Couvrez cette blockchain que je ne saurais accepter : le paradoxe de la transparence des technologies blockchain dans une situation extrême de gestion

Cédric Baudet, Maximiliano Jeanneret Medina

Couvrez cette *blockchain* que je ne saurais accepter : le paradoxe de la transparence des technologies *blockchain* dans une situation extrême de gestion

Cédric Baudet*
Maximiliano Jeanneret Medina ****

* HEG Arc, HES-SO // University of Applied Sciences Western Switzerland, Neuchâtel, Switzerland

** Human-IST Institute, University of Fribourg, Fribourg, Switzerland

Résumé :

La République et Canton du Jura (Suisse) a décidé d'intégrer le sceau numérique CERTUS et la *blockchain* KSI comme briques technologiques centrales de leur Guichet virtuel et plus largement de leur système d'information cyberadministratif. Or, ce projet s'opère dans une situation de gestion que l'on peut qualifier d'extrême. Alors que les technologies *blockchain* souffrent parfois d'une mauvaise réputation, que les administrations suisses subissent des cyberattaques et qu'un projet qui s'appuie sur la *blockchain* estonienne KSI a été rejeté par la Confédération, comment faire accepter ces technologies aux administrés de la République et Canton du Jura ? Au travers d'une recherche-action et afin de résoudre des problèmes pratiques, nous exposons quatre recommandations managériales, dont une qui propose de communiquer en deux niveaux d'abstraction afin de limiter les tensions dans une situation extrême de gestion. Le premier niveau doit exposer les cas métiers et l'importance pour un citoyen de rester de rester souverain de ses données. Un deuxième niveau, destiné aux spécialistes des technologies, peut exposer le fonctionnement des briques technologiques CERTUS et de la *blockchain* KSI. Enfin, dans une visée de création de connaissance scientifique, nous discutons d'un certain paradoxe de la transparence des technologies *blockchain* dans une situation extrême de gestion.

Mots clés :

acceptation ; transparence ; *blockchain* ; cyberadministration ; recherche-action

1. Introduction

Les gouvernements, les organisations ou encore les individus s'appuient sur les systèmes d'information (SI) afin de résister aux effets négatifs produits par la crise de la Covid-19. Dans ce désastre pandémique, les gouvernements voient les applications de *pass*, fussent-ils sanitaires ou vaccinaux, comme l'un des moyens les plus efficaces de lutte contre la propagation des différents variants. Dans une situation marquée par les multiples tensions, les gouvernements ont dû sélectionner rapidement une solution technologique fiable et sécurisée pour stocker les certificats Covid sous forme numérique.

Après avoir reçu une cinquantaine de propositions d'application de *pass* sanitaire, la Confédération helvétique a sélectionné puis examiné deux solutions techniques permettant aux personnes vaccinées, guéries ou ayant reçu le résultat d'un test négatif de présenter un certificat Covid[1]. La première solution technique est proposée par l'Office fédéral de l'informatique et de la télécommunication (OFIT). Ce service de la confédération met en évidence la compatibilité de leur système avec celui de l'Union européenne, la sécurité ou encore le code *open source*. La deuxième solution technique s'appuie sur un sceau numérique stocké dans la *blockchain* KSI. Proposée par les entreprises lausannoises ELCA et Sicpa, cette solution met en lumière la simplicité d'utilisation tout en respectant la sphère privée des utilisateurs. Alors que cette deuxième solution était considérée comme la favorite par certains experts[2], la confédération a choisi en mai 2021 la solution de *pass* développée par l'OFIT[3].

Toutefois, le perdant n'a certainement pas tout perdu. En effet, la République et Canton du Jura a décidé d'intégrer le sceau numérique CERTUS et la *blockchain* KSI comme briques technologiques centrales de leur Guichet virtuel et plus largement de leur système d'information cyberadministratif. Selon les porteurs du projet, ces technologies ont pour objectif de renforcer la confiance numérique entre les administrés et l'État au travers de la sécurisation des documents administratifs[4]. Or, la littérature scientifique considère que la stabilité politique d'un pays comme la Suisse peut être un frein à l'adoption des technologies *blockchain* (Reddick et al., 2019). Dans un contexte de stabilité politique, mais de situations de gestion tendues (Lebraty, 2013), il nous apparaît intéressant d'analyser en profondeur ce cas et de s'interroger plus particulièrement sur l'acceptation de telles technologies. En effet, alors que les technologies qui s'appuient sur la *blockchain* souffrent parfois d'une mauvaise réputation pour des raisons écologiques, que la solution de Scipa a été rejetée par la Confédération suisse et que les administrations suisses font actuellement face à une vague de cyberattaques sans précédent[5][6], comment faire accepter ces technologies aux administrés de la République et Canton du Jura dans une situation extrême de gestion ?

---

[1] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-83216.html
[2] https://www.ictjournal.ch/news/2021-04-23/qui-pour-fournir-le-certificat-covid-en-suisse
[3] https://www.rts.ch/info/suisse/12181531-le-certificat-covid-sera-realise-par-ladministration-federale-dici-fin-juin.html
[4] https://www.jura.ch/CHA/SIC/Centre-medias/Communiques-2021/La-confiance-numerique-comme-pilier-des-prestations-en-ligne.html
[5] https://www.rts.ch/info/regions/vaud/12442317-la-gravite-de-la-cyberattaque-de-la-commune-de-rolle-sousestimee-par-les-autorites.html
[6] https://www.rts.ch/info/regions/vaud/12555731-la-commune-de-montreux-a-son-tour-victime-dune-cyberattaque.html

Afin de répondre à cette question de recherche, nous avons mené une recherche-action d'avril à novembre 2021. Cette question de recherche nous apparaît pertinente tant pour les praticiens que pour les chercheurs, car elle adresse une question d'actualité ainsi que des problèmes organisationnels (Benbasat et Zmud, 1999) tout en veillant à alimenter la base de connaissance scientifique sur l'adoption des technologies *blockchain*.

Notre proposition de communication se structure en 4 sections. Après avoir introduit notre sujet, nous présentons une brève revue de littérature sur les technologies *blockchain* dans un contexte de cyberadministration. Dans une deuxième section, nous présentons le contexte de notre recherche. La méthodologie de cette recherche-action est décrite dans une troisième section. Enfin, dans une quatrième section nous exposons notre diagnostic puis mettons en lumière un certain paradoxe dans la volonté de transparence de l'État.

2. La *Blockchain* dans la cyberadministration : enjeux, adoption et implémentations

Depuis son introduction en 2008 au travers de la cryptomonnaie *Bitcoin* (Nakamoto, 2008), la *blockchain* s'est positionnée comme l'une des technologies incontournables de l'économie numérique (Brynjolfsson et al., 2021). Une *blockchain* est un système qui s'appuie sur un réseau *peer-to-peer* et qui permet de valider et de stocker de manière permanente des transactions horodatées sur un grand livre partagé et distribué sur tous les nœuds du réseau (Lacity, 2018). Il existe différents types de *blockchain* et il est nécessaire de distinguer la *blockchain* elle-même, des technologies qui s'appuient sur cette dernière telle que les *Smart Contracts*, les *DAO* ou encore les *NFT* (Jeanneret Medina et al., 2020). Dans le contexte des SI de cyberadministration, la capacité de la *blockchain* à enregistrer les transactions distribuées permet d'améliorer la transparence, de prévenir la fraude et d'augmenter la confiance envers le secteur public (Batubara et al., 2018). Au-delà de ces deux avantages, il nous semble intéressant d'exposer plus en détail les enjeux, les barrières à l'adoption ainsi que des exemples d'implémentations des technologies *blockchain* dans le domaine cyberadministratif.

