RAPPORT 3

Livrable n°3 :

Enjeux d'implantation d'une chaîne de blocs dans un écosystème gouvernemental

Table des matières

Listes de recommandations 3
Introduction 5
Enjeux techniques d'implantation de la chaîne de de blocs 5
Enjeux humains d'implantation de la chaîne de blocs 10
Enjeux organisationnels d'implantation de la chaîne de blocs 13
Références 21

Listes de recommandations

Recommandation 1 : Les organisations gouvernementales doivent mettre en place des stratégies pour la sécurisation des données contre les attaques de 51%. 5

Recommandation 2 : Les organisations gouvernementales qui adoptent les applications basées sur la chaîne de blocs doivent se rassurer de la correction de leurs codes sources, à travers différents tests appropriés, avant leur implantation. 6

Recommandation 3 : Les organisations gouvernementales qui souhaitent adopter la chaîne de blocs doivent identifier les données hautement sensibles à stocker *« on-chain »* et les données moins sensibles *« off-chain »*..... 6

Recommandation 4 : Les organisations gouvernementales qui recourent à ces systèmes de stockage centralisés pour le stockage « off-chain » doivent mettre en place des stratégies de mitigation des risques de sécurité inhérents à ces systèmes. 7

Recommandation 5 : Les organisations gouvernementales doivent mettre en place des mécanismes de sécurité adaptés pour le chiffrement des données et l'anonymat des utilisateurs afin d'assurer la confidentialité des échanges réalisés dans le réseau. 7

Recommandation 6 : Les organisations gouvernementales doivent tenir compte des capacités de traitement des données des chaînes de blocs qu'elles souhaitent adopter en fonction de la vitesse de traitement de leurs données. 7

Recommandation 7 : Les organisations peuvent adopter les chaînes de blocs dont l'algorithme de consensus est différent du PoW, soit le PoS. 8

Recommandation 8 : Les organisations gouvernementales peuvent recourir aux applications basées sur la chaîne de blocs disponibles dans le cloud computing lorsqu'elles ne disposent pas de l'infrastructure requise pour supporter l'exploitation de ces applications. 8

Recommandation 9 : Les organisations gouvernementales doivent choisir des solutions basées sur la chaîne de blocs interopérables. Ceci permet à ces organisations d'échanger facilement des informations d'entre elles pour améliorer les services rendus aux citoyens ou aux autres partenaires ayant besoin de leurs services. 9

Recommandation 10 : Sensibiliser les adoptants potentiels sur les bénéfices et les défis d'implantation des applications basées sur la chaîne de blocs en ce qui concerne les coûts et les ressources humaines et matérielles à mobiliser. 10

Recommandation 11 : Adopter une approche graduelle d'implantation de la chaîne de blocs pour faire face à de nombreux obstacles organisationnels, technologiques et institutionnels rencontrés tout au long du processus d'implantation de la chaîne de blocs. 11

Recommandation 12 : Instaurer une culture de sécurité chez les développeurs et les adoptants de la chaîne de blocs pour éviter certains risques de sécurité qui pourraient provenir de la mauvaise utilisation et développement des applications basées sur la chaîne de blocs. 11

Recommandation 13 : Les organisations gouvernementales qui adoptent la chaîne de blocs doivent s'assurer que les données saisies par les utilisateurs (oracles) sont valides, car la chaîne de blocs garantit l'intégrité à toute donnée, même invalide (non exact), qui y est stockée. 12

Recommandation 14 : La compréhension des éléments à gouverner et la manière de gouverner les applications basées sur la chaîne de blocs sont fondamentales pour le succès de leur implantation dans le contexte gouvernemental. 15

Recommandation 15 : Les organisations gouvernementales devront adopter d'autres stratégies de stockage des données, à l'occurrence le stockage « off-Chain » qui consiste à stocker les données personnelles des individus dans leurs bases de données locales. Ensuite, n'utiliser la chaîne de blocs que pour sécuriser ces données à travers des mécanismes cryptographiques. 16

Recommandation 16 : L'adoption de la chaîne de blocs par les organisations gouvernementales exige à ces dernières de développer des stratégies pour garantir la confidentialité des données dans la chaîne de blocs étant donné que les données sont transparentes dans le réseau. 17

Recommandation 17 : Les organisations doivent veiller à la performance des applications basées sur la chaîne de blocs en procédant aux tests de sécurité et de fiabilité ainsi que ceux d'intégration de ces applications avec les systèmes existants. 18

Recommandation 18 : Les organisations gouvernementales devraient privilégier l'utilisation des chaînes de blocs qui respectent les exigences écologiques et environnementales en faisant recours, par exemple, aux chaînes de blocs qui implémentent l'algorithme PoS ou aux chaînes de blocs de troisième génération. 18

Introduction

Cette section présente les enjeux et les défis d'implantation de la chaîne de blocs au sein des organisations gouvernementales. Dans la littérature académique et professionnelle, plusieurs auteurs se sont intéressés aux enjeux d'implémentation de la chaîne de blocs dans différents secteurs d'activités (Koteska et al., 2017, Zheng et al., 2018). Ces auteurs analysent les enjeux d'implantation de la chaîne de blocs sur trois principaux aspects, à savoir l'aspect technique, humain et organisationnel. Par conséquent, la présente section est divisée en trois sous-sections qui présentent respectivement les enjeux techniques, humains et organisationnels d'implantation de la chaîne de blocs avec une attention particulière au domaine gouvernemental.

Enjeux techniques d'implantation de la chaîne de de blocs

Les enjeux techniques d'implantation de la chaîne de blocs concernent les défis liés à cette technologie et à son infrastructure technique de mise en œuvre (Koteska et al., 2017, Zheng et al., 2018, Tan et al., 2022). Dans leur étude, Koteska et al. (2017) analysent les défis d'implantation de la chaîne de blocs en mentionnant que l'implantation de la chaîne de blocs doit s'adapter à certaines impératives techniques liées à son infrastructure technique et aux limites inhérentes à cette technologie. Principalement, les défis sont liés à la sécurité et à la confidentialité garanties par la chaîne de blocs, à la validité des données, à la transparence du registre des données, à la capacité de stockage et au débit ou à la vitesse de traitement des transactions (Upadhyay, 2020).

