais qu'en est-il des autres technologies ? Rencontrent-elles la même pénurie d'archivistes spécialisés ?

D'autres technologies à potentiel élevé pourraient faire l'objet d'un travail de recherche similaire. Nous pensons au format de fichier "*Parchive*", qui est un code d'effacement (Gallagher, 2001). Dans le cas où une partie d'un fichier se retrouve endommagée suite à un partage sur un canal ou d'un stockage peu optimal, ce format va pouvoir le réparer. C'est une fonction qui nous semble intéressante à envisager avec les BCs, dans le cas où l'institution ne dispose pas d'un SAE.

Ensuite, pour une institution qui n'a pas les moyens d'avoir un SAE, il pourrait être envisagé d'utiliser les BCs comme roue de secours en remplacement aux journaux chaînés. La BC pourrait ainsi être utilisée pour réduire les risques de non-disponibilité des preuves. La conservation pérenne des documents serait toutefois non adressée. Si tel est le cas, les archivistes se verront dans l'obligation de s'adapter.

C'est justement cette adaptation qui est intéressante. L'apprentissage est continu, car les pratiques vont évoluer, tout comme les technologies. L'archiviste devra s'informer dans les technos pour lesquelles il dispose de peu de connaissances

[24] Pour en savoir plus sur la loi de l'instrument de Maslow : https://www.observatoire-ocm.com/management/loi-de-linstrument/#:~:text=La%20loi%20de%20l'instrument,dans%20le%20monde%20du%20travail.

[25] Voir Partie 2) 2.1. : Blockchain et sécurité, p.41.

préliminaires. Il ne nous semble pas nécessaire de se spécialiser dans une technologie, en particulier, comme précisé dans la conclusion du préambule[26]. En effet, nous ne comprenons pas le fonctionnement purement informatique et mathématique derrière les BCs, nous laissons cela aux métiers qui y sont dédiés. En revanche, disposer d'une compréhension de base est plus que nécessaire pour comprendre les enjeux et les aboutissements, d'une part pour la profession ; et d'autre part, pour les implications qu'elles engendrent sur l'institution en question. Les entretiens que nous avons effectués le démontrent.

[26] Voir Fonctionnement des blockchains, p. 16.

CONCLUSION

Les arnaques, les fraudes documentaires, la cybercriminalité ne font qu'augmenter. Pour y remédier, nous sommes constamment à la recherche de solutions permettant de solutionner les problèmes soulevés, d'où la recherche du potentiel derrière les technologies BCs pour le domaine archivistique. Nous avons analysé l'usage possible de cette technologie pour garantir la fiabilité, l'authenticité et la traçabilité des archives et des records. L'objectif de ce mémoire était de nous questionner sur le régime de confiance que nous sommes en mesure d'injecter dans les BCs.

La littérature scientifique n'est pas en mesure de répondre à notre problématique, elle apporte des propositions d'innovation en reliant les applications avec des usages. Cependant, ces solutions ont été pensées dans un cadre qui restait théorique. La pratique en elle-même montre une tout autre réalité. C'est pourquoi la réponse se trouve directement auprès des professionnels. Néanmoins, il fut difficile de trouver des personnes s'intéressant au sujet. Les BCs ne sont pas les premières solutions trouvées pour apporter les preuves nécessaires dans les archives.

Aujourd'hui, il n'existe pas un système qui soit sans faille, qui ne peut être corrompu. Et il en est de même pour la confiance. En effet, nous avons vu dans la première partie qu'il n'existait pas de confiance qui soit acquise et totale à 100%, il faut sans cesse la travailler, la revoir. Ceci implique qu'il faut choisir l'option la plus sûre à l'heure actuelle. De l'immuabilité à la traçabilité ; pour l'ensemble du cycle de vie, de la création du document, jusqu'à sa destruction ou sa conservation pérenne. Autrement dit : "*penser le mieux, éviter le pire*" (entretien avec A. Gaudinat, 7 juin).

Au travers des entretiens, nous pouvons conclure qu'aujourd'hui nous sommes encore en phase de transition. Des réflexions sont surtout menées pour se renseigner sur les capacités de la technologie, mais peu est encore mis en place. Il y a de nombreux doutes quant à l'usage qui peut en être fait pour la gestion des archives et des records. Le domaine notarial évoque cette même problématique. Le rapport au réel fut plusieurs fois évoqué au cours des entretiens. Il est difficile de faire reposer l'ensemble de la gestion documentaire sur la BC, car nous ne pouvons avoir confiance dans les Hommes pour nous assurer que la transaction a bien été réalisée physiquement. D'où l'importance des tiers de confiance qui sont responsables de tenir un régime de confiance, entre la BC (si elle est utilisée) et les clients/utilisateurs.

Puis, le type de BC utilisé va agir sur la confiance dans la technologie. Si la BC est privée ou de consortium, ce sont les nœuds du réseau qui décident qui peut avoir accès ou non. Il faut donc que les utilisateurs aient une confiance absolue et totale dans ces derniers pour qu'elle puisse être pleinement utilisée. Il nous semble invraisemblable de faire usage d'une BC publique, la confiance ne peut être accordée en tout un chacun pour la gestion des documents d'archives d'une institution, il s'agit d'un travail qui doit être strictement limité en interne. Cet argument a été confirmé dans la première partie du mémoire : au plus des personnes sont impliquées dans un régime de confiance, au plus les risques d'abus seront visibles.

Ensuite, si la BC est effectivement utilisée pour ajouter une couche de sécurité supplémentaire, il reste le problème des empreintes numériques. En effet, les hashs ne vont plus correspondre dès qu'il y a une altération effectuée sur le document. Or, nous n'avons pas d'indications supplémentaires quant aux modifications opérées,

seulement que le document n'est pas une copie fidèle et fiable de l'original. De même, le SAE va opérer des transformations sur le document, dans le but d'assurer sa conservation pérenne. Ceci enclenchera une modification du hash, tandis que le document sera toujours considéré comme authentique, d'un point de vue archivistique.

Enfin, la technologie n'étant pas capable de stocker l'entièreté des documents, les organismes sont toujours dans le besoin de conserver leur SAE et GED. Les BCs se limitent à enregistrer des empreintes, les horodatages, des métadonnées, autrement dit, des "bouts" de documents. C'est pourquoi elle va plutôt ajouter une couche de sécurité supplémentaire, couche qui n'est pas perçue comme utile en comparaison à nos outils plus "traditionnels". Or, si nous nous référons à la loi de l'instrument de Marlow, il pourrait être effectivement utile de disposer d'une couche de sécurité supplémentaire pour ne pas tout faire reposer sur le SAE, par exemple. Ceci permettrait de disposer d'une sécurité à double niveau. Toutefois, cela reste théorique, au cours des entretiens nous avons été confrontés à la réalité de terrain, qui ne voit pas les solutions que la technologie pourrait apporter en plus.

Rappelons que nous ne sommes pas capables de décrire avec certitude lorsque nous nous situons dans un régime de confiance, car elle se remarque plutôt par son absence. Ceci fut confirmé au fil des entretiens, les esprits restent ouverts, les startups et autres entreprises qui proposent leurs services BCs sont tout de même entendus. Archipels a pu démontrer ses produits et services au Ministère de la Justice, ainsi qu'à l'ADSN. Nous considérons ceci positif, car il y a une volonté de s'armer des technologies pour faciliter les processus métiers. Il s'agit ici d'une confiance dans les technologies dès lors qu'elles sont considérées comme utiles.

Dans une ère régie par le numérique, des problématiques surgissent, mais il y a tout de même une envie de s'aider, en retour, d'autres technologies qui sont susceptibles de pallier les défauts de la première. Par exemple, l'historique teinté des BCs n'a pas pour autant suffi à diminuer la confiance dans la technologie, pour les personnes qui ont réalisé la démarche de s'informer sur cette dernière. Cependant, il faut être vigilant lors de l'ajout d'autres technologies à la BC, au plus elle est externalisée, au plus il y a des risques de défaut en termes de sécurité. Il faut donc parvenir à trouver le juste de milieu, à faire des expérimentations, afin de parvenir à trouver le bon équilibre.

Nous pouvons conclure que nous avons été confrontés à un ensemble de spécialistes qui se sont tous et toutes intéressés à la technologie. Nous avons un réel clivage qui se forme entre les personnes partisanes des BCs qui y voient un avantage en matière de sécurité supplémentaire et d'ajout de données concernant les preuves des actions menées sur les documents. Et d'autres qui ont exprimé une curiosité face aux BCs, mais qui après s'être formés, n'ont pas perçu les bénéfices pour leur profession. Nous avons donc deux tempéraments différents face à la technologie. Le second tempérament est une confiance qui peut être rapprochée à la confiance économique et philosophique citée dans la première partie de ce mémoire. Il y a une recherche d'intérêt, de bénéfices, d'avantages qui pourront être tirés de la relation BC/Archives-Records.