Nous soulignons les enjeux pour les deux principales parties prenantes du domaine de la cyberadministration : les gouvernements et les citoyens. Pour les gouvernements, les principaux gains de la mise en œuvre des technologies *blockchain* consistent en une amélioration de l'efficacité, notamment par la réduction de la bureaucratie ou encore par l'amélioration de la coordination entre fonctionnaires (Cagigas et al., 2021). De plus, par la suppression d'intermédiaires, la *blockchain* permet de réduire les coûts (Alexopoulos et al., 2019). D'un autre côté, la mise en œuvre de technologies *blockchain* dans un contexte cyberadministratif dévoile une face plus sombre. Cette technologie révèle des risques sur lesquels il est nécessaire de se pencher. Le manque de normes, les incertitudes réglementaires ainsi que les questions relatives à l'évolutivité de ces technologies sont considérés comme des risques majeurs pour les gouvernements (Rana et al., 2021 ; Cagigas et al., 2021). Pour les citoyens, la sécurité et la transparence sont identifiées comme les principaux avantages offerts par les technologies *blockchain* (ibid., 2021). Les avantages relatifs à la sécurité découlent principalement de l'immuabilité des données inscrites dans la *blockchain*. Quant à la transparence de la *blockchain*, elle permet aux citoyens d'exercer un plus grand contrôle sur leurs données personnelles. Dans son essence, la *blockchain* est conçue pour donner au propriétaire des données un identifiant unique pour y accéder ainsi que la possibilité de partager uniquement les données qu'il désire (ibid., 2021). Ainsi, la question de la protection des données semble la préoccupation centrale des citoyens (Rana et al., 2021 ; Cagigas et al., 2021).

Selon l'article le plus cité en SI, « les gains en performance sont souvent freinés par la réticence des utilisateurs à accepter et à utiliser les systèmes d'information disponibles » (Davis, 1989 : 319). À nos yeux, les technologies *blockchain* ne font pas exception. D'ailleurs, Cagigas et al. (2021) relèvent le risque de la non-acceptation des technologies *blockchain* par les fonctionnaires, soit par manque de connaissances, soit par manque de compétences en la matière. Selon Batubara et al. (2018), les barrières à l'adoption peuvent être de trois ordres. Du point de vue environnemental, le manque de lois et des réglementations peuvent limiter l'adoption. Du point de vue organisationnel, la résistance aux changements ou encore le besoin de nouveaux modèles de gouvernance sont présentés comme les principaux obstacles à l'adoption. Enfin et d'un point de vue plus technologique, les barrières à l'adoption sont nombreuses telles que le manque de sécurité, de fiabilité, d'évolutivité ou encore de convivialité. Reddick et al. (2019) utilisent la théorie de la diffusion de l'innovation pour examiner les adoptions de technologies *blockchain* par des gouvernements. Six facteurs d'adoption de la *blockchain* ont été testés à l'aide d'une régression logistique : cybersécurité, contrôle de la corruption, développement du gouvernement électronique, efficacité du gouvernement, stabilité politique et participation démocratique. Leur analyse tend à démontrer que la cybersécurité, l'efficacité du gouvernement et la stabilité politique sont des prédicteurs significatifs. Des niveaux élevés de cybersécurité et d'efficacité gouvernementale augmentent la probabilité que les pays adoptent la *blockchain*. Enfin, nous relevons qu'un degré plus élevé de stabilité politique diminue la probabilité d'une adoption précoce de la *blockchain*.

Malgré les côtés positifs et négatifs des technologies *blockchain* ainsi que les barrières à leur adoption, l'intérêt des gouvernements est grandissant et le nombre de projets cyberadministratifs qui s'appuie sur ces technologies est en forte augmentation (Alexopoulos et al., 2019; Allessie et al., 2019). Alexopoulos et al. (2019) explorent quelques implémentations des technologies *blockchain* en Europe et mettent la lumière sur leur adoption par le gouvernement estonien. L'Estonie est considérée par les experts comme le pays le plus avancé dans l'exploitation de ces technologies (Alexopoulos et al., 2019). L'approche cyberadministrative estonienne s'articule autour d'un écosystème riche en services comprenant environ 3'000 prestations, dont la gestion de l'identité numérique, le vote *online*, la gestion électronique des données des patients, la perception des impôts, etc. Trois briques technologiques constituent le socle du système d'information cyberadministratif estonien : l'e-ID, X-Road et la *blockchain* KSI[7]. L'e-ID est la clé de l'identité numérique de chaque citoyen. La plateforme X-Road assure la gestion décentralisée des données. Enfin, la *blockchain* KSI est en charge de l'intégrité des données cyberadministratives. Si la *blockchain* fait l'objet de beaucoup d'intérêt dans la communauté scientifique[8], ce n'est pas le cas de la *blockchain* KSI[9]. Développée en 2007 afin de répondre à une vague de cyberattaques, la *blockchain* KSI se démarque par une faible consommation énergétique, une bonne capacité de mise à l'échelle et une rapidité dans l'obtention du consensus[10].

Au travers de cette brève revue de littérature, nous constatons que les recherches sur les technologies *blockchain* dans un contexte de cyberadministration sont généralement conduites

[7] https://e-estonia.com/solutions/cyber-security/ksi-blockchain/
[8] Une requête lancée sur la base de données scientifique *Web of Science* début 2022 renvoie plus de 41'000 résultats.
[9] Une requête lancée sur la base de données scientifique *Web of Science* début 2022 ne renvoie que 5 résultats, dont aucun dans le domaine du management.
[10] https://m.guardtime.com/files/KSI_data_sheet_201509.pdf

ex post. De plus, leurs résultats nous semblent plus descriptifs que prescriptifs. Ainsi, dans le cadre d'une recherche-action, il est légitime de s'interroger sur comment faire accepter les technologies *blockchain* aux administrés de la République et Canton du Jura dans une situation extrême de gestion ?

3. Contexte de la recherche

3.1 Un projet de cyberadministration pour améliorer la confiance numérique

La République et Canton du Jura est l'un des 26 cantons suisses. Nous rappelons qu'en Suisse, les cantons jouissent de souveraineté. Cette autonomie engendre que chaque canton doive prendre ses propres décisions par exemple en matière de fiscalité, de système éducatif ou encore de processus administratifs[11]. La République et Canton du Jura a défini puis mis en œuvre une stratégie numérique afin de transformer en profondeur les processus de l'État[12]. Pour cela, de nombreux projets technologiques, considérés comme innovants[13], visent à numériser l'administration jurassienne tout en oeuvrant à réduire la fracture numérique[14] et à augmenter la confiance numérique[1516]. La plupart de ces projets technologiques sont implémentés au travers du Guichet virtuel, véritable extension numérique des services physiques proposés par l'État[17].