Le défi lié à la sécurité et à la confidentialité renvoie aux vulnérabilités des applications basées sur la chaîne de blocs, comme par exemple le risque d'avoir un nœud du réseau qui contrôle 51% de la puissance de calcul de l'ensemble des membres du réseau (Zheng *et al.*, 2017). Cette situation donne la possibilité à un nœud du réseau de modifier facilement le registre des données de la chaîne de blocs. Dans le contexte gouvernemental, le type de la chaîne de blocs adopté est généralement privé ou en consortium (Kim, 2021). Ce type de chaîne de blocs comprend un nombre relativement faible de participants ce qui pourrait faciliter aux nœuds malveillants d'atteindre une puissance de calcul qui dépasse la puissance de calcul du réseau et de modifier, par conséquent, le registre des données.

Recommandation 1 : Les organisations gouvernementales doivent mettre en place des stratégies pour la sécurisation des données contre les attaques de 51%.

Le deuxième défi lié à la sécurité des données est le caractère irréversible (non modifiable) du registre de la chaîne de blocs empêchant la modification et la suppression des données enregistrées dans ce registre. L'immuabilité de la chaîne de blocs, en plus d'être un avantage, constitue également un risque de sécurité pour les applications basées sur la chaîne de blocs, car il rend impossible la correction des erreurs de codage de ces applications, comme les contrats intelligents (Zamani et al., 2020). Ces erreurs de codage sont utilisées par les pirates informatiques pour attaquer les applications basées sur la chaîne de blocs. C'est l'exemple, en 2016, de l'attaque de DAO servant à une collecte de fonds qui a causé une perte de plusieurs millions de dollars (Zamani et al., 2020).

Recommandation 2 : Les organisations gouvernementales qui adoptent les applications basées sur la chaîne de blocs doivent se rassurer de la correction de leurs codes sources, à travers différents tests appropriés, avant leur implantation.

Les défis liés à la capacité de stockage et au débit de traitement des transactions sont inhérents aux caractéristiques et aux types de la chaîne de blocs. En effet, chaque bloc du réseau de la chaîne de blocs a une capacité de stockage limitée (Zheng *et al.*, 2017). Avec une capacité limitée, il est impossible à la chaîne de blocs de stocker de grandes quantités de données. D'où le recours au stockage « *off-chain »* dans plusieurs applications basées sur la chaîne de blocs (Gordon and Catalini, 2018). Le choix du stockage *« off-chain »* s'explique également par le coût de stockage des données élevé lorsqu'on adopte le stockage *« on-chain »* des données (Gürsoy et al., 2020).

Recommandation 3 : Les organisations gouvernementales qui souhaitent adopter la chaîne de blocs doivent identifier les données hautement sensibles à stocker *« on-chain »* et les données moins sensibles *« off-chain »*.

Les organisations gouvernementales peuvent également réduire les coûts de stockage des données en gardant uniquement les métadonnées sur la chaîne de blocs et les données brutes dans leurs bases de données locales. De même, les organisations qui souhaitent contourner les problèmes liés à la capacité de stockage et au débit de traitement des transactions peuvent recourir aux chaînes de blocs de troisième génération, comme Cardano, Solana, Chia, Nano, IOTA. En effet, cette génération de la chaîne de blocs apporte des solutions aux problèmes des générations précédentes, comme le manque d'évolutivité, d'interopérabilité et de durabilité des chaînes de blocs (Futura, 2021).

Les systèmes de stockage « *off-chain* » auxquels peuvent recourir les organisations gouvernementales sont pour la plupart centralisés (par exemple, le système cloud computing ou serveurs locaux centralisés). La configuration centralisée de ces systèmes les expose à plusieurs risques de sécurité, comme le point de défaillance unique (Hao et al., 2019, Hao et al., 2020).

Recommandation 4 : Les organisations gouvernementales qui recourent à ces systèmes de stockage centralisés pour le stockage « off-chain » doivent mettre en place des stratégies de mitigation des risques de sécurité inhérents à ces systèmes.

Un autre défi majeur de la technologie de la chaîne de blocs est le caractère transparent du registre des données pour l'ensemble des membres du réseau (Casino *et al.*, 2019). Le caractère transparent de la chaîne de blocs suppose que l'ensemble d'informations (transactions) qu'elle stocke est visible pour toutes les parties prenantes du réseau de la chaîne de blocs (Gürsoy et al., 2020).

Recommandation 5 : Les organisations gouvernementales doivent mettre en place des mécanismes de sécurité adaptés pour le chiffrement des données et l'anonymat des utilisateurs afin d'assurer la confidentialité des échanges réalisés dans le réseau.

Grâce à ces mécanismes de protection, seules les personnes autorisées pourront avoir accès aux données stockées dans le réseau. L'absence de ces mécanismes de protection expose les systèmes basés sur la chaîne de blocs au problème de confidentialité des données échangées au sein du réseau.

La faible vitesse de traitement des transactions reste toujours une limite permanente pour les chaînes de blocs de deuxième génération, et en particulier dans les chaînes de blocs publiques qui utilisent les algorithmes de consensus PoW (Agbo et Mahmoud, 2020). En effet, le débit de traitement des informations de ces chaînes de blocs est limité à 7 transactions par seconde et la production de chaque nouveau bloc intervient chaque 10 minutes (Zheng *et al.*, 2017). Ce qui constitue un grand désavantage de ces chaînes de blocs dans un environnement où la rapidité de traitement de l'information est de rigueur.

Recommandation 6 : Les organisations gouvernementales doivent tenir compte des capacités de traitement des données des chaînes de blocs qu'elles souhaitent adopter en fonction de la vitesse de traitement de leurs données.

En cas d'exigence des systèmes avec des vitesses de traitement élevées des transactions, les organisations peuvent recourir aux chaînes de blocs de troisième génération (Futura, 2021). La

chaîne de blocs est une technologie dont le fonctionnement occasionne le gaspillage des ressources lorsqu'elle utilise l'algorithme de consensus PoW (Roman-Belmonte *et al.*, 2018). En effet, les mineurs d'un réseau de la chaîne de blocs qui utilise cet algorithme sont continuellement en compétition pour obtenir la preuve de travail nécessaire à la production des blocs valides (Zheng *et al.*, 2017). Ceci nécessite une puissance de calcul très importante, ce qui implique une consommation excessive d'énergie électrique. Cette consommation excessive d'énergie augmente les coûts liés à l'utilisation des applications basées sur la chaîne de blocs et pourrait négativement influencer le rendement attendu de l'implantation de la chaîne de blocs dans les organisations gouvernementales. Pour contourner cette limite, deux solutions s'offrent aux organisations gouvernementales (recommandations 7 et 8).

Recommandation 7 : Les organisations peuvent adopter les chaînes de blocs dont l'algorithme de consensus est différent du PoW, soit le PoS.