En revanche, nous avons pu constater que la question de la confiance n'a pas été questionnée davantage. Celle-ci semblait intervenir naturellement lors du processus d'autoformation, car la confiance s'établit au fil des échanges et des discussions avec d'autres professionnels, car la part d'inconnu doit être minimisée. Toutefois, nous avons constaté que la confiance est présente dans la technologie,

autrement, elle n'aurait pas été envisagée/étudiée pour un éventuel usage. Les experts qui expriment une réserve face aux BCs ne sont pas *fermés* quant à un éventuel usage. Il serait plus juste de déclarer qu'ils sont dans l'attente. Que ce soit pour d'autres cas d'usage pertinents qui se rapprochent de leur domaine ou une avancée dans les normes et dans la législation, par exemple. Il semblerait donc que la technologie n'a pas (encore ?) fait ses preuves dans les domaines étudiés. Cette constatation nous rapproche de la confiance telle que perçue dans les sciences politiques et des sciences du management : la confiance est un jugement collectif, les archivistes semblent être dans l'attente que des expériences positives et utiles soient réalisées, la confiance est établie sur un ensemble de valeurs, de règles qui sont instaurées par une autre catégorie d'agents. La confiance se crée par la collaboration.

Les technologies à elles seules ne sont pas dangereuses, mais elles dépendent grandement de l'utilisation que les Hommes en feront. Néanmoins, la fracture numérique qui s'inscrit avec la dépendance aux technologies, car nous craignons qu'elle s'étende de plus en plus, mais ceci est de l'ordre d'un nouveau travail de recherche à mener.

En définitive, nous ne nous situons pas dans une confiance innocente, elle est d'ordre purement rationnel. La part émotionnelle qui existe dans les relations sociales n’entre nullement en considération, car elle est un risque, elle place l'institution dans une position de faiblesse. La confiance n'est pas multidimensionnelle, elle se situe uniquement dans une protection des intérêts de la conservation des preuves dans les documents.

Ce mémoire permet de croiser le domaine archivistique avec les technologies. En effet, l'avenir semble s'ouvrir vers des technologies – qu'elles soient anciennes ou nouvelles. Il est intéressant de les questionner pour un éventuel usage dans notre secteur afin de faciliter nos tâches, de garantir la préservation et gestion des documents sur les court ou long termes dans le but de renforcer notre confiance dans le numérique. Notre métier est-il voué (ou contraint ?) à se voir modifier pour être plus orienté vers les technologies à venir ? Les formations vont-elles subir des changements pour apprendre à utiliser des technologies possiblement intéressantes ? Sommes-nous voués à être des e-archivistes ?

L'avenir nous le dira.

SOURCES

- Arnaud Gaudinat : Professeur en sciences de l'information à la Haute Ecole de Gestion de Genève. Formation d'ingénieur en informatique.
  - Visio Teams le 07 juin 2023.
- Emmanuel Di Pretoro : Chargé de projet de numérisation pour la Commune d'Uccle (Bruxelles).
  - Plusieurs échanges par mail du 23 mai au 14 juin 2023.
- Christian Dubourg : Consultant expert en gestion de contenu et de management, membre du working group blockchain.
  - Appel téléphonique le 15 juin 2023.
- Antoine Meissonnier : Chef du département des archives, de la documentation et du patrimoine pour le Ministère de la Justice.
  - Appel téléphonique le 28 juin 2023.
- Hanane Wahibi : Account manager chez Archipels pour la blockchain, self sovereign identity, le Web 3.
  - Visio Teams le 03 juillet 2023.
- Stéphane Schoffit : Directeur des produits et services métiers de l'ADSN.
  - Visio Teams le 19 juillet 2023.

BIBLIOGRAPHIE

Historique des blockchains

Organisation internationale de normalisation (AFNOR). (2022). *NF en ISO 22739 : Chaîne de blocs et technologies de registres distribués : Vocabulaire*. AFNOR. https://viewerbdc.afnor.org/pdf/viewer/oQPEnXey7rI1?proxy=true

✷ Monographies :

Assange, J., Appelbaum, J., Muller-Maguhn, A., and Zimmermann, J. (2016). *Cypherpunks: Freedom and the Future of the Internet*. New York, NY: OR Books.

Bouzeghoub, M., & Mosseri, R. (2017). *Les Big data à découvert*. CNRS éditions.

Calderan, L., Laurent, P., Lowinger, H., & Millet, J. (2015*). Big data : Nouvelles partitions de l'information : Actes du séminaire IST Inria*, octobre 2014. De Boeck Supérieur.

Chouli, B., Goujon, F., & Leporcher, Y.-M. (2017). *Les blockchains : De la théorie à la pratique, de l'idée à l'implémentation.* Eni ed.

Leloup, L. (2017). *Blockchain : La révolution de la confiance* (Vol. 1). Eyrolles.

Lewrick, M., & Di Giorgio, C. (2019). *Au cœur de la blockchain : Explorez le nouveau champ des possibles*. Pearson.

Quiniou, M. (2019). *Blockchain : L'avènement de la désintermédiation*. iSTE éditions.

✷ Chapitre de monographies utilisées :

Fanet, H., & Duranton, M. (2017). Les technologies au service du Big Data. In *Les big data à découvert* (pp. 26-27). CNRS éditions.

✷ Articles et ouvrages scientifiques

Brasseur, C. (2016). Chapitre 1. Qu'est-ce que le big data ? In *Enjeux et usages du big data* (Vol. 2, p. 7-24). Lavoisier. https://www.cairn-sciences.info/enjeux-et-usages-du-big-data--9782746247581-page-7.htm

Dhérent, C., Grimoüard, C. S. D., Ott, F., & Brouland, M. (2009). Comprendre les enjeux et les fondamentaux. *Documentaliste-Sciences de l'Information*, *Vol. 46*(2), 32-42. https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2009-2-page-32.htm%23pa1

Findlay, C. (2017). Participatory cultures, trust technologies and decentralisation : Innovation opportunities for recordkeeping. *Archives and Manuscripts*, 45(3), 176 190. https://doi.org/10.1080/01576895.2017.1366864

Hoffman, M. R., Ibáñez, L.-D., & Simperl, E. (2020). Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization : A Systematic Review and a Framework. *Frontiers in Blockchain*, 3. https://www.frontiersin.org/articles/10.3389/fbloc.2020.00035

Lacoursière, M. (2007). Analyse de la trajectoire historique de la monnaie électronique. Les Cahiers de droit, 48(3), 373 448. https://doi.org/10.7202/043936ar

Lafountain, C. (2022). Libraries, blockchain, and decentralized archives. *Computers in libraries*, *42*(8), 22-25. file:///C:/Users/celin/OneDrive/ENSSIB/MASTER2/UE5_InitiationRecherche/Bibliographie/20221110_LibrariesBlockchainDecentralizedArchives_ArticleRevue.pdf

✷ **Sources de sites internet :**

Audureau, W. (30 novembre 2016). *De Napster à zone téléchargement, petite histoire du piratage sur Internet.* Le Monde.fr. https://www.lemonde.fr/pixels/article/2016/11/30/de-napster-a-zone-telechargement-petite-histoire-du-piratage-sur-internet_5040900_4408996.html

babric. (16 décembre 2021). *L'histoire de la cryptographie*. Collégiens Lycéens Ensemble. https://webmedias.ac-nice.fr/colivensemble/2021/12/16/lhistoire-de-la-cryptographie/

Cagle, K. (21 janvier 2015). *Understanding the Big Data Life-Cycle*. Linkedin. https://www.linkedin.com/pulse/four-keys-big-data-life-cycle-kurt-cagle/

Chaulin, C. (3 février 2022). *Qu'est-ce que la révolution industrielle ?* Geo.fr. https://www.geo.fr/histoire/quest-ce-que-la-revolution-industrielle-208173

CIGREF. (9 avril 2013). *Cryptologie, histoire de "l'écriture secrète"*. Histoire-cigref.org. https://www.cigref.fr/archives/histoire-cigref/blog/cryptologie-histoire-de-l-ecriture-secrete/

Commission Nationale de l'Informatique et des Libertés. (25 octobre 2016). *Comprendre les grands principes de la cryptologie et du chiffrement*. CNIL : Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles. https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Commission Nationale de l'Informatique et des Libertés. (s. d.). *Big data*. CNIL : Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles. Consulté 28 mars 2023, à l'adresse https://www.cnil.fr/fr/definition/big-data

Ichbiah, D. (25 mars 2023). *Quelle est la différence entre le Web1, le Web 2.0 et le Web 3.0 ?* Futura. https://www.futura-sciences.com/tech/questions-reponses/internet-difference-web1-web-20-web-30-17368/

Kennassiri. (7 janvier 2014). *Une histoire de l'informatique [Billet]*. Hypothèses : introduction à l'architecture de l'information. https://archinfo01.hypotheses.org/770

Lumni. (14 juin 2022). *L'invention de l'imprimerie*. Lumni enseignement. https://www.lumni.fr/article/l-invention-de-l-imprimerie

Lumni. (14 juin 2022). *Les moines copistes du Moyen Âge*. Lumni enseignement. https://www.lumni.fr/article/les-moines-copistes-du-moyen-age

Maupu, G., Boudin Le Bihan, G., & Percot, S. (2019*). L'histoire des réseaux pair-à-pair ou repères historiques pour comprendre l'évolution du P2P (peer-to-peer).* Académie de Nantes. https://www.pedagogie.ac-nantes.fr/medias/fichier/t1-internet-ressource-documentaire-histoire-p2p_1562663870592-pdf?ID_FICHE=1424110212620&INLINE=FALSE

May, T. (1988). *The Crypto Anarchist Manifesto*. The Crypto Anarchist Manifesto. https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Nabi Khan, R. & Unesco. (1987). *La Troisième révolution industrielle : Tour d'horizon économique*. La Troisième révolution industrielle (Erès). https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000075479_fre&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_6ce01961-58e8-4217-b8f3-46d03515f0c1%3F_%3D075479freo.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000075479_fre/PDF/075479freo.pdf#%5B%7B%22num%22%3A68%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2Cnull%2Cnull%2C0%5D

Ronfaut, L. (11 mars 2019). *Quelle est la différence entre le Web et Internet?* LEFIGARO. https://www.lefigaro.fr/secteur/high-tech/2019/03/11/32001-20190311ARTFIG00004-quelle-est-la-difference-entre-le-web-et-internet.php

Blockchain : fonctionnement

✷ **Monographies :**

De Filippi, P. (2018). *Blockchain et cryptomonnaies*. Humensis.