L'un des projets actuels du canton du Jura consiste à implémenter la technologie de sceau numérique CERTUS et la *blockchain* KSI pour en faire les briques technologiques centrales de leur Guichet virtuel et plus largement de leur système d'information. Ces briques technologiques visent principalement à améliorer la confiance des citoyens envers les services numériques proposés par l'État. Dans le livre blanc du projet, le canton indique que « chaque citoyen jurassien dispose d'un environnement client où il peut échanger les documents qui le concerne avec l'administration. Ainsi, le citoyen peut déposer des documents à l'attention de l'administration et de la même manière, l'administration va mettre à disposition du citoyen des documents ou des certificats. Actuellement, ce système est basé (*sic*) sur la confiance que le citoyen a dans la sécurité et l'intégrité des systèmes informatiques de l'État. Si toutefois un citoyen devait avoir un litige avec l'État sur une opération digitale, il serait très difficile, voire impossible pour le citoyen de prouver sa bonne foi, sans la coopération active des services de l'État. Dans le cadre de la « Vision Confiance numérique », le premier but de ce projet est de proposer une solution permettant au citoyen d'avoir la souveraineté complète sur ses données et sur ses interactions digitales avec l'État en introduisant un « reçu digital ». De même, l'État pourra à tout moment prouver l'intégrité des données dont il a la responsabilité ou la garde et

---

[11] https://www.eda.admin.ch/aboutswitzerland/fr/home/politik-geschichte/politisches-system/politisches-system-der-schweiz---fakten-und-zahlen.html
[12] https://www.staatslabor.ch/fr/numerisation-dans-le-canton-du-jura-nos-sept-questions-a-matthieu-lachat-chef-du-service-de
[13] https://www.jura.ch/CHA/SIC/Centre-medias/Communiques-2016/Le-Guichet-virtuel-du-Canton-du-Jura-retenu-comme-projet-innovant-par-la-Confederation.html
[14] https://www.ictjournal.ch/news/2021-04-21/administration-jurassienne-des-bornes-interactives-avec-assistance-en
[15] https://www.jura.ch/confiance-numerique
[16] https://www.jura.ch/CHA/SIC/Centre-medias/Communiques-2021/La-confiance-numerique-comme-pilier-des-prestations-en-ligne.html
[17] https://guichet.jura.ch/Pages/Default.aspx

permettre à chaque citoyen de vérifier lesdites preuves, indépendamment de l'État. » (République et Canton du Jura, 2021, p. 7).

Le premier cas d'utilisation du sceau numérique CERTUS et de la *blockchain* KSI sélectionné par la République et Canton du Jura a trait aux extraits du registre des poursuites. Un extrait du registre des poursuites permet à un citoyen de prouver qu'il n'a pas de dettes impayées. Un tel document d'attestation de solvabilité émise par l'État est nécessaire par exemple lors d'une demande de location de logement, de prêt bancaire ou encore de leasing[18]. Sur action du citoyen et lors de l'émission du document au travers du Guichet virtuel de l'État, un QR code est apposé sur l'attestation (cas A sur la figure 1). Sur présentation de l'attestation, tant au format papier que numérique et à l'aide d'une application web ou mobile dédiée, une organisation ou un citoyen peut vérifier l'authenticité de l'extrait du registre des poursuites d'un citoyen jurassien (cas B sur la figure 1).

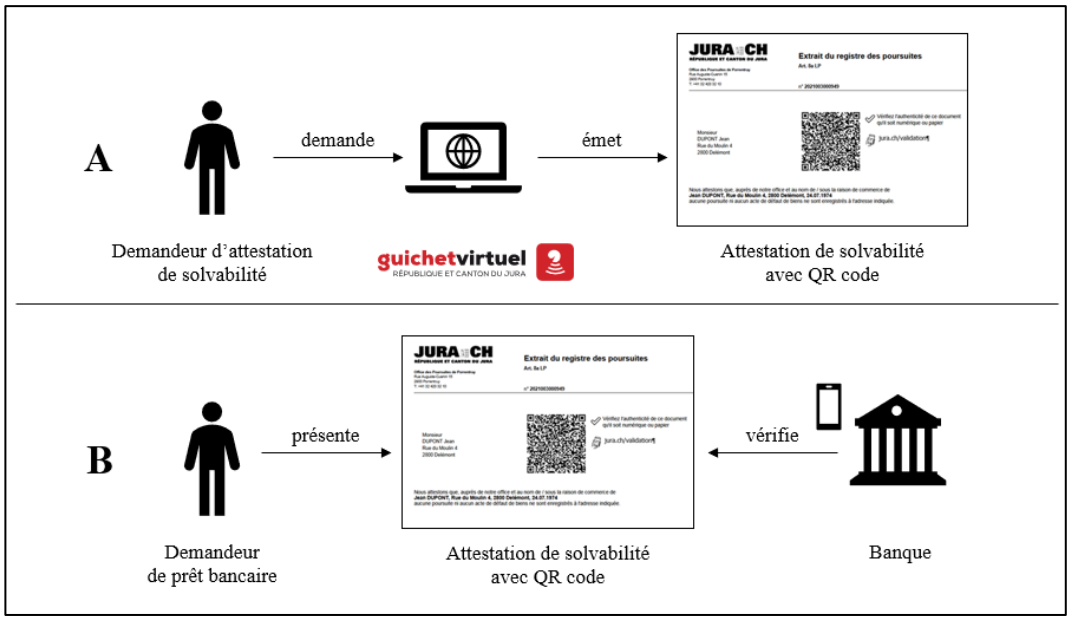

Figure 1 : cas d'utilisation de l'extrait du registre des poursuites (source : auteurs)

Lors de l'émission de l'attestation de solvabilité, un processus informatique est déclenché. Nous le synthétisons en cinq étapes (voir figure 2) : 1) le QR code est apposé sur l'attestation. Ce dernier n'est aucunement relié à une base de données centralisée du canton du Jura et contient les données de l'attestation en texte lisible ainsi qu'une signature cryptographique unique qui assure l'intégrité de ce document ; 2) le sceau numérique CERTUS scelle le QR code afin d'en garantir la sécurité ; 3) une empreinte digitale unique est générée en s'appuyant sur le sceau numérique ; 4) l'empreinte est horodatée sur la *blockchain* KSI afin d'assurer l'immuabilité des informations ; 5) la *blockchain* KSI renvoie une signature numérique qui fait office de reçu digital et qui est stockée dans l'espace personnel du Guichet virtuel du citoyen. Par ce processus, la confiance numérique est assurée par un « tiers garant » qui n'a aucun accès aux données des citoyens qui en gardent ainsi la souveraineté.