Comme mentionné dans la section 1.1.1 de la présente revue de littérature, PoS est un algorithme de consensus qui n'exige pas de puissance de calcul élevée pour valider les transactions du réseau, car les valideurs des blocs sont choisis aléatoirement, entre autres, en fonction de la quantité des cryptomonnaies détenue dans leurs portefeuilles numériques (Zheng et al., 2017). En plus du choix de l'algorithme PoS, les organisations qui ne disposent pas de l'infrastructure requise pour supporter les applications basées sur la chaîne de blocs peuvent exploiter les offres de services basées sur la chaîne de blocs disponibles dans le cloud computing (Clohessy and Acton, 2019).

Recommandation 8 : Les organisations gouvernementales peuvent recourir aux applications basées sur la chaîne de blocs disponibles dans le cloud computing lorsqu'elles ne disposent pas de l'infrastructure requise pour supporter l'exploitation de ces applications.

Cette recommandation permet aux organisations gouvernementales de ne pas supporter la charge et les dépenses liées à la possession de l'infrastructure technique de la chaîne de blocs (Clohessy and Acton, 2019). Manuel Badel (2019) s'est également intéressé aux enjeux techniques d'implantation de la chaîne de blocs. Pour cet auteur, il s'agit des contraintes techniques qui doivent être respectées lors du développement et de l'implantation des applications basées sur la chaîne de blocs dans un secteur d'activités particulier. Ces contraintes concernent, entre autres, l'intégration d'une approche basée sur la chaîne de blocs dès le début d'un projet basé sur la chaîne de blocs; l'interopérabilité entre différentes chaînes de blocs

utilisées dans le secteur d'activités, d'une part, et l'interopérabilité entre la chaîne de blocs et systèmes existants, d'autre part; l'évolutivité de la chaîne de blocs qui doit prendre en compte la capacité de traiter des gros volumes des transactions. L'interopérabilité des chaînes de blocs suppose la capacité de ces dernières, bien que différentes, à partager facilement les données (Lafourcade and Lombard-Platet, 2020). Cette exigence d'interopérabilité est un enjeu majeur dans le contexte gouvernemental, car certaines offres de services rendus aux citoyens exigent souvent que plusieurs organisations gouvernementales échangent des informations (Kim, 2021). Cette absence d'interopérabilité entre chaînes de blocs justifie, pour la plupart, la résistance à l'adoption de la chaîne de blocs dans plusieurs secteurs d'activités (Hylock and Zeng, 2019, Daraghmi et al., 2019).

Recommandation 9 : Les organisations gouvernementales doivent choisir des solutions basées sur la chaîne de blocs interopérables. Ceci permet à ces organisations d'échanger facilement des informations d'entre elles pour améliorer les services rendus aux citoyens ou aux autres partenaires ayant besoin de leurs services.

Meinert et al. (2019) se sont également intéressés à l'implantation des applications basées sur la chaîne de blocs dans le secteur de la santé en mettant en évidence certains défis qui doivent être prise en compte par les adoptants qui sont les structures de santé et les patients. Il s'agit des défis de sécurité, d'interopérabilité et d'accès rapide aux données médicales ou d'évolutivité de la chaîne de blocs. La figure 1 présente les principaux enjeux et défis techniques d'implantation des applications basées sur la chaîne de blocs.

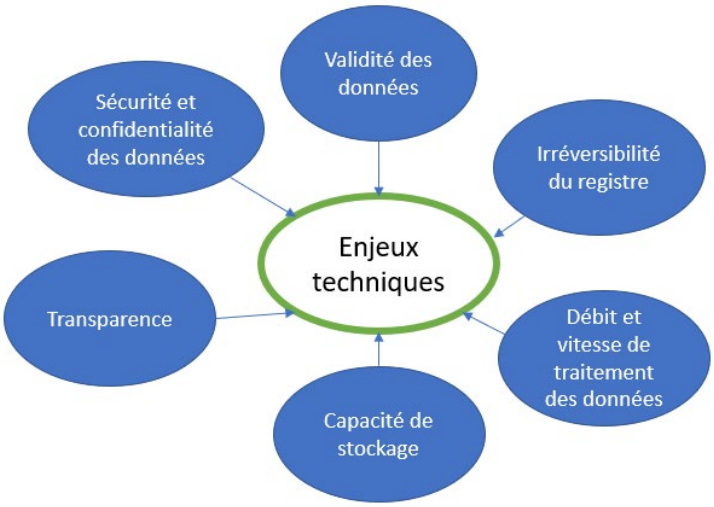

Figure 1. Enjeux techniques d'implantation des applications basées sur la chaîne de blocs

Enjeux humains d'implantation de la chaîne de blocs

Les enjeux humains d'implantation de la chaîne de blocs renvoient aux facteurs humains qui conditionnent le développement, l'implantation et l'utilisation efficaces des applications basées sur la chaîne de blocs (Zamani et al., 2020). Ces enjeux incluent, entre autres, le manque d'informations concernant cette technologie, la perception des adoptants potentiels, les compétences en informatique et en sécurité des utilisateurs et des développeurs, la crédibilité des oracles, la culture de la sécurité (Zamani et al., 2020, White et al., 2020, Putz and Pernul, 2020) (cf. figure 3).

Le manque d'informations fait référence au manque des connaissances claires sur la chaîne de blocs étant donné le caractère « nouveau » de la technologie (Mendling et al., 2018). Ce manque d'informations se justifie par la faible sensibilisation sur les bénéfices et les défis d'implantation de la chaîne de blocs (Mendling et al., 2018).

En plus du manque d'information sur la chaîne de blocs, les défis humains d'implantation de cette technologie concernent également l'absence des ressources qualifiées pour développer, gérer et contrôler les solutions basées sur cette technologie (Zamani et al., 2020). Ce manque d'informations et des ressources limitent la mesure dans laquelle ces solutions sont développées et déployées (Mendling et al., 2018). L'autre défi lié au manque d'information sur la chaîne de blocs est le manque des précisions sur les coûts de développement et d'implantation des solutions basées sur la chaîne de blocs (Mendling et al., 2018). Ceci influence négativement l'adoption et la diffusion généralisée de la chaîne de blocs dans les organisations.

Parmi les auteurs qui se sont intéressés aux défis humains d'implantation de la chaîne de blocs, Manuel Badel (2019) mentionne que la perception et la compréhension de la chaîne de blocs par les adoptants potentiels constituent un enjeu majeur d'adoption et d'implantation de la chaîne de blocs dans un secteur d'activités. En effet, la prise en compte de ce défi dans l'implantation de la chaîne de blocs, surtout dans le secteur public où interviennent les organisations gouvernementales et les citoyens, permet de comprendre la manière dont la communauté perçoive cette technologie et les risques y associés (Iredale, 2021). Ceci permet de mieux formuler des stratégies d'information et de sensibilisation en rapport avec cette technologie.