Della Chiesa, M., Hiault, F., Téqui, C., Bouzou, N., & Gress, T. (2019). *Blockchain : Vers de nouvelles chaînes de valeur* (Nouvelle édition augmentée). Editions Eyrolles.

Dumas, J.-G., Lafourcade, P., Tichit, A., & Varrette, S. (2018). *Les blockchains en 50 questions : Comprendre le fonctionnement et les enjeux de cette technologie innovante*. Dunod.

Editions FuturTech. (2022). *La blockchain : Une technologie disruptive pour tous les domaines* (Vol. 4). FuturTech.

Loignon, S. (2017). *Big bang blockchain : La seconde révolution d'internet* (Vol. 1). Tallandier.

Mekki, M. (2020). Les mystères de la blockchain. In *La blockchain* (p. 9-24). Dalloz.

✷ Articles et ouvrages scientifiques :

Bhatia, S., Douglas, E. K., & Most, M. (2020). Blockchain and records management : Disruptive force or new approach? *Records Management Journal*, *30*(3), 277-286. https://doi.org/10.1108/RMJ-08-2019-0040

Bhatia, S., & Wright, A. (2019). Blockchain is already here. What does that mean for records management and archives ? *Journal of archival organization*, *16*(1), 75-84. https://doi.org/10.1080/15332748.2019.1655614

Faure-Muntian, V., De Ganay, C., & Le Gleut, R. (2018). *Les enjeux technologique des blockchains (chaines de blocs)* (N° 584). OPECST. https://www.senat.fr/rap/r17-584/r17-584.html

Fénéron Plisson, C. (2017). La blockchain, un bouleversement économique, juridique voire sociétal. *Information, données et documents (i2D)*, *54*(3), 20-22. https://doi.org/10.3917/i2d.173.0020

Findlay, C. (2017). Participatory cultures, trust technologies and decentralisation : Innovation opportunities for recordkeeping. Archives and Manuscripts, 45(3), 176-190. https://doi.org/10.1080/01576895.2017.1366864

Laurent, M. (2018). La blockchain est-elle une technologie de confiance ? Institut Mines-Télécom. https://hal.science/hal-01778949/document

Ndèla Marone, R. M., Mbengue, M., & Diakhaté, D. (2021). Archivage des données numériques massives : Contribution de l'intelligence artificielle et de la blockchain. *Djiboul*, *5*(2), 6-21. https://hal.archives-ouvertes.fr/hal-03540340/document

✷ Sources de sites internet :

Amazon AWS. (9 juin 2023). *Qu'est-ce que la technologie Blockchain ? : La technologie Blockchain expliquée*. AWS. https://aws.amazon.com/fr/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

Bellanca, C. (18 avril 2023). La blockchain : Une technologie, des centaines d'applications. *Coinhouse*. https://www.coinhouse.com/fr/academie/la-blockchain-une-technologie-des-centaines-dapplications/

Bercy infos. (12 avril 2022). *Qu'est-ce qu'une chaîne de blocs (blockchain) ?* Ministère de l'économie des finances et de la souveraineté industrielle et numérique. https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application

Berné, R. (2018, septembre 5). *Qu'est-ce qu'un Oracle ? Blockchain et monde réel*. Cryptoast. https://cryptoast.fr/oracle-blockchain/

Binance Academy. (1 février 2023). *Qu'est-ce que le trilemme de la blockchain ?* Binance Academy. https://academy.binance.com/fr/articles/what-is-the-blockchain-trilemma

Caine, P. (4 mars 2021). *Comment restaurer la confiance dans la technologie*. Linkedin. https://www.linkedin.com/pulse/comment-restaurer-la-confiance-dans-technologie-patrice-caine/?originalSubdomain=fr

Coin Academy. (s. d.). *Que sont les Arbres de Merkle ? (Merkle tree)*. Coin Academy. Consulté 28 juin 2023, à l'adresse https://coinacademy.fr/academie/arbres-merkle-tree-hash-fonction-hachage/

Confédération suisse. (2017). *La technologie blockchain permet de réduire les coûts et d'accroître la transparence*. Portail PME pour petites et moyennes entreprises. https://www.kmu.admin.ch/kmu/fr/home/aktuell/interviews/2017/die-blockchain-bringt-kostensenkungen-und-mehr-transparenz.html

Debelloir, M. (23 novembre 2022). *NFT : Nos explications pour tout comprendre en quelques minutes*. Cryptoast. https://cryptoast.fr/non-fungible-token-nft-ou-token-non-fongible/

Delahaye, J.-P. (24 octobre 2019). Comprendre la blockchain. *myLIFE*. https://my-life.lu/comprendre-la-blockchain-50022/

Goffinet, F. (1 janvier 2018). *Cryptographie asymétrique*. Linux Administration. https://linux.goffinet.org/administration/confidentialite/chiffrement-asymetrique

Gomez, W. (6 avril 2023). *Qu'est-ce qu'un arbre Merkle?* bit2me academy. https://academy.bit2me.com/fr/qu%27est-ce-qu%27un-arbre-merkle/

International Business Machines Corporation (IBM). (s. d.). *Qu'est-ce que la technologie Blockchain ?* Consulté 25 juin 2023, à l'adresse https://www.ibm.com/fr-fr/topics/blockchain

Karayan, R. (10 mai 2023). BNP Paribas s'associe à une nouvelle blockchain de consortium. Consulté 27 juin 2023, à l'adresse L'usine digitale website: https://www.usine-digitale.fr/article/bnp-paribas-s-associe-a-une-nouvelle-blockchain-de-consortium.N2130931

Ledieu, M.-A., & Gaïde, S. (19 septembre 2017). *Protocole blockchain : Aspects techniques pour non scientifiques*. Ledieu avocats. https://technique-et-droit-du-numerique.fr/protocole-blockchain-aspects-techniques/

✷ **Normes :**

Organisation internationale de normalisation (AFNOR). (2022). *NF en ISO 22739 : Chaîne de blocs et technologies de registres distribués : Vocabulaire*. AFNOR. https://viewerbdc.afnor.org/pdf/viewer/oQPEnXey7rI1?proxy=true

✷ **Vidéo :**

Meissonnier, A. (Réalisateur). (3 juin 2019). *Les nouveaux paradigmes de l'Archive : Permanence des missions et nouveaux paradigmes de la preuve*. https://yewtu.be/watch?v=0hOycRMRS7Y

La confiance : terminologie

✷ Cours et présentations :

Duplouy, L. (2023). *Signature électronique : Partie 1*. Cours de conservation et archivage, Villeurbanne.

✷ Monographies :

Algan, Y., & Cahuc, P. (2007). *La société de défiance : Comment le modèle social français s'autodétruit*. ENS rue d'Ulm.

Bachimont, B. (2017). *Patrimoine et numérique : technique et politique de la mémoire*. Médias et Humanités.

Hardin, R. (2006). *Trust*. Grande-Bretagne : Polity. ISBN 0745624650.

Karmis, D. & Rocher, F. (2018). *Trust, distrust, and mistrust in multinational democracies : comparative perspectives*. Canada : McGill-Queen's University Press.

Laurent, É. (2019). *L'économie de la confiance*. Paris : La Découverte.

Mucchielli, A. (1995), *Les sciences de l'information et de la communication*, Hachette.

Watzlawick, P., Helmick Beavin J. et Jackson D.D. (1972), *Une logique de la communication*, Le Seuil, Paris.

✷ Chapitre de monographies utilisés :

Granovetter, M. S. (1994). "Les institutions économiques comme constructions sociales : un cadre d'analyse", dans Orléan A. (Eds), *Analyse Economique des Conventions*, Paris : PUF, pp.79-94.

✷ Articles et ouvrages scientifiques :

Akrout, H. (2005). Nature et antécédents de la confiance interpersonnelle entre client-fournisseur en milieu industriel. *Management & Avenir*, 4, pp. 27-57. https://doi.org/10.3917/mav.004.0027

Cornu, L. (2003). La confiance. *Le Télémaque*, *n°24*(2), pp.21-30. https://doi.org/10.3917/tele.024.0021

Deutsch, M. (1958). *Trust and Suspicion*. *Journal of Conflict Resolution*, 2(4), pp.265-279. https://doi.org/10.1177/002200275800200401

Evans, A. M. & Krueger, J. I. (2009). The psychology (and economics) of trust. *Social and Personality Psychology Compass*, 3(6), pp. 1003–1017.