[18] https://www.ch.ch/fr/logement/location-d-un-logement/extrait-du-registre-des-poursuites/

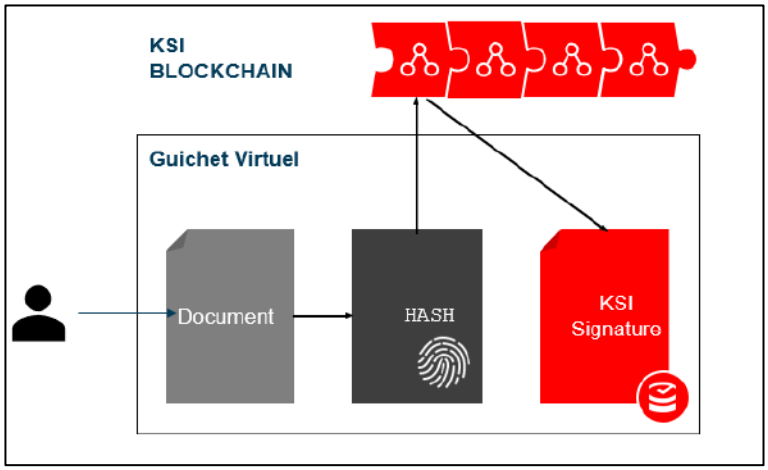

Figure 2 : processus informatique lors de l'émission d'une attestation (source : Canton du Jura)

3.2 Un projet dans une situation extrême de gestion

Le projet CERTUS et *blockchain* KSI de la République et Canton du Jura s'opère dans une situation de gestion que l'on peut qualifier d'extrême. Cette dernière est à distinguer d'une situation classique de gestion par les tensions, la forte évolutivité, l'incertitude ainsi que les risques qui la caractérisent (Godé et al., 2012). La temporalité des décisions dans une telle situation a une valeur particulière (Lièvre, 2016). L'environnement dans lequel ce projet s'est inscrit est marqué par trois sources de tensions. Premièrement, nous rappelons que la Confédération suisse a pré sélectionné deux applications de *pass* sanitaire destinées à lutter contre la propagation des variants pendant la pandémie de la Covid-19. L'application rejetée s'appuie sur les mêmes briques technologiques que celles du projet de la République et Canton du Jura ce qui a créé des tensions dès le début du projet. Deuxièmement, les technologies de la *blockchain* souffrent parfois d'une mauvaise réputation chez le grand public pour des raisons écologiques ou encore de criminalité économique. Troisièmement, des communes suisses font actuellement face à une vague de cyberattaques sans précédent. C'est dans ce contexte tendu qu'en avril 2021, la République et Canton du Jura a contacté notre institution tertiaire d'enseignement et de recherche afin que nous l'accompagnions dans la suite de ce projet.

Nous avons négocié puis convenu avec la République et Canton du Jura de mener une recherche-action (RA) qui vise à mener deux actions d'ici fin 2021 : 1) communiquer sur le projet CERTUS et *blockchain* KSI auprès des différentes parties prenantes dans une situation extrême de gestion et 2) identifier les barrières à l'acceptation de la technologie de sceau numérique et de la *blockchain* KSI. Au-delà de vouloir mener ces deux actions pratiques, notre RA a pour visée de créer de la connaissance scientifique. Pour cette raison, nous avons transformé les actions précédentes en question de recherche, à savoir, comment faire accepter les technologies *blockchain* aux administrés de la République et Canton du Jura dans une situation extrême de gestion ?

4. Méthodologie de recherche

Afin de répondre à notre question de recherche, nous avons mené une recherche-action d'avril à novembre 2021. En intervenant directement avec les acteurs du terrain de recherche, nous visons à satisfaire trois objectifs qui font écho aux caractéristiques de la RA telles que décrites par Baskerville (1999) : 1) créer de la connaissance scientifique en répondant à notre question de recherche tout en résolvant des problèmes pratiques ; 2) rapprocher les praticiens et les chercheurs en SI en nourrissant les compétences de chaque acteur ; 3) appréhender la complexité de cette situation extrême de gestion. Bien que la RA dans le champ des SI puisse épouser des formes diverses (Baskerville & Wood-Harper, 1998), nous avons mené notre recherche en nous inspirant de la méthode cyclique en cinq étapes de Baskerville et Pries-Heje (1999).

Cette RA a été menée en deux itérations. Chacune d'elles vise à répondre à l'un des deux principaux problèmes de la République et Canton du Jura (cf. contexte de la recherche) tout en produisant de la connaissance. La première itération, conduit d'avril à mai 2021, s'intéresse à la communication du projet dans une situation extrême de gestion. Lors de la deuxième itération, conduit de juin à novembre 2021, nous avons traité de l'acceptation de la technologie de sceau numérique CERTUS et de la *blockchain* KSI par la population jurassienne. Conformément aux principes de la RA (Baskerville & Pries-Heje, 1999), chaque itération s'est articulée en cinq phases auxquelles nous avons ajouté quelques aller-retour : (1) diagnostic, (2) plan d'action, (3) réalisation, (4) évaluation et (5) connaissances acquises. Nous précisons enfin que chaque itération a été conduite dans un « environnement de recherche » différent (Baskerville & Wood-Harper, 1998). La figure 3 ci-dessous synthétise la méthodologie de recherche adoptée.

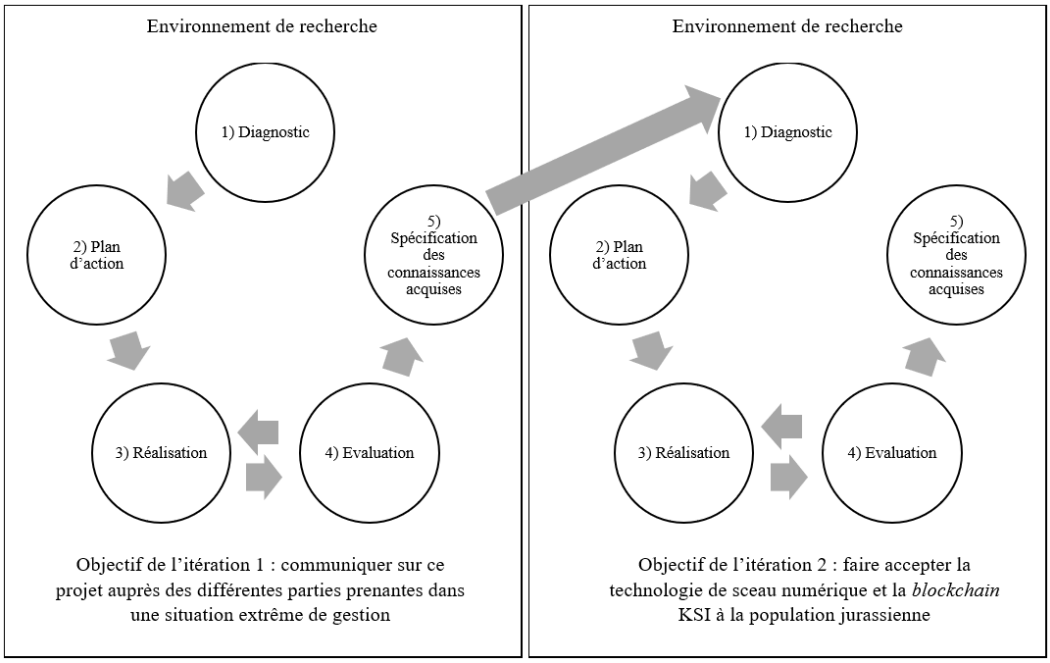

Figure 3 : Synthèse des itérations de notre RA

5. Description et résultats des itérations

Dans cette section, nous décrivons pour chacune des itérations de cette RA : l'environnement de recherche, le diagnostic, le plan d'action, la réalisation puis l'évaluation des actions menées. De plus, nous y exposons les recommandations managériales proposées à la République et Canton du Jura à la fin de cette RA. Nous précisons que les connaissances acquises seront discutées dans la prochaine section.