Recommandation 10 : Sensibiliser les adoptants potentiels sur les bénéfices et les défis d'implantation des applications basées sur la chaîne de blocs en ce qui concerne les coûts et les ressources humaines et matérielles à mobiliser.

Cette sensibilisation doit viser à informer les adoptants potentiels (organisations gouvernementales et les citoyens) sur des questions souvent mises en avant, comme la défaillance technologique, l'évolutivité, l'impact écologique du protocole de consensus, la protection des données personnelles et la manière dont la chaîne de blocs viendra impacter leurs activités quotidiennes (Joëlle Toledano, 2018, Iredale, 2021). La sensibilisation des adoptants potentiels sur les changements qu'apporterait l'utilisation de la chaîne de blocs dans leurs activités permet de combattre anticipativement la résistance des individus à adopter les applications basées sur cette technologie. Cette résistance pourrait également être surmontée par une adoption graduelle des applications basées sur la chaîne de blocs (MIGNON, 2019). En effet, la mise en place des applications basées sur la chaîne de blocs exige une évolution des pratiques et des mentalités des adoptants, puisque son adoption revient à abandonner une longue tradition de gestion centralisée au profit d'un système décentralisé et dépourvu de toute autorité de contrôle (MIGNON, 2019).

Recommandation 11 : Adopter une approche graduelle d'implantation de la chaîne de blocs pour faire face à de nombreux obstacles organisationnels, technologiques et institutionnels rencontrés tout au long du processus d'implantation de la chaîne de blocs.

Pour Zamani et al. (2020), les défis humains d'implantation de la chaîne de blocs concernent également les compétences en sécurité des utilisateurs et des développeurs des applications basées sur la chaîne de blocs. En effet, leurs compétences en sécurité permettent de concevoir et de développer des applications basées sur la chaîne de blocs qui respectent certaines normes de sécurité (Hasanova et al., 2019).

Recommandation 12 : Instaurer une culture de sécurité chez les développeurs et les adoptants de la chaîne de blocs pour éviter certains risques de sécurité qui pourraient provenir de la mauvaise utilisation et développement des applications basées sur la chaîne de blocs.

Bien que la chaîne de blocs assure la sécurité des données, il se pose toujours le problème de la validité des données saisies en entrée ou en provenance des oracles qui peuvent être des humains ou des matériels (Lemieux, 2016), car une fois les données saisies par les utilisateurs sont validées par les membres du réseau, elles deviennent directement une vérité dans le réseau de la chaîne de blocs (Upadhyay, 2020). La validité des données est plus étroitement liée à la manière dont elles sont créées et à leur origine qu'à la manière dont elles sont par la suite conservées (Lemieux, 2016). Ainsi, la saisie des données non exactes peut entraîner des

conséquences négatives dans les domaines sensibles comme la santé ou la chaîne de production et d'approvisionnement des produits médicaux.

De ce qui précède, il ressort que l'intégrité des données dans la chaîne de blocs dépend non seulement des caractéristiques de cette technologie, mais aussi du facteur humain étant donné que la chaîne de blocs ne garantit l'intégrité qu'aux données déjà stockées sur la chaîne de blocs (Zubaydi et al., 2019, Upadhyay, 2020).

Recommandation 13 : Les organisations gouvernementales qui adoptent la chaîne de blocs doivent s'assurer que les données saisies par les utilisateurs (oracles) sont valides, car la chaîne de blocs garantit l'intégrité à toute donnée, même invalide (non exact), qui y est stockée.

Les données qui entrent dans une chaîne de blocs subissent un certain nombre de traitements qui peuvent impacter négativement leurs validités[1] (voir Figure 1). La figure 1 montre que la violation de l'intégrité des données peut se produire lors du processus de leur création, de stockage ou lors de leur passage dans un oracle (qui est exposé à certains risques de sécurité). Ce qui justifie la pertinence d'une bonne gouvernance de la chaîne de blocs et une sensibilisation efficace des utilisateurs sur l'importance de la validité des données à introduire dans le registre de la chaîne de blocs (Tan et al., 2022).

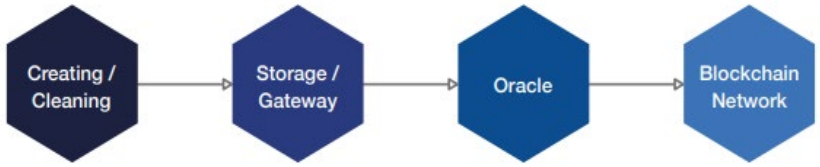

Figure 2. Traitement des données en amont de la chaîne de blocs[2]

[1] WEF Blockchain Toolkit (weforum.org)
[2] https://widgets.weforum.org/blockchain-toolkit/pdf/data-integrity.pdf

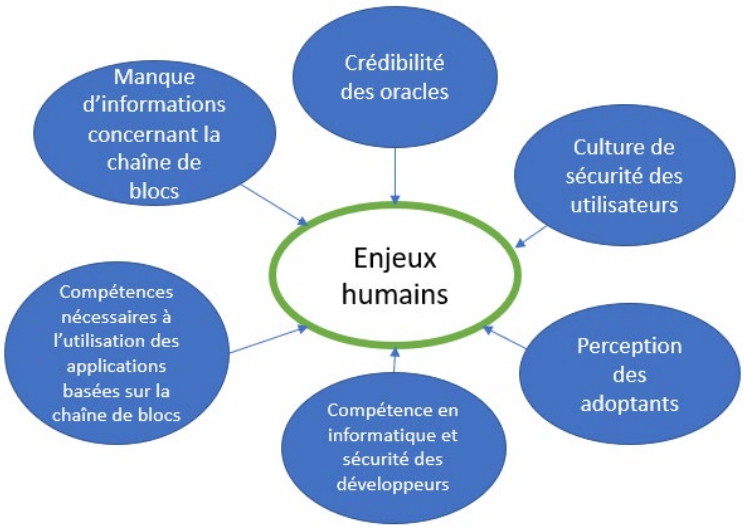

Figure 3. Enjeux humains d'implantation des applications basées sur la chaîne de blocs