Frega, R. (2020). Les dimensions de la confiance. *Esprit*, pp. 47-55. https://doi.org/10.3917/espri.2010.0047

Liothin, A. & Riccio, P.-M. (2015). Vers la confiance numérique. *Management des technologies organisationnelles*, *4*(1), pp.197-203. https://www.cairn.info/revue-management-des-technologies-organisationnelles-2015-1-page-197.htm

Palus, J.-P., Revault d'Allonnes, A., & Jouandeau, N. (2022). La confiance comme posture de crédulité. *Rencontres Francophones sur la Logique Floue et ses Applications (LFA)*. https://doi.org/hal-03832463f

Quéré L. (2005). "Les 'dispositifs de confiance' dans l'espace public". *Réseaux*, 4(132), pp. 185-217. ISSN 1777-5809.

Rousseau, D. M.; Sitkin, S. B.; Burt, R. S. & Camerer, C. (1998). Not so different after all : A cross-discipline view of trust. *Academy of management review*, 23(3), pp.393-404.

Rutter, J. (2001). From the sociology of trust towards a sociology of 'e-trust'. *Int. journal of new product development & innovation management*, 2(4), pp.371–385.

Schilke, O., Reimann, M. & Cook, K. S. (2021). Trust in social relations. *Annual Review of Sociology*, *47*, pp.239–259.

Uslaner, E. M. (2009). "Where you stand depends upon where your grandparents sat : the inheritability of generalized trust". *Public Opinion Quarterly*, 2(4), pp. 725-740. 10.1093/poq/nfn058

✷ **Sources de sites internet :**

InterPARES 2. (s. d.). *Les concepts de fiabilité, d'exactitude et d'authenticité revus à cette aune*. Elec. Consulté 31 mai 2023, à l'adresse http://elec.enc.sorbonne.fr/interpares2/revision

✷ **Dictionnaires et encyclopédies :**

Académie française. (2019). *Dictionnaire de l'Académie française*. Dictionnaire de l'Académie française. http://www.dictionnaire-academie.fr/article/A9C3500

Le Robert. (2023). *Fiabilité : Définitions, synonymes, exemples*. Le Robert : dico en ligne. https://dictionnaire.lerobert.com/definition/fiabilite

Le Robert. (2022). *Foi : Définitions, synonymes, conjugaison, exemples*. Le Robert : dico en ligne. https://dictionnaire.lerobert.com/definition/foi

Blockchain et archives

✷ **Cours et présentations :**

Dubois, A. (2019). *Stratégie de préservation numérique* [Cours de numérisation des archives].

Guyon, C. (2023). *Le contrôle de la création des documents : Les caractères essentiels des records* [Cours de Records Management].

Leibenguth, C. (2019). *Cours n°2 : Analyse des besoins : Partie 1*.

Lemieux, V. & Association des archivistes du Québec. (4 juin 2020). *La vie d'un document à l'ère de la blockchain*. 49e Congrès de l'Association des archivistes du Québec, Québec, Canada. https://archivistes.qc.ca/wp-content/uploads/2020/06/AAQPresentation07042020-1.pdf

Makhlouf Shabou, B. (19 septembre 2019). *Cours 1 : Concepts de base* [Fiche descriptive : présentation Power Point]. Records Management 1, Genève.

✷ **Normes :**

Organisation internationale de normalisation (AFNOR). (2020). *NF Z42-013 : Archivage électronique : Recommandations et exigences*. AFNOR.

✷ **Articles et ouvrages scientifiques :**

Bhatia, S., & Wright, A. (2019). Blockchain is already here. What does that mean for records management and archives ? *Journal of archival organization*, *16*(1), 75-84. https://doi.org/10.1080/15332748.2019.1655614

Bhatia, S., Douglas, E. K., & Most, M. (2020). Blockchain and records management : Disruptive force or new approach? *Records Management Journal*, *30*(3), 277-286. https://doi.org/10.1108/RMJ-08-2019-0040

Collomosse, John, Tu Bui, Alan Brown, John Sheridan, Alex Green, Mark Bell, Jamie Fawcett, Jez Higgins, et Olivier Thereaux. (2018). "ARCHANGEL: Trusted archives of digital public documents". Dans Proceedings of the ACM Symposium on Document Engineering 2018., pp. 1-4.

Jost, C., Le Ven, E., & Texier, B. (2021). La blockchain, la machine à créer de la confiance tient-elle ses promesses ? In *Confiance numérique : Quelles technologies pour la garantir ?* https://www.calameo.com/read/0040596139364b0485a65?authid=E8hWD8Mm3rGt

Palop, K. (2017). La blockchain : Enfant promotteur du digital. *Blockchain : le nouveau cadre de confiance*, *Archimag guide pratique* (59), 4-15.

Sylvestre, G. (2020). *La social graph due diligence sur twitter, une méthodologie d'analyse stratégique qui combine algorithmes de sciences sociales, datavisualisation et expertise humaine*. *1*, 38-45. https://www.abd-bvd.be/wp-content/uploads/2020-1_Sylvestre.pdf

Poullet, Y. (2009). *Le droit économique à l'heure des TIC*. Pp.183-205. https://pure.unamur.be/ws/portalfiles/portal/54678199/6246.pdf

✷ **Sites internet :**

Collomosse, J., Bui, T., Brown, A., Sheridan, J., Green, A., Bell, M., Fawcett, J., Higgins, J., & Thereaux, O. (2018). *ARCHANGEL : Trusted Archives of Digital Public Documents* (arXiv:1804.08342). arXiv : http://arxiv.org/abs/1804.08342

eFutura. (s. d.). *Présentation et objectifs de l'associtation professionnelle eFutura*. eFutura : association professionnelle. Consulté 17 août 2023, à l'adresse https://www.efutura.fr/qui-sommes-nous/

Gallagher, R. (2001). *Parchive : Parity Archive Tool*. Parchive. https://parchive.sourceforge.net/

International Business Machines Corporation (IBM). (s. d.). *Qu'est-ce que la technologie Blockchain ?* Consulté 25 juin 2023, à l'adresse https://www.ibm.com/fr-fr/topics/blockchain

Jakobson, L. (24 avril 2019). MIT leads coalition putting academic credentials on blockchain. *Modern Consensus*. https://modernconsensus.com/uncategorized/mit-universities-academic-credentials-blockchain/

Paltz, E. (s. d.). *La Blockchain des archivistes*. Spark Archives. Consulté 17 juillet 2023, à l'adresse https://www.spark-archives.com/fr/blockchain-des-archivistes

Stern, J. & Agence nationale de la sécurité des systèmes d'information (ANSSI). (s. d.). *Cryptologie : Art ou science du secret ?* Chapitre 1. Consulté 17 août 2023, à l'adresse https://www.ssi.gouv.fr/particulier/bonnes-pratiques/crypto-le-webdoc/cryptologie-art-ou-science-du-secret/

✷ **Vidéos :**

Caprioli, E., & Agosti, P. (Réalisateurs). (23 mai 2023). *Journée confiance numérique 2023 : Guichet juridique*. https://www.youtube.com/watch?v=LPwYPD910Xk

Archives et confiance

✷ **Monographies :**

Couture, C., & Rouseau, J.-Y. (1987). *Vie du document : Une approche globale de la gestion des archives et des documents*. Vehicule press.

✷ **Normes :**

Organisation internationale de normalisation (AFNOR). (2016). *NF ISO 15489-1 : Information et documentation : gestion des documents d'activité : partie 1 : concepts et principes*. AFNOR. ISSN 0335-3931.

✷ **Articles et ouvrages scientifiques :**

Belin, A., & Rietsch, J.-M. (2016). Archivage électronique et analyse de risque : Les nouveaux défis de l'archiviste. *Archives*, *46*(1), 47-60. https://doi.org/10.7202/1035722ar

Girard, T. (2004). Les tiers de confiance sont-ils les archivistes de l'avenir? *Document numérique*, *8*(2), pp.117-125. https://doi.org/10.3166/dn.8.2.117-125

✷ **Sites internet :**

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). (s. d.). *L'édito du Directeur général*. ANSSI. Consulté 17 août 2023, à l'adresse https://www.ssi.gouv.fr/agence/missions/ledito-du-dg/

Blockchain Research Institute™. (2023). *Toward WEB3 : Digital assets, digital transformation*. BRI Membership. https://www.blockchainresearchinstitute.org/bri-membership/