5.1 Première itération : communication du projet dans une situation extrême de gestion

Nous rappelons que le projet s'est déroulé dans une situation extrême de gestion (cf. contexte de la recherche). Cette situation a influencé l'environnement de recherche de la première itération sur plusieurs plans. Sur un premier plan, l'urgence du contexte sanitaire a engendré une forte tension temporelle. Sur un deuxième plan, le choix de la Confédération suisse d'écarter les briques technologiques CERTUS et la *blockchain* KSI a augmenté l'incertitude et les risques, sources de complexité dans les projets (Missonier, 2014). Afin d'appréhender au mieux cette complexité, nous avons créé une équipe de recherche pluridisciplinaire composée d'un côté de chercheurs en systèmes d'information, en informatique, en communication et en droit des affaires et d'un autre côté de praticiens en informatique, d'entrepreneurs du domaine de la *blockchain* et de journalistes. Afin de clarifier l'objectif de la première itération auprès des membres de l'équipe de RA, nous leur avons rappelé que nous visons à communiquer sur le projet auprès des différentes parties prenantes dans une situation extrême de gestion.

Afin de poser un diagnostic, une partie de l'équipe de RA a adopté un positionnement critique sur l'initiative menée par la République et Canton du Jura. Pour cela, nous avons réalisé trois tâches complémentaires : 1) un groupe de travail restreint composé de deux chercheurs et de trois praticiens en informatique de la République et Canton du Jura s'est penché dans un premier temps sur le fonctionnement des briques technologiques CERTUS et KSI ; 2) puis dans un deuxième temps sur les opportunités métiers (e-gouvernement) offertes par ces technologies ; 3) trois chercheurs et un entrepreneur dans le domaine de la *blockchain* ont analysé en profondeur le livre blanc du projet CERTUS et *blockchain* KSI notamment en le confrontant à la littérature scientifique du domaine[19]. Le diagnostic confirme que le contexte impose qu'un effort important soit fourni sur la communication de ce projet. Le diagnostic révèle enfin qu'il pourrait exister de nombreuses barrières à l'acceptation de la technologie de sceau numérique CERTUS et de la *blockchain* KSI.

À la suite de ce diagnostic, nous avons planifié puis réalisé quatre actions pour répondre à la problématique relative à la communication du projet. Premièrement, la République et Canton du Jura a rédigé une première version du communiqué de presse de présentation du projet CERTUS et KSI. Le communiqué de presse a été analysé par cinq membres de l'équipe de RA qui en a relevé les points forts ainsi que les points d'efforts. Deuxièmement, l'ensemble de l'équipe de RA a organisé et participé à une conférence de presse « à blanc ». Le but était « d'entraîner » les porteurs du projet à répondre adéquatement aux questions potentielles des journalistes. L'équipe de RA a joué le rôle des journalistes. À l'issue de la conférence de presse, de nombreuses critiques ont été émises puis discutées entre les participants. Ces dernières ont été synthétisées dans un rapport qui intégrait également des argumentaires destinés à alimenter les questions potentielles des journalistes lors de la conférence de presse « réelle ».

[19] https://www.egovernment.ch/files/2616/2013/7850/LivreBlanc_Blockchain_CantonJU_2021.pdf

Troisièmement, le communiqué de presse final a été rédigé par la République et Canton du Jura. Quatrièmement, fin mai 2021, le Ministre sponsor de ce projet, le directeur informatique ainsi que le chef de projet de la République et Canton du Jura ont tenu une conférence de presse devant un parterre de journalistes.

Nous avons évalué les actions décrites ci-dessus au travers des articles de presse et des réactions du public. Des journaux locaux, nationaux, grand public ou plus spécialisés dans l'informatique ont repris une partie du communiqué de presse ainsi que les propos du Ministre et de l'équipe du projet. Nous avons été attentifs aux commentaires des internautes sur les sites des journaux et ainsi qu'au retour de la population jurassienne vers les autorités cantonales. Nous n'avons pas relevé de critiques négatives dans un contexte pourtant marqué par les fortes tensions.

Nous les synthétisons les actions menées lors de la première itération ci-dessous.

Phase	**Action**
Diagnostic	Étude du fonctionnement des briques technologiques CERTUS et KSI.
Diagnostic	Identification des opportunités métiers offertes par les technologies CERTUS et KSI.
Diagnostic	Analyse en profondeur le livre blanc du projet en le confrontant à la littérature scientifique du domaine.
Réalisation	Rédaction du communiqué de presse, version 1.
Réalisation	Tenue d'une conférence de presse « à blanc ».
Réalisation	Rédaction du communiqué de presse final.
Réalisation	Tenue de la conférence de presse en présence du Ministre.
Évaluation	Analyse des articles des journaux et des réactions de la population.

Tableau 1 - Actions menées lors de la première itération

5.2 Deuxième itération : l'acceptation de la technologie de sceau numérique et de la *blockchain* KSI

Une partie du diagnostic établi lors de la première itération a œuvré comme point d'entrée d'une deuxième itération de RA. Cela s'inscrit parfaitement dans une approche de RA qui conseille d'exécuter deux itérations afin que les résultats du premier cycle soient approfondis dans le second (Recker, 2013). L'équipe de RA de la deuxième itération est composée de deux chercheurs en systèmes d'information et de trois praticiens de la République et Canton du Jura. L'objectif de cette itération est de faire accepter la technologie de sceau numérique CERTUS et la *blockchain* KSI à la population jurassienne. Pour y répondre, nous avons planifié puis mené trois actions durant la deuxième itération de RA : 1) analyse des maquettes de commande d'un extrait du registre des poursuites ; 2) atelier participatif orienté « grand public » ; 3) atelier participatif orienté « expert en informatique ».

En juillet 2021, nous avons reçu des maquettes des formulaires de commande d'un extrait du registre des poursuites ainsi que des extraits avec un QR Code (scellé numérique CERTUS). Nous les avons analysés au travers de trois tâches séquentielles et complémentaires : 1) étude des composants des formulaires web (labels, champs de saisie, actions, aides, messages et validations) ; 2) étude de l'usabilité au travers des heuristiques de Nielsen (1994) ; 3) étude du séquencement logique du processus métier (extrait du registre des poursuites). Nous avons remis un rapport contenant nos analyses et nos propositions d'amélioration en juillet 2021 à la République et Canton du Jura.