Enjeux organisationnels d'implantation de la chaîne de blocs

En plus des approches techniques et humaines d'analyse des enjeux d'implantation de la chaîne de blocs, plusieurs auteurs ont mis l'accent sur l'approche organisationnelle d'analyse des enjeux d'implantation de la chaîne de blocs (Tan et al., 2022, Martin Primeau, 2018) (cf. figure 4). Dans leurs études, Tan et al. (2022) mentionnent la gouvernance de la chaîne de blocs et le consensus de l'industrie sur la pertinence d'utilisation de la chaîne de blocs comme enjeux majeurs de développement et d'utilisation des applications basées sur la chaîne de blocs. Pour Martin Primeau (2018), la complexité de la gouvernance de la chaîne de blocs repose sur la difficulté de gérer les accès aux données du registre et l'analyse des données qu'elle stocke. En effet, le but principal de la chaîne de blocs est de stocker les données et non pas de les analyser, et chaque fois qu'on consulte la chaîne de blocs, on ralentit la vitesse à laquelle les données sont analysées (Martin Primeau, 2018). Tan et al. (2022), quant à eux, définissent la gouvernance de la chaîne de blocs comme un ensemble des décisions prises dans le développement et l'utilisation des applications de cette technologie (Tan et al., 2022). Tan et al. (2022) ont identifié, un ensemble des décisions à prendre en compte dans la gouvernance des applications basées sur la chaîne de blocs dans le secteur public. Ces décisions concernent, entre autres, l'infrastructure de la chaîne de blocs, l'architecture de l'application, l'interopérabilité avec les systèmes existants, mécanismes de consensus et d'incitation des mineurs, l'organisation, la responsabilité et le contrôle de la gouvernance. Bien que la gouvernance de la chaîne de blocs soit un enjeu de taille dans l'implémentation de la chaîne de blocs dans tous les secteurs d'activités, plusieurs auteurs

mentionnent qu'elle est un défi important dans le secteur public (Meijer and Ubacht, 2018, Atzori, 2017).

Pour Tan et al. (2022), la gouvernance de la chaîne de blocs se situe à trois niveaux différents : **micro, meso et macro**. La gouvernance des applications basées sur la chaîne de blocs au niveau ***micro*** se concentre sur les choix du concepteur du système concernant l'infrastructure de la blockchain, la modularité et les normes de construction, de mise à niveau et d'adoption du système. L'unité d'analyse est individuelle et les types de décisions prises à ce niveau concernent l'architecture de la chaîne de blocs, l'architecture applicative et l'interopérabilité avec les systèmes existants (Tan et al., 2022). Au niveau micro de gouvernance, les adoptants de la chaîne de blocs doivent identifier les types de la chaîne de blocs qui peuvent être public, privé, avec permission ou sans permission. Ensuite, ils doivent justifier la pertinence de développer des contrats intelligents et d'autres applications décentralisées. Enfin, le besoin ou non d'interopérabilité de la chaîne de blocs avec les systèmes existants doit être clairement identifié (Tan et al., 2022). Ce défi d'intégration des applications de la chaîne de blocs avec les systèmes existants a été également soulevé par Mougayar (2016) qui s'intéresse à l'implémentation de la chaîne de blocs dans les chaînes d'approvisionnement. Cet auteur met en évidence la complexité de la mise en place de la chaîne de blocs dans les systèmes de chaîne d'approvisionnement existants, car ces systèmes sont difficiles à modifier et à adapter. De même, Islam et al. (2021) mentionnent que le changement des systèmes existants avec une nouvelle application basée sur la chaîne de blocs est un défi important pour les organisations en termes de coûts, la configuration de l'infrastructure, les perceptions des utilisateurs du nouveau système et des attentes de gestionnaires.

Le niveau ***meso*** de la gouvernance de la chaîne de blocs se concentre sur les processus organisationnels qui guident la prise de décision collective et des actions dans un réseau de la chaîne de blocs. Par conséquent, l'unité d'analyse est organisationnelle et les types de décisions prises à ce niveau concernent le mécanisme de prise de décision dans le réseau de la chaîne de blocs, d'incitation des mineurs et de consensus (Tan et al., 2022). De manière particulière, les décisions à ce niveau renvoient, entre autres, au type de stockage des données (on-chain/off-chain), les types de mécanismes d'incitation (recompasses liées à la participation du réseau) et des algorithmes de consensus à adopter pour la validation des données (PoW, PoS, DPoS, etc.). En plus de ces décisions techniques, il est important de mentionner un autre défi important à ce niveau auquel les adoptants de la chaîne de blocs doivent accorder plus d'attention qui est l'alignement entre la chaîne de blocs et les processus organisationnels de l'organisation (Nofer

et al., 2017). En effet, la chaîne de blocs est considérée comme une technologie perturbatrice, car elle est en mesure de modifier considérablement de nombreux modèles d'affaires existants et d'en créer de nouveaux avec des impacts significatifs (positifs et négatifs) sur l'ensemble des industries (Nofer et al., 2017). Pour Gaur (2020), l'adoption de la chaîne de blocs dans un secteur d'activités est un processus qui comprend plusieurs phases dont chacune fait face à certains défis, comme la réingénierie des processus d'affaires pour obtenir un alignement entre la technologie et les processus organisationnels.

Enfin, la gouvernance de la chaîne de blocs au niveau *macro* concerne les règles et normes institutionnelles qui découlent des fondements constitutionnels, culturels, historiques et juridiques (Tan et al., 2022). À ce niveau, l'organisation est l'unité d'analyse et les types de décisions prises à ce niveau concernent l'organisation de la gouvernance, les responsabilités de chaque participant du réseau dans la gouvernance et le contrôle de la gouvernance (Tan et al., 2022). Les défis dans ce niveau de gouvernance concernent, entre autres, la distribution des rôles dans la gouvernance de la chaîne de blocs, la règlementation et l'application des règles ainsi que la décision des processus organisationnels à placer sous le contrôle humain et ceux à automatiser (Tan et al., 2022). Les enjeux de la gouvernance au niveau macro exigent également la prise en compte d'un certain nombre de questions auxquelles les adoptants de la chaîne de blocs doivent apporter des solutions pour le succès de son implantation dans leur secteur d'activités. Il s'agit, entre autres, des questions en rapport avec les personnes qui auront accès à la chaîne de blocs, de l'entité qui décider d'ajouter les membres dans le réseau, de la personne susceptible de changer les protocoles de la chaîne de blocs (Educacation, 2021).

Recommandation 14 : La compréhension des éléments à gouverner et la manière de gouverner les applications basées sur la chaîne de blocs sont fondamentales pour le succès de leur implantation dans le contexte gouvernemental.