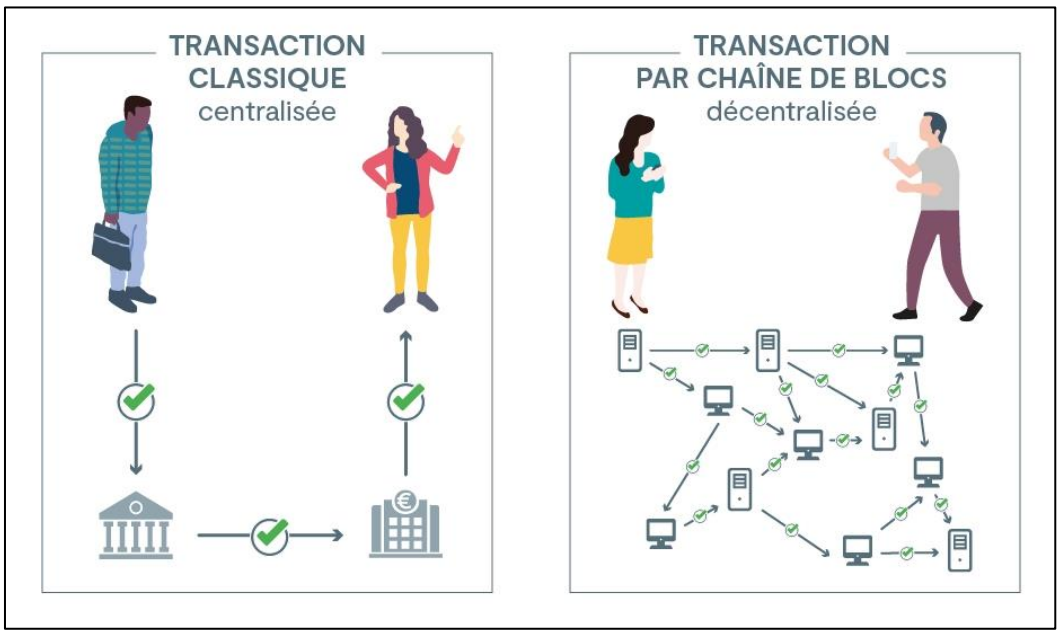
EDIFICAS & IALTA. (2000). *Guide de l'archivage électronique sécurisé : Recommandations pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations*. https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2000/2000_-_Guide_de_l_archivage_electronique_securise.pdf

Goldman Sachs. (s. d.). *Blockchain : The new technology of trust*. Goldman Sachs. Consulté 17 août 2023, à l'adresse https://www.goldmansachs.com/intelligence/pages/blockchain/

ANNEXES

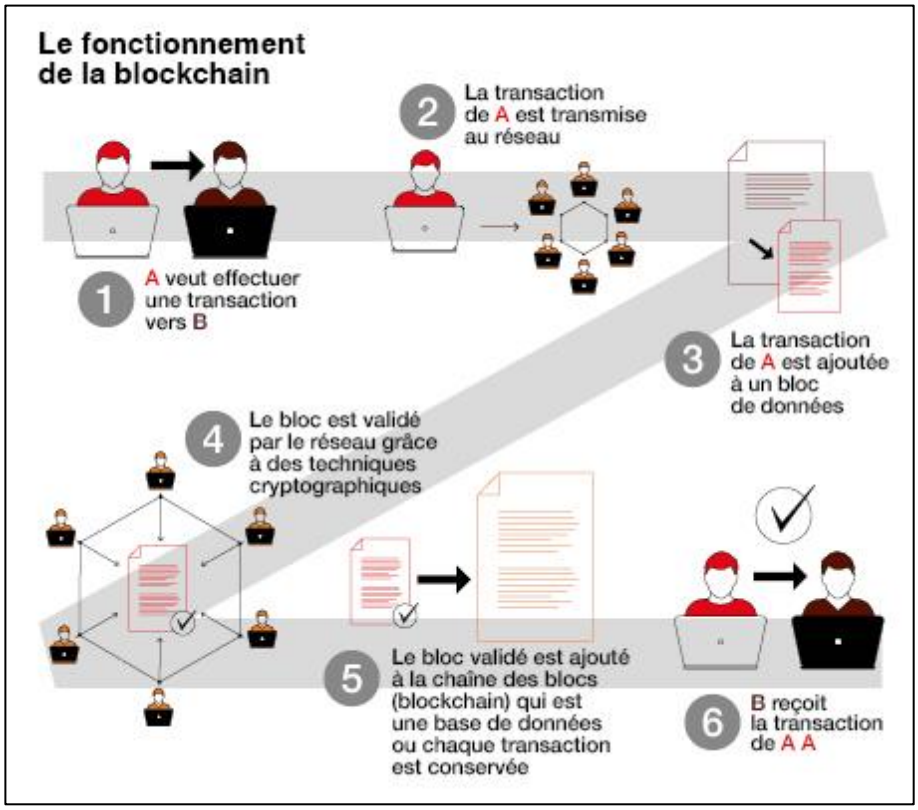
Table des annexes

ANNEXE 1 : SYSTEMES CENTRALISES ET DECENTRALISES



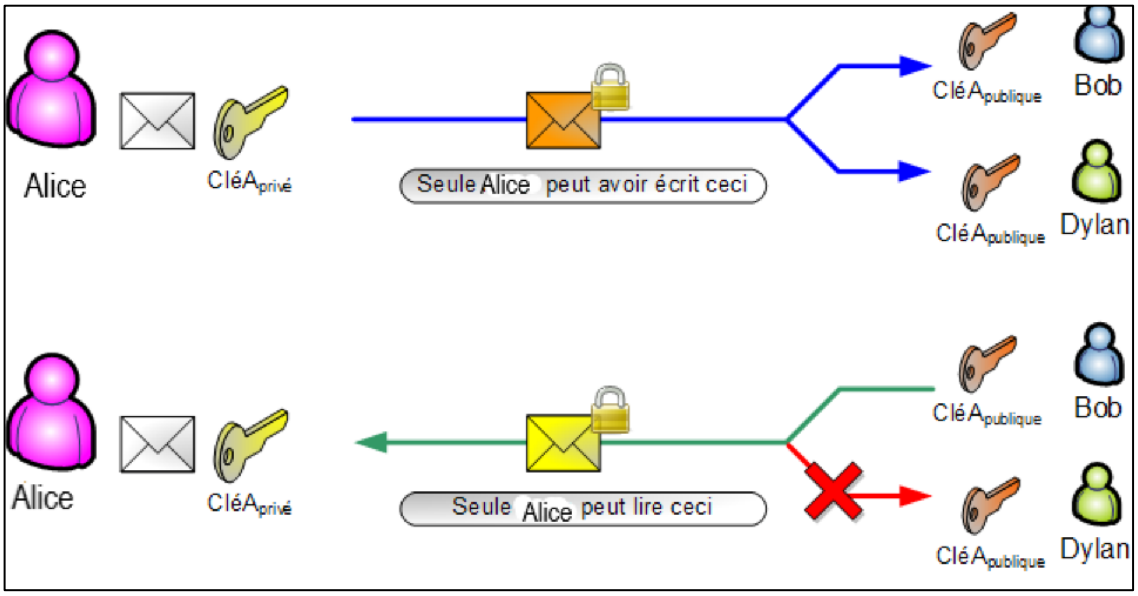
(Bercy Infos, 2022.)

ANNEXE 2 : LES BLOCKCHAINS PAS A PAS



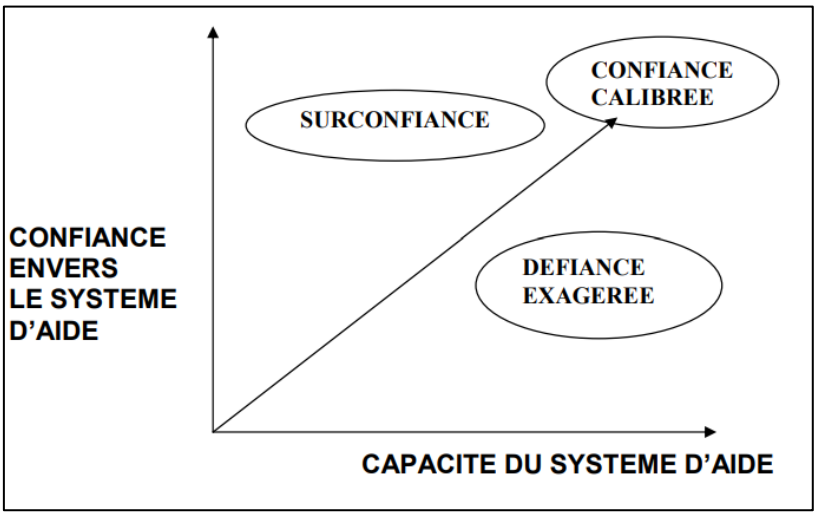
(Confédération Suisse, 2022)

ANNEXE 3 : CRYPTOGRAPHIE ASYMETRIQUE



(Goffinet, juin 2021)

ANNEXE 4 : GRAPHIQUE : CONFIANCE ET SUR-CONFIANCE



(Kassaagi et al., 2006)

ANNEXE 5 : EXEMPLE DE LA GRILLE D'ENTRETIEN POUR LES ARCHIVISTES

Utilisation de la blockchain avec les records/archives

Pensez-vous que la blockchain peut avoir une valeur ajoutée pour le domaine archivistique ? Dans sa conférence dit qu'il y en a pas donc pourquoi faire ? *"Quelle institution verrait de l'utilité la derrière ? Déjà convaincre une constitution d'adopter un SAE, GED qui soit conforme à une norme est difficile, alors là, c'est rajout de couche de preuve"*

On le sait aussi, il y a de gros problèmes d'obsolescence technologique, avec des répercussions sur les archives et leur dispositifs de lecture, etc. Dans la conférence, vous aviez dit que la blockchain ne rencontrait pas cette problématique, parce que (dans mes mots) bouge très peu au niveau de l'évolution. Est-ce qu'on peut revenir dessus, je n'ai pas très bien saisi les raisons qui font ça ?