En automne 2021, nous avons conduit deux ateliers participatifs d'une durée d'environ 2 heures et destinés à identifier les barrières à l'acceptation des technologies CERTUS et KSI. Le premier atelier, était orienté grand public, tandis que le second était destiné à des experts en informatique. Les ateliers ont chacun réuni quatre participants, deux observateurs de la République et Canton du Jura et a été conduit par deux modérateurs de l'équipe de RA. Un guide d'atelier a été élaboré en s'appuyant sur les principaux attributs du construit d'utilisabilité (Sagar & Saha, 2020) et des modèles quantitatifs couramment utilisés pour mesurer l'utilisabilité perçue (Lewis, 2018). Chaque atelier comportait deux parties. Dans une première partie orientée « tâches », nous avons mené une expérience d'utilisation des extraits du registre des poursuites sur un système de test. Dans une deuxième partie, nous nous sommes entretenus avec les participants sur le thème de la *blockchain* et de la confiance numérique. Chaque atelier a été enregistré puis retranscrit. Pour des raisons de flexibilité et de traçabilité du processus de recherche, nous avons mobilisé NVivo afin de traiter les retranscriptions des ateliers. Nous avons opté pour une stratégie de codage en deux temps : ouvert puis axial. Ce codage nous a permis d'analyser en profondeur le déroulement des ateliers et nous a dirigés lors de la rédaction du rapport d'analyse (résultats et recommandations) des ateliers participatifs. Les retours des participants ainsi qu'un entretien final avec la République et Canton du Jura nous a permis d'évaluer les actions menées.

Nous les synthétisons les actions menées lors de la deuxième itération ci-dessous.

Phase	**Action**
Réalisation	Analyse des maquettes des formulaires de commandes d'un extrait du registre des poursuites.
Réalisation	Tenue d'un atelier participatif orienté grand public. Expérience d'utilisation des extraits. Entretiens sur le thème de la confiance numérique.
Réalisation	Tenue d'un atelier participatif destiné aux spécialistes en informatique. Expérience d'utilisation des extraits. Entretiens sur le thème de la confiance numérique.
Évaluation	Discussion avec les participants et entretien final avec la République et Canton du Jura.

Tableau 2 - Actions menées lors de la deuxième itération

5.3 Recommandations managériales issues des itérations

Au-delà de répondre aux deux problématiques soulevées par la République et Canton du Jura, la RA a mis en lumière quatre principales recommandations managériales.

La première recommandation managériale concerne le processus de vérification de la conformité d'un extrait du registre des poursuites. En effet, l'expérience d'utilisation des extraits durant les ateliers participatifs a mis en lumière le rejet de la population de l'application de vérification des scellés numérique CERTUS. Cette dernière est siglée CERTUS, or, la population jurassienne connaît peu cette organisation. Elle fait confiance aux institutions de son canton et ne comprend pas l'usage d'une *app* externe. Après avoir réalisé des simulations sur maquettes, nous avons ainsi recommandé de mettre à disposition sur les stores une *app* de vérification de scellé numérique siglée République et Canton du Jura.

Nous rappelons que la République et Canton du Jura a décidé d'intégrer le sceau numérique et la *blockchain* KSI comme briques technologiques centrales de leur Guichet virtuel et plus largement de leur système d'information cyberadministratif. Afin que ces technologies soient utilisées au-delà des extraits de registre des poursuites et qu'elles s'inscrivent dans de multiples cas d'usage, notre deuxième recommandation consiste à identifier toutes les prestations offertes par l'État qui nécessitent un besoin de confiance.

Notre troisième recommandation consiste à faire évoluer les expérimentations citoyennes. L'atelier orienté expérience utilisateurs mené sur les maquettes fonctionnelles nous a permis de récolter de nombreuses informations. Toutefois, un nombre important de remarques négatives était lié à l'environnement de test. Nous recommandons de faire évoluer le guichet virtuel de test en un miroir du guichet virtuel en production. Ainsi, les données collectées correspondront davantage à la réalité et des sujets seront écartés par défaut. Enfin et pour poursuivre dans les expérimentations avec la population, nous recommandons de mettre en place un tiers lieu. Étant donné que la participation aux initiatives (p. ex. dans le cadre politique) dépend aussi de la forme ou du lieu de la participation, nous recommandons de se tourner vers des espaces d'engagement discrets et quotidiens (Jupp, 2008). Un tiers lieu nous semble nécessaire pour comprendre la perception des citoyens des initiatives de la République et du Canton du Jura, mais aussi pour analyser comment les citoyens interagissent avec l'information fournie par l'administration (Evans & Campos, 2012).

La dernière recommandation managériale a trait à la communication sur le thème de la confiance numérique et de la *blockchain*. Dans une volonté de transparence, la République et Canton du Jura a présenté de façon détaillée l'origine du projet CERTUS et KSI, son fonctionnement technologique et les apports pour la population jurassienne. Afin de ne pas ajouter de tensions dans une situation d'ores et déjà extrême, nous recommandons de communiquer en deux niveaux d'abstraction. Le premier niveau doit exposer les cas métiers et l'importance pour un citoyen de rester de rester souverain de ses données. Un deuxième niveau d'abstraction, destiné aux spécialistes des technologies, peut exposer le fonctionnement des briques technologiques CERTUS et de la blockchain KSI. Nous revenons sur cette recommandation plus en profondeur dans la section discussion.

Nous synthétisons les recommandations managériales ainsi que leur but principal dans le tableau ci-dessous (cf. tableau 3).

Recommandation	But
1. Développer une application de vérification CERTUS siglée Jura.	Renforcer le sentiment d'avoir un seul SI piloté par un seul interlocuteur (l'État) afin de limiter le rejet par la population d'une *app* externe.
2. Identifier les services de l'État nécessitant un besoin de confiance.	Justifier le projet par des besoins « métier » et les bénéfices pour la population.
3. Faire évoluer les expérimentations citoyennes.	Limiter le nombre important de remarques négatives relatives à l'environnement de test utilisé lors des ateliers d'expérience utilisateurs.
4. Communiquer en deux niveaux d'abstraction.	Limiter les sources de tensions dans une situation extrême de gestion.

Tableau 3 – Recommandations managériales

5.4 Épilogue

Les briques technologies CERTUS et la *blockchain* KSI ont été mises en production au premier trimestre 2022. Les citoyens jurassiens pourront commander des extraits du registre des poursuites avec scellé numérique dès mars 2022. Une organisation ou un citoyen pourra ainsi vérifier l'authenticité de l'extrait du registre des poursuites d'un citoyen jurassien. Un communiqué de presse pour informer la population sera publié en mars 2022.

6. Discussion

Nous constatons qu'afin d'améliorer la confiance des citoyens envers ses services numériques, la République et Canton du Jura a sélectionné la *blockchain* KSI comme brique technologique centrale de son système d'information. Au terme de l'implémentation de ce projet et au vu des résultats de la RA, il nous apparaît nécessaire de discuter de l'acceptation des technologies *blockchain* dans un contexte cyberadministratif.