La gouvernance de la chaîne de blocs prend également compte des aspects liés aux défis juridiques et de performance dans le projet d'implantation des applications basées sur la chaîne de blocs (Zamani et al., 2020, White et al., 2020, Putz and Pernul, 2020, Gordon and Catalini, 2018). C'est l'exemple du caractère immuable de la chaîne de blocs qui empêche les applications basées sur cette technologie d'être en conformité avec les exigences du Règlement Général sur la Protection des Données (RGPD). Ce règlement donne le droit d'oubli à toute personne qui veut obtenir l'effacement de ses données personnelles stockées dans les systèmes informatiques (Subramanian et al., 2020).

Recommandation 15 : Les organisations gouvernementales devront adopter d'autres stratégies de stockage des données, à l'occurrence le stockage « off-Chain » qui consiste à stocker les données personnelles des individus dans leurs bases de données locales. Ensuite, n'utiliser la chaîne de blocs que pour sécuriser ces données à travers des mécanismes cryptographiques.

Le défi de l'incertitude règlementaire concernant l'utilisation de la chaîne de blocs constitue également l'une des grandes préoccupations des organisations publiques concernant l'adoption des applications basée sur cette technologie (Talapina, 2020). Pour Talapina (2020), un réaménagement des cadres règlementaire et juridique en faveur de la chaîne de blocs est nécessaire dans plusieurs pays pour faciliter la conformité juridique et règlementaire de cette technologie dans les organisations gouvernementales qui veulent l'adopter. Ainsi, la différence de cadre réglementaire et juridique entre les pays ne favorise pas l'adoption massive de la chaîne de blocs dans différents secteurs d'activités. De plus, la chaîne de blocs évolue rapidement que le cadre règlementaire qui l'encadre et ce cadre varie d'un pays à un autre (PwC France, 2012). Par exemple, les gouvernements chinois et coréens interdisent les projets de collecte de fonds sous forme de cryptomonnaies (Initial Coin Offering : ICO) pendant que ces projets sont autorisés dans d'autres pays (PwC France, 2012). Le défi de conformité règlementaire peut également être un enjeu majeur dans l'adoption de la chaîne de blocs pour les organisations gouvernementales des pays différents qui partagent d'informations, mais dont les règlementations concernant la chaîne de blocs sont différentes.

Un autre enjeu majeur d'implantation de la chaîne de blocs dans le secteur public est l'existence d'un conflit potentiel entre la chaîne de blocs et la protection des données personnelles (Manuel Badel, 2019). Plusieurs juridictions dans le monde adoptent aujourd'hui des règlements plus stricts en matière de protection des renseignements personnels. Par exemple, le règlement général sur la protection des données applicable au sein de l'Union européenne ou à l'actuelle révision de la loi sur la protection des renseignements personnels et les documents électroniques au Canada. Le resserrement de ces mesures réglementaires concerne les organisations qui collectent et stockent des données personnelles. C'est le cas des organisations gouvernementales qui ont besoin des données personnelles des citoyens pour traiter certaines de leurs demandes, comme l'établissement des documents officiels : passeports, permis de conduire, déclaration d'impôts, certificats de naissance ou de décès (Radanović and Likić, 2018, Dai, 2018).

Recommandation 16 : L'adoption de la chaîne de blocs par les organisations gouvernementales exige à ces dernières de développer des stratégies pour garantir la confidentialité des données dans la chaîne de blocs étant donné que les données sont transparentes dans le réseau.

En plus des considérations juridiques, la gouvernance de la chaîne de blocs encadre également le développement des applications basées sur cette technologie en proposant un ensemble de tests visant à se rassurer de la performance de ces applications en termes de sécurité et de fiabilité (Koteska et al. (2017). Koteska et al. (2017) précisent que le test des applications basées sur la chaîne de blocs doit prendre en considération plusieurs aspects de leur implémentation. Par exemple, un système basé sur une chaîne de blocs privée nécessite plus d'effort dans le test, car le faible nombre des nœuds dans le réseau rend le système plus vulnérable aux attaques de sécurité (Zheng et al., 2017). En plus du type de la chaîne de blocs, la nécessité de continuer à utiliser les anciens systèmes exige le recours aux tests d'intégration pour se rassurer de la performance du système basé sur la chaîne de blocs (Koteska et al., 2017). Ces deux types de tests (de sécurité et d'intégration) sont nécessaires lorsque la chaîne de blocs est utilisée dans un contexte gouvernemental. En effet, les organisations gouvernementales adoptent généralement les chaînes de blocs de type consortium qui comptent moins d'utilisateurs (Kim, 2021) et par conséquent vulnérables à certaines attaques de sécurité (attaque à 51% par exemple).

La garantie de la performance des systèmes basés sur la chaîne de blocs est une grande préoccupation des adoptants de cette technologie (Koteska et al., 2017). L'exigence de performance des applications basées sur la chaîne de blocs est nécessaire dans le contexte gouvernemental pour garantir la qualité des services offerts aux citoyens (Berryhill et al., 2018). Ceci a conduit plusieurs auteurs à proposer un processus de test des systèmes basés sur la chaîne de blocs (Koteska et al., 2017, Zheng et al., 2018). Zheng et al. (2018) mentionnent que certains développeurs des systèmes basés sur la chaîne de blocs sont tentés de falsifier les performances de leurs systèmes pour attirer des investisseurs motivés par les avantages reconnus de la chaîne de blocs. En outre, lorsque les utilisateurs souhaitent combiner la chaîne de blocs dans les affaires, ils doivent savoir quelle chaîne de blocs correspond à leurs besoins. Un mécanisme de test de la chaîne de blocs doit donc être mis en place pour tester différents systèmes basés sur la chaîne de blocs afin d'être sûrs de leurs performances (Zheng et al., 2018).

Les tests de la chaîne de blocs sont séparés en deux phases : la phase de normalisation et la phase de test (Koteska et al., 2017). Dans la phase de normalisation, tous les critères de performance doivent être définis et acceptés. Lorsqu'une chaîne de blocs est créée, elle pourrait être testée

avec les critères convenus pour valider si elle fonctionne correctement comme le prétendent les développeurs. En ce qui concerne la phase de test, les tests de la chaîne de blocs doivent être effectués avec différents critères. Par exemple, un utilisateur responsable d'une entreprise de vente au détail en ligne se soucie du débit et de la capacité de stockage de la chaîne de blocs, de sorte que l'examen doit tester le temps moyen entre l'envoi d'une transaction par un utilisateur et l'enregistrement de ladite transaction dans le registre de la chaîne de blocs ainsi que de la capacité d'un bloc de la chaîne de blocs.