Est-ce qu'il serait difficile d'améliorer le système s'il est, comme vous dites, non obsolète ?

Degré de confiance

Quelles sont vos préoccupations concernant l'utilisation de la blockchain pour les archives ?

Dans les cas d'usage, on en voit pas mal dans la littérature. Mais il y a d'une part un discours de "la blockchain va révolutionner le monde". Puis, sur le terrain, dans le concret, c'est rare. Je pense aux notaires (notamment et vous le dites), ils pourraient en faire usage avec les smart contracts. Vous le dites, le monde financier, les cryptomonnaies, ça a eu un tel succès. Mais à part ça, pour le reste il y a un refus catégorique. Pourquoi pensez-vous qu'il y a un tel refus ? Est-ce une peur ? Un manque de confiance ?

On nous présente des cas d'usage mais vous dites (et je vous suis) qu'il y a des impensés. Pourquoi c'est pas plus mis en avant ? On a un discours tellement révolutionnaire, mais les limites sont presque passées sous silence. Pourquoi on nous l'a vend comme ça? Des enjeux économiques ? Ces enjeux sont-ils une source de défiance ?

Le fait qu'on ait mis en avant que blockchain = révolution (et c'est pas vrai). Est-ce une raison pour en avoir une perte de confiance ?

Vous parlez d'expérimenter avec des projets plus "petits", avant de foncer direct dans la blockchain; via l'exemple de dématérialiser l'état civil des français venant de l'étranger. Pensez-vous qu'il faille procéder de la même manière avec l'archivage ?

Est-ce qu'on peut revenir au RGPD ? Vous avez dit que ça ne posait pas de problèmes. Dans la littérature scientifique, j'ai pu lire que "Complications avec le RGPD : impossible d'enlever ou corriger les données enregistrées dans la bl.". Est-ce qu'on pourrait revenir sur ce sujet ?

Vous citez de nombreux avantages, mais aussi de nombreuses limites, difficiles à surmonter. Est-il fondamentalement possible de faire confiance en la blockchain ??

Quels sont les critères permettant d'avoir confiance ?

Futur

Pensez-vous que les archivistes sont encore trop timides face à la technologie ? Pour quelles raisons ? Le domaine archivistique est-il prêt ?

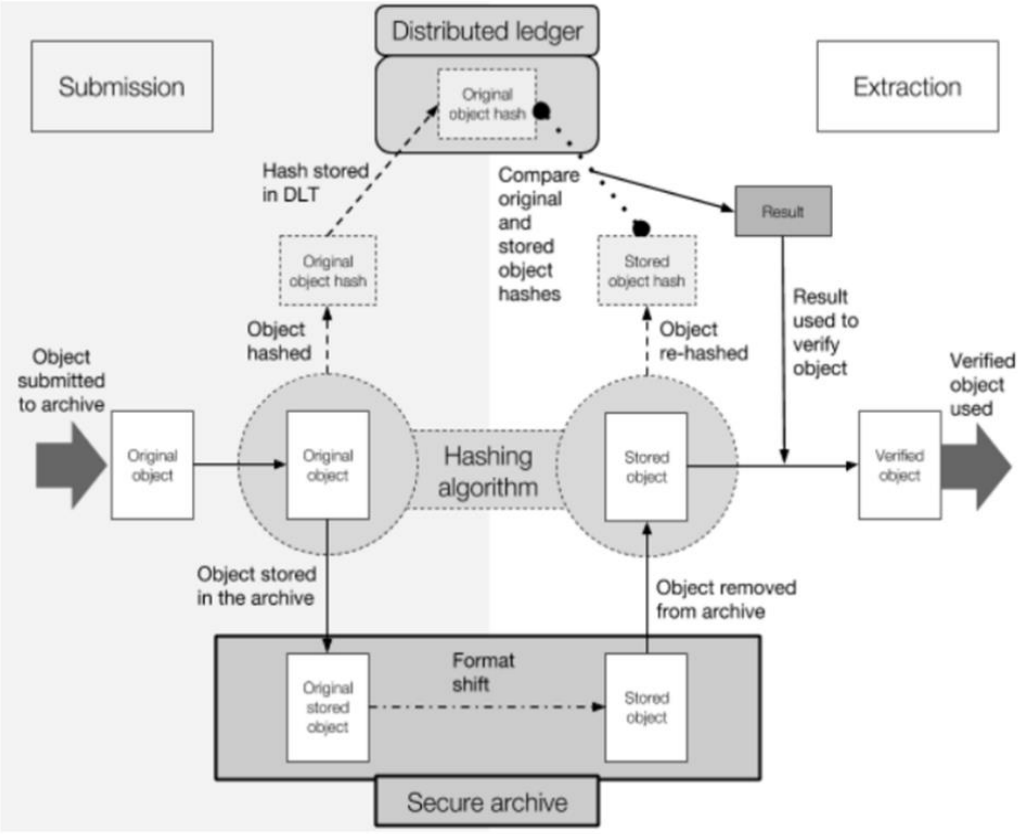
Quelles sont les améliorations ou les développements futurs que vous aimeriez voir pour renforcer votre confiance dans l'utilisation de la blockchain pour les archives ?

Pensez-vous qu'un jour nous pourrions tendre vers une utilisation dans les entreprises, les administrations pour les records, les archives ? Ou c'est utopique ?

Pensez-vous qu'il faille créer des formations, des cours pour former les archivistes ? Où en tout cas les sensibiliser au sujet ? Je pense aux écoles aussi, par exemple.

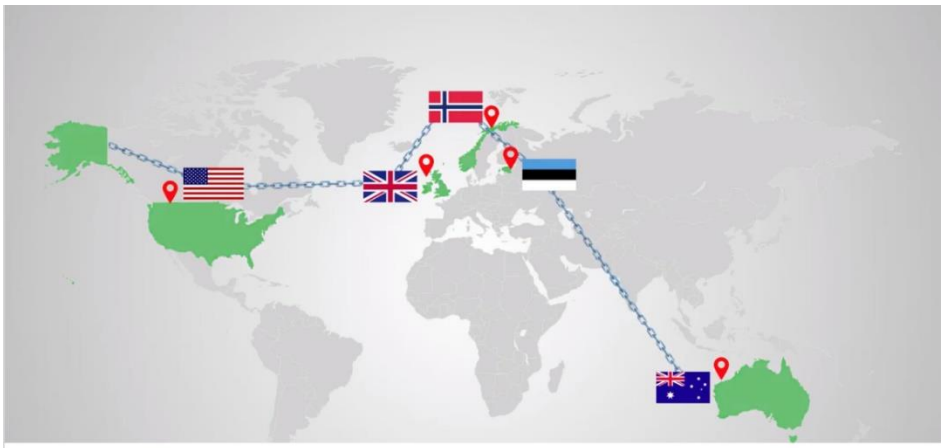
Vous pensez que l'adoption de la blockchain pour la gestion des archives est une question d'époque ? Qu'un jour nous pourrions parvenir à populariser son utilisation de manière courante ?

ANNEXE 6 : ARCHITECTURE DU PROJET ARCHANGEL



(Collomosse et al., 2018)

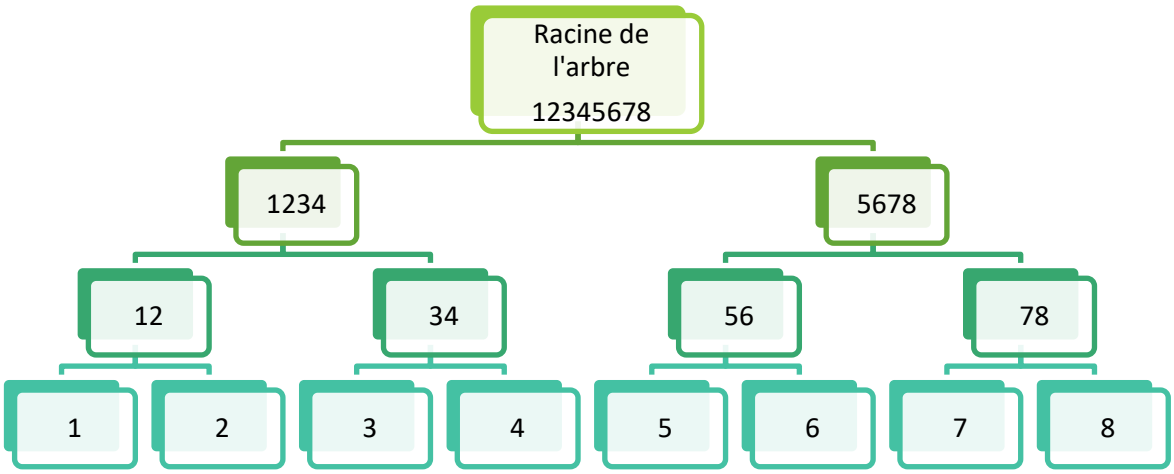
ANNEXE 7 : NŒUDS DU PROJET ARCHANGEL



Les archives à travers le monde peuvent aider à garantir l'intégrité des données d'archivage des autres sans avoir à partager des informations

(Lemieux & Association des archivistes du Québec, 2020)

ANNEXE 8 : ARCHITECTURE DE L'ARBRE DE MERKLE



(Brems, 2023)

GLOSSAIRE

Terminologies liées aux blockchains

Trois types de blockchains existantes :

Leur différence réside dans leur ouverture (Fénéron Plisson, 2017).