L'importance croissante de la transformation numérique de la société mène tant les chercheurs que les praticiens à se pencher sur l'acceptation ou sur le refus des individus à utiliser des technologies de l'information et de la communication. Du côté des chercheurs, de très nombreux travaux sont conduits sur l'acceptation des technologies dans le champ des systèmes d'information. Du côté des praticiens, le projet CERTUS et *blockchain* KSI de la République et Canton du Jura illustre l'importance pour une institution de s'interroger sur l'acceptation de nouvelles technologies qui deviendront les briques centrales du système d'information. Conformément aux travaux de Baudet et Lebraty (2021), la centralité d'une technologie renvoie à sa position dans l'ensemble de l'architecture des technologies de l'information de l'organisation. Dans le cas décrit dans cette communication, la position centrale des technologies CERTUS et KSI est un enjeu majeur pour la République et Canton du Jura. Dans le contexte où cette dernière a fait de la confiance numérique la priorité sur laquelle s'appuyer pour transformer en profondeur l'administration, les porteurs du projet ont émis l'hypothèse que la *blockchain* KSI, comme technologie centrale de leur architecture, va renforcer positivement la confiance numérique des citoyens envers l'administration en ligne.

Afin de valider cette hypothèse, les porteurs du projet postulent que 1) CERTUS et la *blockchain* KSI, par leurs propriétés, peuvent garantir l'authenticité et la sécurité des données des citoyens ; 2) de par son immuabilité et sa transparence, la *blockchain* KSI est amenée à agir comme un tiers de confiance indépendant de l'État. Ces deux points font d'ailleurs écho à deux principaux objectifs escomptés de la *blockchain* présentés dans la littérature scientifique du domaine : 1) garantir la confidentialité des données et 2) accroître la confiance entre les parties prenantes (Tshering & Gao, 2020). Bien que nous soyons convaincus par les bénéfices des technologies *blockchain* dans un contexte cyberadministratif et que soutenons en partie l'hypothèse émise par les porteurs du projet, il nous apparaît nécessaire 1) d'en discuter les limites et 2) de mettre en lumière un certain paradoxe de la transparence des technologies *blockchain* dans une situation extrême de gestion.

6.1 Un fonctionnaire dans son *smartphone* pour renforcer la confiance numérique

Nos résultats tendent à démontrer que la mise en œuvre de la *blockchain* KSI diminue la confiance des citoyens envers l'État. Selon les porteurs du projet, un besoin de confiance est nécessaire entre les citoyens et l'État. Or, un très haut niveau de confiance existe d'ores et déjà entre ces deux parties. La population jurassienne fait confiance à ses institutions. Positionner la *blockchain* KSI comme tiers de confiance indépendant de l'État contribue au contraire à diminuer la confiance entre les citoyens et l'État pour trois raisons : 1) des citoyens émettent un doute quant au lieu de stockage de leurs données bien que ces dernières restent en Suisse ; 2) les technologies *blockchain* ont mauvaise réputation ; 3) la *blockchain* KSI est d'origine estonienne. Ces raisons se sont révélées être des barrières à l'acceptation par les citoyens des technologies de ce projet. Une partie de la communication de ce projet avait pour visée de lever ces barrières à l'adoption. En effet, le livre blanc met en lumière 1) l'intérêt pour le citoyen de garder la souveraineté complète sur ses données et sur ses interactions digitales avec l'État ; 2) les avantages écologiques et sécures de la *blockchain* KSI ; 3) l'historique du projet KSI et sa fiabilité.

Nos résultats tendent également à démontrer que la mise en œuvre de la *blockchain* KSI renforce la confiance entre citoyens. En effet, le besoin de confiance doit être augmenté entre les citoyens. Prenons l'exemple d'un citoyen A qui désire louer un bien immobilier à un citoyen B. Via l'*app* dédiée, le citoyen A peut contrôler l'authenticité et la conformité de l'extrait du registre des poursuites du citoyen B. Dans un tel cas, nous relevons que l'*app* de vérification de l'extrait du registre des poursuites permet de renforcer la confiance entre les citoyens.

6.2 Le paradoxe de la transparence des technologies *blockchain* dans une situation extrême de gestion

Afin de ne pas ajouter de tensions dans une situation d'ores et déjà extrême, nous avons recommandé à la République et Canton du Jura de communiquer en deux niveaux d'abstraction sur le thème de la confiance numérique et de la *blockchain* : 1) exposer les cas métiers et l'importance pour un citoyen de rester souverain de ses données ; 2) exposer aux spécialistes des technologies le fonctionnement des briques technologiques CERTUS et de la *blockchain* KSI. Communiquer sur un projet de cette nature, tant compliqué techniquement que complexe dans une situation de gestion extrême n'est pas aisé. Nous relevons que s'il existe des instruments pour évaluer l'utilité des technologies *blockchain* (voir Koens & Poll, 2018) ou comparer des projets s'appuyant sur ces technologies dans un contexte de cyberadministration (Allessie et al., 2019), il n'existe pas à notre connaissance, de travaux scientifiques qui livrent

des clés sur comment communiquer de tels projets vers les différentes parties prenantes. Comme nous l'avons souligné ci-dessus, une partie de la communication autour du projet nous semble adéquate et de qualité. La partie très (trop) transparente sur le fonctionnement des nouvelles briques technologiques ajoute encore des tensions dans une situation d'ores et déjà extrême. Enfin, la volonté de la République et Canton du Jura de communiquer de façon transparente met en lumière un certain paradoxe.

Le mot transparence vient du latin *trans* (au-delà) et *parere* (apparaître). Dans un sens figuré, il peut s'agir de la « qualité d'une institution qui informe complètement sur son fonctionnement, ses pratiques »[20]. Cela est repris dans un contexte gouvernemental, où la notion de transparence englobe en partie celle de la responsabilité (Ball, 2009). Dans le champ des systèmes d'information, la littérature s'intéresse depuis de nombreuses années à la transparence des informations récoltées par les entreprises (Awad & Krishnan, 2006) ou encore à la transparence dans la communication des entreprises (Street & Meister, 2004). Dans le contexte des technologies *blockchain* dans la cyberadministration, nous rappelons que Batubara et al. (2018) affirment que la capacité de la *blockchain* à enregistrer les transactions distribuées permet d'améliorer la transparence, de prévenir la fraude et d'augmenter la confiance envers le secteur public. Cagigas et al. (2021), exposent que la transparence offerte par la *blockchain* permet aux citoyens d'exercer un plus grand contrôle sur leurs données personnelles.

Communiquer de façon transparente sur les technologies *blockchain* apparaissait de prime abord comme une voie naturelle. Paradoxalement, informer la population de façon exhaustive quant au fonctionnement des technologies CERTUS et KSI a amené de la confusion dans une situation déjà tendue, d'une part, car de nombreux éléments sont sujets à discussion, et d'autre part, car des citoyens non intéressés/sans compétences technologiques n'ont pas les clés de lectures nécessaires afin d'être réceptifs à des argumentaires techniques. Il en résulte de cette volonté de transparence de mauvaises interprétations qui se révèlent être des barrières à l'adoption de telles technologies. Paradoxalement encore, la communication d'un projet conduit par un gouvernement se doit d'être transparente. Toutefois, s'il est nécessaire d'informer les citoyens par exemple sur les bénéfices escomptés, les coûts ou encore sur les processus de sélection des partenaires d'un projet, il nous semble non nécessaire « d'ouvrir le capot » pour exposer le fonctionnement des technologies *blockchain*. Preuve peut-être que les technologies *blockchain* sont devenues matures.