Recommandation 17 : Les organisations doivent veiller à la performance des applications basées sur la chaîne de blocs en procédant aux tests de sécurité et de fiabilité ainsi que ceux d'intégration de ces applications avec les systèmes existants.

Un autre enjeu organisationnel d'implantation de la chaîne de blocs est le manque de consensus de l'industrie sur la pertinence d'utilisation de cette technologie (Educacation, 2021). Ce manque de consensus se justifie par le faible niveau d'exploitation de la chaîne de blocs dans une industrie et constitue une barrière à certains partenariats au sein cette industrie. Par exemple, une adoption généralisée de la chaîne de blocs dans le secteur public permettrait à plusieurs organisations gouvernementales de créer des partenariats pour l'échange des données dans le but d'améliorer les services offerts aux citoyens. Le défi lié à l'impact environnemental d'exploitation à grande échelle de la chaîne de blocs est également à prendre en compte dans l'analyse des enjeux organisationnel d'implantation de cette technologie (Educacation, 2021). En effet, les opérations de vérification, de validation et de cryptographie sont très consommatrices en électricité et une large expansion des applications basées sur la chaîne de blocs pourrait alors avoir un impact négatif sur l'environnement (Futura, 2021, Bamakan et al., 2020).

Recommandation 18 : Les organisations gouvernementales devraient privilégier l'utilisation des chaînes de blocs qui respectent les exigences écologiques et environnementales en faisant recours, par exemple, aux chaînes de blocs qui implémentent l'algorithme PoS ou aux chaînes de blocs de troisième génération.

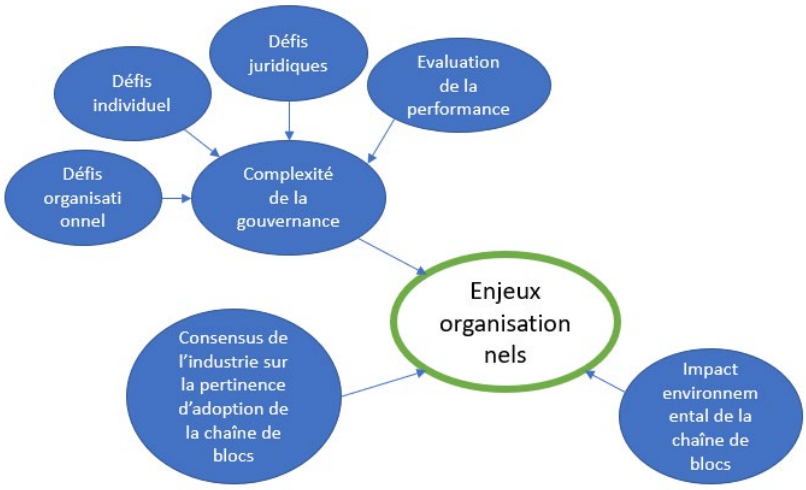

Figure 4. Enjeux organisationnels d'implantation des applications basées sur la chaîne de blocs

Pour terminer, nous présentons dans la figure 5 un récapitulatif des enjeux d'implantation des applications basées sur la chaîne de blocs dans un contexte gouvernemental.

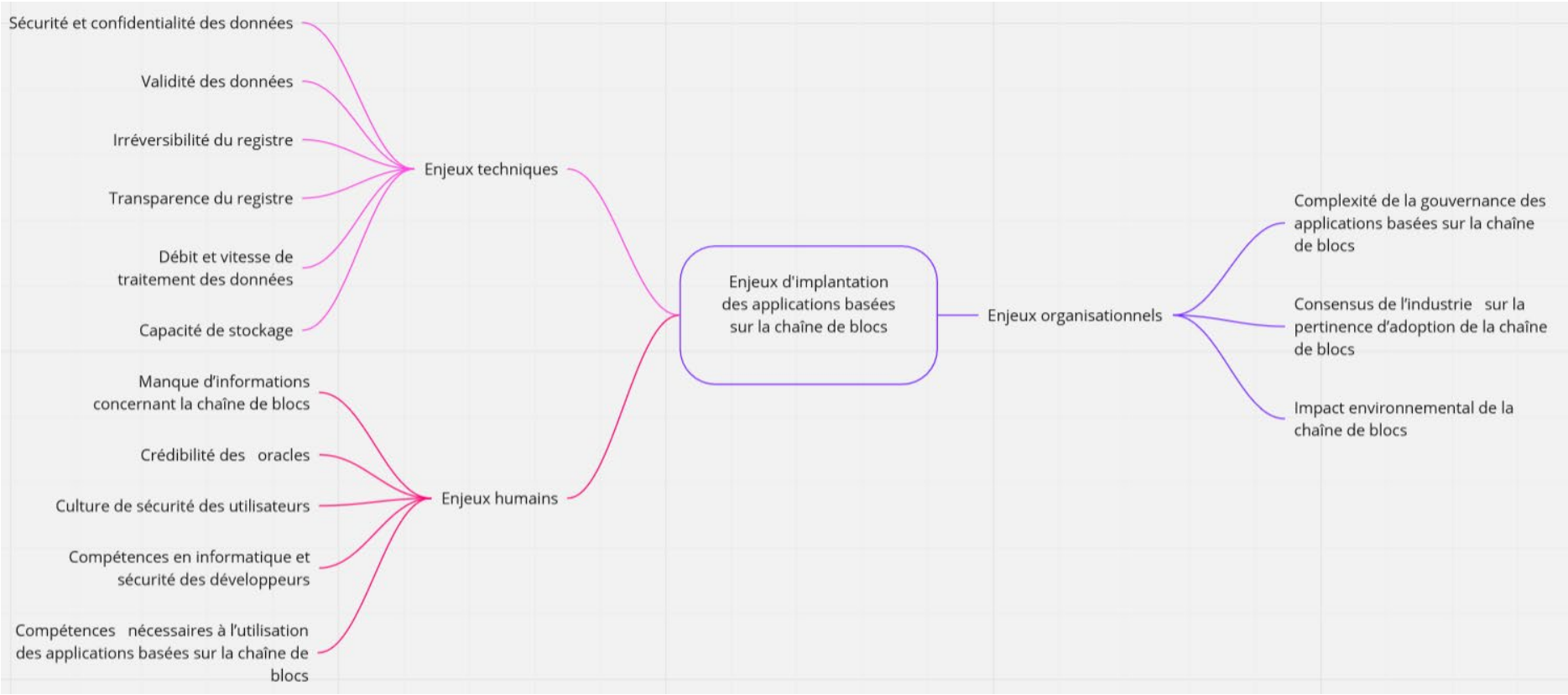

Figure 5. Récapitulatif des enjeux d'implantation des applications basées sur la chaîne de blocs

Références

Atzori, M. (2017) Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation,* **6** (1)**,** 45-62.