- **Blockchains publiques** : réseau large, grande échelle de participants (Bhatia et al., 2020). C'est un réseau ouvert à tous, sans restriction (Della Chiesa et al., 2019,p.103). Les données contenues dans la chaîne de blocs sont également ouvertes à tous. Elles sont souvent open-source ce qui signifie que le code de programmation de la blockchain est connu par le grand public. Bitcoin et Ethereum en font partie, c'est des blockchains qui sont surtout utilisées pour les cryptomonnaies. La blockchain peut donc être consultée et utilisée par tout le monde, sans restriction (Fénéron Plisson, 2017), il s'agit de la blockchain "pure" née d'une vision historique libertarienne. Il est aussi possible de retracer les mouvements financiers en utilisant les clés publiques (Loignon, 2017, pp. 72-73). Le milieu des affaires n'est donc pas avantagé par cette blockchain. C'est pourquoi les blockchains privées vont y remédier.
- **Blockchains privées :** utilisation pour le partage d'informations sensibles, puisque c'est un réseau fermé (Loignon, 2017, p.65). Les accès pour participation se limitent aux membres, il faut donc être autorisé par une autorisation venant des membres ou de l'administrateur désigné par les membres (par exemple un régulateur) (pp.72-73) ; tout le monde peut néanmoins consulter la chaîne (Fénéron Plisson, 2017). Elle se limite à un domaine d'activité très précis, ce qui présente un avantage considérable pour les entreprises, afin de certifier les documents, par exemple (Bhatia et al., 2020). Un autre intérêt de l'utilisation des blockchains privées étant la rapidité des transactions. Il y a une meilleure scalabilité (Bhatia et al., 2020), car il y a moins de nœuds sur le réseau, c'est-à-dire moins de trafic et donc un principe de consensus plus efficace pour ajouter des nœuds. Les données vont donc être échangées entre les entreprises, dans les réseaux (Loignon, 2017, p.73).
- **Blockchains de consortium** ou **hybrides** : utilisation dans le secteur bancaire, les start-ups, surtout, car il y a une application stricte de la réglementation (Fénéron Plisson, 2017). C'est un ensemble d'acteurs (souvent des institutions, des entreprises) qui vont contrôler la chaîne de blocs. Au sein duquel les accès sont limités à certains nœuds, le réseau peut donc être limité à un certain nombre d'utilisateurs (Della Chiesa et al., 2019, p.104). Pour entrer dans le réseau, il faut être validé par les membres du consensus, à savoir les nœuds, c'est un algorithme de consensus qui se base sur l'identité des nœuds (p.106), puisqu'au sein de ce réseau, les nœuds n'auront pas les mêmes droits d'accès (p.104).

Bloc : Suite de tokens écrite dans un bloc. Sorte de grappe de centaines, de milliers d'actifs numériques (Loignon, 2017, p.47).

Arbre de Merkle[27] : résultat de l'ensemble des fonctions de hachage (Laurent, 2018), c'est pourquoi il est aussi nommé "arbre de hash". Il solidifie la structure des blocs avec les transactions. Il s'agit d'un calcul de hash successifs pour lequel il est possible de remonter à la racine de l'arbre (Coin Academy, s. d.). Il facilite la

[27] Voir Annexe 8 : Architecture de l'arbre de Merkle, p. 90

vérification de quantités de données volumineuses. Chaque nœud va être relié à une racine unique au moyen du hash. Les feuilles (1, 2, 3, 4, etc.) vont être reliés à leur nœud enfant (12, 34, 56 et 78) qui lui-même sera relié à son nœud parent (1234 et 5678), et ainsi de suite jusqu'à parvenir à la racine de l'arbre. L'empreinte de cette racine va être reliée à tous les nœuds de l'arbre (Gomez, 2023). Les données peuvent donc être reliées en un seul point, ce qui permet de gagner en efficacité puisqu'il ne faut plus que vérifier la racine et non pas l'ensemble de la structure une à une. Si un hash est modifié, c'est l'ensemble des autres hash qui subiront le même sort. C'est est un pilier derrière la technologie blockchain. Si un nœud désire télécharger l'historique de la blockchain, il peut plutôt télécharger l'arbre de hash pour réduire la taille de téléchargement et être plus rapide lors de la vérification de l'authenticité des données. L'arbre de Merkle se présente comme une version plus amoindrie de l'ensemble de l'historique.

Bitcoin, aussi appelée "*mère de toutes les blockchains*" (Lewrick & Di Giorgio, 2019, p. 21) ou "*modèle d'origine des blockchains*" (Loignon, 2017, p.65), il s'agit de la première expérimentation de la blockchain sur une échelle aussi importante (Palop, 2017, p.5). Bitcoin est utilisé pour échanger et transférer des monnaies virtuelles appelées cryptomonnaies. La monnaie Bitcoin est nommée *coin*.

Ethereum est souvent mis en compétition face au Bitcoin. Le créateur, Vitalik Buterin désirait aller plus loin dans les usages que la simple transaction d'argent, (Leloup, 2017 p. 73), cur cette plateforme, les utilisateurs sont en mesure de développer des applications fonctionnant de façon sécurisées, décentralisées et transparentes (Della Chiesa et al., 2019, p.91-92). La blockchain devient programmable (Laurent, 2018). Toute une communauté de développeurs s'est ainsi mise en place pour gouverner de manière collaborative le protocole Ethereum (Leloup, 2017 p. 73). Elle intéresse surtout le monde des affaires au moyen de sa plateforme de smart-contracts (Leloup, 2017, p.76), ce qui permet de créer des marchés, de déplacer des fonds. La blockchain, elle ne se limite plus qu'au stockage, il y a une exécution automatique (p.80). Il y a un ensemble d'applications décentralisées permettant de créer ses propres mesures comme les formats des transactions (Della Chiesa et al., 2019, p.102). Ces applications sont aussi connues sous le nom de DAO. N'importe quel développeur peut désormais créer des applications décentralisées, aussi aisément qu'une application mobile (Loignon, 2017, p.71).

Réseau en peer-to-peer (pair à pair ou P2P) : Technologie dont l'architecture est distribuée, l'ensemble forme un réseau de nœuds – nodes – en pair à pair (Findlay, 2017). Les participants du réseau se partagent les tâches. Les participants – appelés pairs ou nœuds– sont donc égaux car ils alimentent tous le réseau. Il n'y a pas d'institution ou d'individu se situant au milieu agissant en tant qu'intermédiaire ou organisme de contrôle. Toute la confiance va venir reposer sur la réputation du système. L'innovation derrière les blockchains repose sur ce système décentralisé.

Système décentralisé ou distribué : les données sont hébergées chez chaque participant du réseau, elles sont distribuées (Loignon, 2017, pp.47-48). Ces participants ont la responsabilité de valider et sécuriser les données inscrites dans les blocs (Editions FuturTech, 2022, p.5). A l'opposé, nous retrouvons les systèmes dit centralisés, qui sont plus "traditionnels". Les données sont stockées sur un serveur central, celui de l'intermédiaire central (Loignon, 2017, pp.47-48).

Protocole informatique : chaque blockchain va avoir un domaine d'application, c'est ainsi que les blockchains se distinguent et se différencient (Amazon AWS, 2023). Ceci est possible au moyen d'un protocole informatique, puisque chaque plateforme blockchain va avoir le sien qui lui est propre (Bellanca, 2023). Le protocole va se réguler de lui-même. Il s'agit d'une "couche" que Bitcoin utilise, par exemple, le protocole Simple Mail Transfer Protocol (SMTP) qui permet de réaliser une tâche précise (le transfert d'argent).

Fonction de hachage ou hash: Chaîne de caractères utilisée pour calculer l'empreinte numérique d'un fichier (Duplouy, 2023). Cette opération permet de l'identifier de façon unique et de contrôler sont intégrité, il peut être rapproché à un identifiant unique ou un algorithme, c'est la carte d'identité d'un document. Elle va permettre d'attester qu'une modification a été opérée (Fénéron Plisson, 2017). Si nous modifions ne serait-ce qu'un octet du fichier, le hash ne correspondra plus à celui du départ, le résultat sera différent. Le hash permet de gagner du temps pour ne pas avoir à comparer les contenus de deux fichiers entre eux. Si les deux hash sont les mêmes : les documents sont égaux. Si les hashs sont différents, l'un des fichiers a été modifié. Les formats de hash possibles sont le plus souvent du MD5 ou SHA-256. Dans les blockchains, le format SHA est privilégié il a une taille d'empreinte de 256 bits (32 caractères), une plus grande majorité d'ordinateurs est en mesure de lire cet algorithme. Ethereum utilise le format SHA3-256, tandis que Bitcoin utilise un format plus ancien, SHA-256.