6. Conclusion

Comment faire accepter les technologies *blockchain* aux administrés de la République et Canton du Jura dans une situation extrême de gestion ? En limitant les sources de tensions par une communication en deux niveaux : 1) de façon transparente sur les apports pour la population sans évoquer les aspects techniques des technologies *blockchain* ; 2) de façon détaillée sur les aspects techniques pour les spécialistes qui le désirent.

Les quatre recommandations managériales présentées dans cette communication constituent à nos yeux un apport important qui, nous l'espérons, permettra de rapprocher les mondes quelques fois trop éloignés des praticiens et des chercheurs en gestion. D'un point de vue

[20] https://www.cnrtl.fr/definition/transparence

méthodologique, cette communication peut servir de modèle aux chercheurs qui désirent résoudre des problèmes pratiques tout en créant de la connaissance scientifique.

Deux limites importantes méritent d'être soulignées. Premièrement, l'analyse en profondeur d'un cas ne permet aucune généralisation bien que les résultats présentés ici soient potentiellement transférables à d'autres cas aux caractéristiques quasi similaires. Deuxièmement, lors de notre RA, nous avons identifié de nombreuses pistes de réflexion possibles au travers de ce cas. Le foisonnement de données récoltées a compliqué la rédaction de cette communication. Ainsi, nous avons fait le choix de présenter notre cas sous le prisme de l'acceptation et de discuter d'un certain paradoxe de la transparence des technologies *blockchain* dans une situation extrême de gestion. La communication portée par un Ministre, la citoyenneté des données ou encore les cas d'usage d'une *app* de validation de la conformité de documents émis par l'État méritent quant à eux aussi d'être analysés en profondeur.

Références

Alexopoulos, C., Charalabidis, Y., Androutsopoulou, A., Loutsaris, M. A., Lachana, Z. (2019), Benefits and obstacles of blockchain applications in e-government, *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Hawaii, USA.

Allessie, D., Sobolewski, M., Vaccari, L., Pignatelli, F. (2019), *Blockchain for digital government*, Publications Office of the European Union, Luxembourg.

Awad, N. F., & Krishnan, M. S. (2006), The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS Quarterly*, vol. 30, n°1, p. 13-28.

Ball, C. (2009), What Is Transparency?, *Public Integrity*, vol. 11, n°4, p. 293-308.

Baskerville, R. L. (1999), Investigating information systems with action research. *Communications of the association for information systems*, vol. 2, n°1, p. 19.

Baskerville, R., Pries-Heje, J. (1999), Grounded action research: a method for understanding IT in practice, *Accounting, Management and Information Technologies*, vol. 9, n°1, p. 1-23.

Baskerville, R., Wood-Harper, A. T. (1998), Diversity in information systems action research methods, *European Journal of information systems*, vol. 7, n°2, p. 90-107.

Batubara, F. R., Ubacht, J., Janssen, M. (2018), Challenges of blockchain technology adoption for e-government: a systematic literature review, *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, Delft, the Netherlands.

Baudet, C., Lebraty, J. F. (2021), Exploration des fondements et des usages de la notion de centralité en SI au travers d'une analyse bibliométrique, *26e conférence de l'Association information et Management*, Nice (online), France.

Benbasat, I., Zmud, R. W. (1999), Empirical Research in Information Systems: The Practice of Relevance, *MIS Quarterly*, vol. 23, n°1, p. 3-16.

Brynjolfsson, E., Wang, C., Zhang, X. (2021), The economics of IT and digitization: eight questions for research, *MIS Quarterly*, vol. 45, n°1, p. 473-477.

Cagigas, D., Clifton, J., Diaz-Fuentes, D., Fernández-Gutiérrez, M. (2021), Blockchain for public services: A systematic literature review, *IEEE Access*, vol. 9, p. 13904-13921.

Davis, F. D. (1989), Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, vol. 13, n°3, p. 319-340.

Evans, A. M., Campos, A. (2012), Open Government Initiatives: Challenges of Citizen Participation, *Journal of Policy Analysis and Management*, vol. 32, N°1, p. 172-185.

Godé, C., Hauch, V., Lasou, M., Lebraty, J.-F. (2012), Une singularité dans l'aide à la décision : le cas de la Liaison 16, *Systèmes d'information et Management*, vol. 17, n°2, p. 9-38.

Jeanneret Medina, M., Baudet, C., Doan, K., Lebraty, J. F. (2020), Les impacts des technologies blockchain sous le prisme de la théorie de l'agence: étude de cas multiple dans le domaine de la supply chain, *25e conférence de l'Association information et Management*, Marrakech (online), Maroc.

Jupp, E. (2008), The feeling of participation: Everyday spaces and urban change, *Geoforum*, vol. 39, n°1, p. 331-343.

Koens, T., Poll, E. (2018), What blockchain alternative do you need?, *ESORICS 2018 International Workshops*, Barcelona, Spain.

Lacity, M. C. (2018), Addressing key challenges to making enterprise blockchain applications a reality, *MIS Quarterly Executive*, vol. 17, n°3, p. 201-222.

Lebraty, J.-F. (2013), SI et situations extrêmes, *Systèmes d'information & Management*, vol. 18 ; n°1, p. 3-10.

Lewis, J. R. (2018), Measuring Perceived Usability: The CSUQ, SUS, and UMUX, *International Journal of Human-Computer Interaction*, vol. 34, n°12, p. 1148- 1156.

Lièvre, P. (2016), État et développement d'un programme de recherche, *Revue française de gestion*, n°4, p. 79-94.

Missonier, S. (2014), Une typologie de la complexité in C. Baudet, *Gestion de projet et innovation*, Editions L'Harmattan, Paris, p. 25-38.

Nakamoto, S. (2008), Bitcoin: A peer-to-peer electronic cash system, *Decentralized Business Review*, p. 9.

Nielsen, J. (1994), Enhancing the explanatory power of usability heuristics, *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, Boston, USA.

Rana, N. P., Dwivedi, Y. K., Hughes, D. L. (2021), Analysis of challenges for blockchain adoption within the Indian public sector: an interpretive structural modelling approach, *Information Technology and People*, https://doi.org/10.1108/ITP-07-2020-0460

Recker, J. (2013), *Scientific research in information systems: a beginner's guide*, Springer, Berlin.

Reddick, C. G., Cid, G. P., Ganapati, S. (2019), Determinants of blockchain adoption in the public sector: An empirical examination, *Information Polity*, vol. 24, n°4, p. 379-396.

République et Canton du Jura. (2021), Solution de sécurisation électronique des documents & services administratifs : La Blockchain au service de la confiance numérique en Suisse, sur le

modèle estonien, Livre blanc
https://www.egovernment.ch/files/2616/2013/7850/LivreBlanc_Blockchain_CantonJU_2021.pdf

Sagar, K., Saha, A. (2020), A systematic review of software usability studies, *International Journal of Information Technology*, https://doi.org/10.1007/s41870-017-0048-1

Street, C. T., Meister, D. B. (2004), Small business growth and internal transparency: The role of information systems, *MIS Quarterly*, vol. 28, n°3, p. 473-506.

Tshering, G., Gao, S. (2020), Understanding security in the government's use of blockchain technology with value focused thinking approach, *Journal of Enterprise Information Management*, vol. 33, n°3, p. 519-540.