Bamakan, S. M. H., Motavali, A. & Babaei Bondarti, A. (2020) A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications,* **154,** 113385.

Berryhill, J., Bourgery, T. & Hanson, A. (2018) Blockchains Unchained:Blockchains Unchained : Blockchain Technology and its Use in the Public Sector *Documents de travail de l'OCDE sur la gouvernance publique.* Paris, OCDE.

Clohessy, T. & Acton, T. (2019) Investigating the influence of organizational factors on blockchain adoption An innovation theory perspective. *Industrial Management & Data Systems,* **119** (7)**,** 1457-1491.

Dai, H.-N. (2018) Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.,* **14** (4)**,** 352–375.

Daraghmi, E. Y., Daraghmi, Y. A. & Yuan, S. M. (2019) MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access,* **7,** 164595-164613.

Educacation, E. P. E. (2021) *Quels sont les principaux enjeux de la blockchain ?* (accessed 28/08/2022 2022).

Futura. (2021) *Quelles sont les trois générations des cryptomonnaies ?* . (accessed.

Gaur, N. (2020) Blockchain challenges in adoption. *Managerial Finance,* **6** (6)**,** 849-858.

Gordon, W. J. & Catalini, C. (2018) Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal,* **16,** 224-230.

Hao, K., Xin, J. C., Wang, Z. Q., Cao, K. Y. & Wang, G. R. (2019) Blockchain-Based Outsourced Storage Schema in Untrusted Environment. *IEEE Access,* **7,** 122707-122721.

Hao, K., Xin, J. C., Wang, Z. Q. & Wang, G. R. (2020) Outsourced data integrity verification based on blockchain in untrusted environment. *WORLD WIDE WEB-INTERNET AND WEB INFORMATION SYSTEMS,* **23** (4)**,** 2215-2238.

Hasanova, H., Baek, U.-j., Shin, M.-g., Cho, K. & Kim, M.-S. (2019) A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT,* **29** (2).

Hylock, R. H. & Zeng, X. M. (2019) A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. *Journal of Medical Internet Research,* **21** (8).

Iredale, G. (2021) Top 10 Blockchain Adoption Challenges. IN 101 Blockchains (Ed.

Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S. & Embong, A. H. (2021) A Review on Blockchain Security Issues and Challenges. *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC).*

Joëlle Toledano (2018) Les enjeux des blockchains. Paris, France stratégie.

Kim, Y. R. (2021) Blockchain Initiatives for Tax Administration. *SSRN Electronic Journal.*

Koteska, B., Karafiloski, E. & Mishev, A. (2017) Blockchain Implementation Quality Challenges: A Literature Review. *SQAMIA.*

Lafourcade, P. & Lombard-Platet, M. (2020) About blockchain interoperability. *Information Processing Letters,* **161** (2020)**,** 105976.

Lemieux, V. L. (2016) Trusting records: is Blockchain technology the answer? *Records Management Journal,* **26** (2)**,** 110-139.

Manuel Badel (2019) La chaîne de blocs et l'industrie canadienne des médias. IN Canada, T. (Ed. HEC Montréal.

Martin Primeau (2018) La difficile implantation des chaînes de blocs. *La presse,*.

Meijer, D. & Ubacht, J. (2018) The governance of blockchain systems from an institutional perspective, a matter of trust or control? *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age.* Delft, The Netherlands, Association for Computing Machinery.

Meinert, E., Alturkistani, A., Foley, K. A., Osama, T., Car, J., Majeed, A., Van Velthoven, M., Wells, G. & Brindley, D. (2019) Blockchain Implementation in Health Care: Protocol for a Systematic Review. *JMIR Res Protoc,* **8** (2)**,** e10994.

Mendling, J., Weber, I., Aalst, W., Brocke, J. v., Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., García-Bañuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M. & Zhu, L. (2018) Blockchains for Business Process Management - Challenges and Opportunities. *ACM Transactions on Management Information Systems,* **. In press, accepted**.

MIGNON, V. (2019) *La blockchain : quels enjeux, défis et conséquences ?* Centre des Professions Financières, Université Paris Nanterre. Available https://medium.com/@professionsfinancieres/la-blockchain-quels-enjeux-d%C3%A9fis-et-cons%C3%A9quences-62defa10bad9. (accessed 27/08/2022.

Mougayar, W. (2016) *The Business Blockchain: Promise, Practice, and Application of Next Internet Technology*. Wiley.

Nofer, M., Gomber, P., Hinz, O. & Schiereck, D. (2017) Blockchain. *Business & Information Systems Engineering,* **59** (3)**,** 183-187.

Putz, B. & Pernul, G. (2020) Detecting Blockchain Security Threats. *2020 IEEE International Conference on Blockchain (Blockchain).*

PwC France. (2012) *Décoder la blockchain et ses enjeux*. France. Available https://www.pwc.fr/fr/vos-enjeux/blockchain/decoder-la-blockchain-et-ses-enjeux.html. (accessed 28/08/2022 2022).

Radanović, I. & Likić, R. (2018) Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy,* **16** (5)**,** 583-590.

Subramanian, H. C., Cousins, K. C., Bouayad, L., Sheth, A., Conway, D., Salcedo, E. & Pineda, J. (2020) Blockchain Regulations and Decentralized Applications: Panel Report from AMCIS 2018. *Communications of the Association for Information Systems,* **47,** 189-206.

Talapina, E. (2020) APPLICATION OF BLOCKCHAIN IN PUBLIC ADMINISTRATION: PROSPECTS FOR LEGAL REGULATION. *Voprosy Gosudarstvennogo I Munitsipalnogo Upravleniya-Public Administration Issues,* (3)**,** 96-113.

Tan, E., Mahula, S. & Crompvoets, J. (2022) Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly,* **39** (1)**,** 101625.

Upadhyay, N. (2020) Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management,* **54,** N.PAG-N.PAG.

White, B. S., King, C. G. & Holladay, J. (2020) Blockchain security risk assessment and the auditor. *Journal of Corporate Accounting & Finance,* **31** (2)**,** 47-53.

Zamani, E., He, Y. & Phillips, M. (2020) On the Security Risks of the Blockchain. *Journal of Computer Information Systems,* **60** (6)**,** 495-506.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. (2018) Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services,* **14** (4)**,** 352-375.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017) An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE international congress on big data (BigData congress).* IEEE.

Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M. & Karuppayah, S. (2019) A Review on the Role of Blockchain Technology in the Healthcare Domain. *Electronics,* **8** (6).