Cryptographie asymétrique : Tout comme le hash, la cryptographie asymétrique est un algorithme. Elle permet de sécuriser les échanges d'informations en attestant l'origine des données (Faure-Muntian et al., 2018). Chaque utilisateur va détenir en sa possession : une clé publique et une clé privée, formant une paire de clés. Ces paires de clés vont être utilisées pour chiffrer ou signer électroniquement un message, la signature électronique est le chiffrement d'une empreinte. Ce message, c'est une suite de chiffres qu'il est impossible à lire sans la paire de clés.

Smart-contract : ou contrat intelligent est une série de programmes (Marin-Dagannaud, 2017). Les nœuds du réseau vont exécuter les conditions du contrat. Une fois les exigences du contrat atteintes, il va être automatiquement exécuté, pour ensuite être sauvegardés et diffusé sur l'ensemble de la blockchain (Bhatia et al., 2020). Par exemple, une fois les termes du contrat remplis (prêt financier, contrat de mariage, etc.) (Leloup, 2017, p.79), le transfert d'argent va être automatiquement exécuté. C'est un tournant pour la logique contractuelle. Une fois le contrat partagé sur le réseau, il sera impossible d'en annuler l'exécution (Marin-Dagannaud, 2017). Le seul moyen pour y arriver étant si l'ensemble du réseau consent à revenir sur l'exécution du contrat. Il faudrait considérer que tous les acteurs sont alors malveillants, ce qui est particulièrement rare. Ce type de contrat est donc entièrement numérique et automatisé (Leloup, 2017, p.79).

DAO ou Decentralized Autonomous Organization ou Organisation autonome décentralisée : il peut s'agir d'une application avec une autre, ou encore de la gouvernance d'une entreprise (Della Chiesa et al., 2019, p.102). C'est un mode d'organisation parmi lequel une organisation (ou une application) ne sera pas dépendante d'une autre. Dans le cas d'une entreprise, les dirigeants ne sont pas nommés, ils détiennent des droits de vote (Chatue-Diop, 2023, p.151) et détiennent les tokens dit natifs (Cryptoast, 2021). Les autres membres peuvent être anonymes, suggérer des propositions d'idées, ou interagir avec les détenteurs des tokens (Chatue-Diop, 2023, p.151). Les tâches seront distribuées : tout le monde peut

participer à la prise de décision. La confiance est placée au sein du réseau même. Les DAO ont un lien direct avec les Smart Contracts (Della Chiesa et al., 2019, p.102). Les règles de la gouvernance seront inscrites dans le contrat. L'application des décisions prises par les membres est automatisée dans les termes du contrat intelligent. Les choix des votes sont dans le contrat, ce qui permet de connaitre les résultats de votes, de façon sécurisée et automatisée.

Token : c'est un jeton numérique. Ce token possède une valeur digitale associé au protocole utilisé au sein de la blockchain (Lewrick & Di Giorgio, 2019, p. IX). Il est plus connu sous la dénomination de cryptomonnaies, crypto-actif ou actif numérique (Della Chiesa et al., 2019, pp.109-110). Le token va circuler dans l'architecture de la blockchain, c'est le résultat d'une donnée qui a été stockée dans un registre.

NFT ou non-fungible token : objet informatique qui est rattaché à un identifiant numérique, le rendant unique et non fongible; c'est-à-dire que le jeton ne peut être remplacé par un autre élément (au contraire de l'argent qui lui peut être échangé) (Debelloir, 2022). Les NFT ont souvent été associés aux fichiers JPG, mais ils peuvent représenter toutes sortes de documents les rendant donc intéressants dans le domaine archivistique. Un morceau de terrain virtuel pourrait donc être vendu sous forme de NFT. LE NFT va être numérisé et inscrit dans la BC, un jeton va pouvoir garder une grande quantité d'informations. Une fois le jeton inscrit dans une chaîne de blocs, le jeton sera accompagné d'un certificat d'authenticité numérique garantissant que la personne qui le détient soit bien le seul et unique propriétaire du jeton non-fugible.

Oracle : intègre des données provenant du monde réel dans des contrats intelligents : température, résultats sportifs, retards aériens, etc; puisque les BCs ne peuvent accéder aux données qui sont extérieures à son réseau (Berné, 2018). En fonction des informations contenues, cela déclenchera ou non le smart contract.

Caractéristiques des blockchains :

Immuabilité : l'information inscrite dans les blocs validés n'est plus modifiable (Lewrick & Di Giorgio, 2019, p.50).

Non-répudiation : cette traçabilité (Ndèla Marone et al., 2021). Il y a une certification de non-modification, la blockchain agit telle une sorte de préservation contre la révision de l'information.

Permanence : accès à l'ensemble de l'historique qui est inscrit dans la blockchain, il s'agit d'un registre permanent (Loignon, 2017, p.31). Les preuves de cet envoi sont permanentes, permet en parallèle de s'assurer que l'objet a bien été envoyé, il est impossible de le nier grâce à l'historique. D'où le surnom donné à la blockchain de "ledger technology" ou la technologie du grand livre (Bhatia & Wright, 2019). Ceci fait référence au grand livre utilisé par les comptables, car il conserve les preuves des transactions qui ont été effectuées, car elles sont inscrites dans chaque bloc.

Principe de consensus : fait référence au principe de majorité sur le réseau, à tout moment les membres de ce réseau se mettent d'accord sur l'état de la blockchain (De Filippi, 2018, p.27). De ce fait, les utilisateurs malveillants vont être exclus par les parties prenantes du réseau (Lewrick & Di Giorgio, 2019, p.19). Les deux plus grands protocoles de consensus sont :

- **Preuve de travail** (Proof Of Work ou PoW) ou protocole de consensus. Il s'agit d'une puissance de calcul. Son intérêt étant qu'elle va venir empêcher toute attaque pouvant intervenir sur le réseau (Dumas et al., 2018). Un contenu frauduleux sera non-rentable grâce au PoW (Lewrick & Di Giorgio, 2019, p.VIII). Pour cela, les mineurs vont devoir résoudre une équation mathématique.
- **Preuve de participation** (Proof of Stake ou PoS) : inventée pour être moins énergivore que le PoW (Loignon, 2017). Il n y a pas de résolution par calcul. Les blocs ne seront pas minés, mais forgés. Les personnes qui tentent de tricher en autorisant un nœud malveillant seront puni. Avant de valider un bloc, les forgeurs vont miser de l'argent sur le bloc. S'ils perdent, alors cette somme leur sera retirée. Ils sont donc plutôt des validateurs de confiance. Mais la faiblesse étant qu'il faut s'assurer qu'ils soient bien fiables. Autrement, s'il y a une majorité de nœuds malveillant, il y a un risque de valider un bloc douteux. La sécurité peut donc être mise à mal plus facilement que le PoW.

Traçabilité et **transparence** : les actions sont vérifiables par tous les membres du réseau (Loignon, 2017, p.50). De plus, l'historique des transactions ou autres actions effectuées sont vérifiables (p.30). Les serveurs conserveront une copie de l'historique complet des messages ou des transactions effectuées depuis le premier bloc de la chaine (Ledieu & Gaïde, 2017).

Terminologies liées aux archives

Record ou document d'activité : information créée ou reçue et que nous allons préserver pour ses qualités de preuves par une personne physique ou morale, afin de conduire son activité. Cette information sera conservée pour respecter les obligations légales en vigueur ou toute transaction liée directement à l'activité de cette personne (Organisation internationale de normalisation (AFNOR), 2016). L'institution dispose ainsi des documents dont elle a besoin, à tout instant. L'information est perçue comme une ressource stratégique, le cycle de vie sera donc plus limité que le cas des archives.

Archives : à contrario du *records*, l'archive est ici perçue comme étant l'identification de documents d'activité qui auront une valeur durable. La conservation des documents se fait en gardant une perspective de long terme, afin de garantir l'authenticité, fiabilité et intégrité des données contenues (Guyon, 2023).

Preuve : information provenant d'une opération effectuée (AFNOR), 2016).

Système documentaire : système d'information qui va enregistrer, organiser, gérer et octroyer les droits d'accès aux documents d'activité dans le temps ((AFNOR), 2016).

Intégrité : document complet, il n'a pas été altéré ou modifié (pas d'ajout ou retrai t d'informations), cela renvoie à l'intégrité physique du document (Guyon, 2023). Le document est le même qu'à l'origine.

Fiabilité : contenu du document pour lequel les informations contenues sont complètes et exactes (Guyon, 2023).

Authenticité : le document est bien ce qu'il prétend être. L'auteur est bien celui énoncé et identifiable. Et le contenu produit par cet auteur est bien créé et validé à la date affichée dans le document (Guyon, 2023).

SAE : SI servant à préserver la sécurité, intégrité, disponibilité et confidentialité des archives pour les conserver sur le long terme (Organisation internationale de normalisation (AFNOR), 2020).

Journal : ensemble de documents reprenant les évènements du SAE qui ont été journalisés. Ils font partie des éléments de preuve (Organisation internationale de normalisation (AFNOR), 2020).

TABLE DES ILLUSTRATIONS

TABLE DES MATIERES