Chaire de recherche sur les contrats intelligents et la chaîne de blocs
Chambre des notaires du Québec

Fondements de la chaîne de blocs et son adéquation pour le secteur public

Wilfried Bazomanza Nzabandora[1]; Martin Tchoukoua[1]

[1] *Chaire de recherche sur les contrats intelligents et la chaîne de blocs, Université Laval, Québec, Canada*

Introduction

La chaîne de blocs est de plus en plus utilisée dans différents secteurs d'activités pour garantir la sécurité des données et des transactions (Rana et al. 2022). Parmi les secteurs d'activités qui exploitent la chaîne de blocs, le secteur gouvernemental occupe une place importante (Tan et al. 2022). Ce secteur utilise la chaîne de blocs, entre autres, dans la gestion des données de santé, le vote électronique ou l'éducation (Tan et al. 2022). Le présent tableau vise à mieux comprendre les cas d'utilisation dans le secteur gouvernemental.

Objectifs

1. Présenter les aspects fondamentaux de la technologie de la chaîne de blocs;
2. Discuter de l'adéquation de la chaîne de blocs avec le contexte gouvernemental;
3. Présenter les domaines d'application de la chaîne de blocs dans un contexte gouvernemental.

Méthodologie

Identification des concepts clés → **Recherche de la littérature** → **Sélection de la littérature pertinente** → **Analyse de la littérature sélectionnée**

Résultats

Aspects fondamentaux de la chaîne de blocs

Définition	Caractéristiques	Générations	Types	Concepts associés
Grand livre public dont toutes les transactions validées sont stockées dans une liste de blocs (Zheng et al., 2017).	Décentralisation, immuabilité, échange des données pair-à-pair, anonymat et transparence (Zheng et al., 2017).	Chaîne de blocs 1.0; Chaîne de blocs 2.0; Chaîne de blocs 3.0 et chaîne de blocs 4.0 (Angelis and Ribeiro da Silva, 2019).	Privé, publique et consortium (Zahed Benisi et al., 2020).	Contrats intelligents, algorithmes de consensus, applications décentralisées, portefeuille numérique de cryptomonnaie et tokenisation

Domaines d'application de la chaîne de blocs dans le contexte gouvernemental

Foncier	Éducation	Chaîne d'approvisionnement	Finance	Santé	Vote
Enregistrement de registre foncier (Bhatia & Wright de Hernandez, 2019)	Authentification des certificats académiques, (Alammary et al., 2019)	Traçabilité des produits sur la base d'informations fiables (S. S. Kamble et al.,2021)	Permettre l'inclusion financière (Schuetz & Venkatesh, 2020)	Gestion des dossiers de santé électroniques (Peterson et al., 2016)	Garantie de la transparence, la confidentialité et la sécurité des votes (Taş & Tanrıöver, 2020).

Adéquation de la chaîne de blocs avec le contexte gouvernemental

Modèle de e-administration traditionnel	Modèle de e-administration basé sur la blockchain
Systèmes hypercentralisés (Kassen, 2022)	Systèmes décentralisés (S. Khan et al. ;2022)
Systèmes vulnérables aux cyberattaques (Elisa et al.,2018)	Intégrité des transactions et des données (Warkentin & Orgeron, 2020)
Mauvaise gestion des actifs et des identités numériques des citoyens (Alammary et al.,2019)	Gestion efficace des identités des citoyens dans les services publics (Clavin et al. ;2020)
Difficultés d'accès et de partage des données (Alammary et al.,2019)	Absence du point de défaillance unique (Cagigas et al. ; 2021)
Risque élevé de perte d'intégrité des données (Berryhill et al.,2018)	Transparence, accessibilité aux données gouvernementales (Mora et al. ;2021)
	Efficacité de la prise de décision fondée sur des données probantes (Cagigas et al. ;2021)

Conclusion

- L'intérêt de la chaîne de blocs est perceptible dans plusieurs secteurs d'activités
- Les caractéristiques de la chaîne de blocs justifient la sécurité qu'elle offre concernant la gestion des données et/ou des transactions;
- A travers les contrats intelligents, l'utilisation de cette technologie se généralise au delà du domaine financier;
- Les différents cas d'utilisation de cette technologie montrent l'intérêt des praticiens envers cette technologie;
- Le secteur public exploite la chaîne de blocs pour la sécurité des données des citoyens et l'optimisation des services publics;
- L'adoption de la chaîne de blocs comprend un certain nombre de défis que les adoptants doivent prendre en compte dans le processus de son adoption.

Remerciements

Cette recherche a été rendue possible grâce au projet de recherche réalisé entre l'Université Laval, Revenu Québec et le Ministère de la cybersécurité et du numérique.

Références

Alammary, A., Alhazmi, S., Almasri, M., and Gillani, S. 2019. "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences (9:12), p. 2400.
Angelis, J., and Ribeiro da Silva, E. 2019. "Blockchain Adoption: A Value Driver Perspective," Business Horizons (62:3), pp. 307-314.
Bhatia, S., and Wright de Hernandez, A. 2019. "Blockchain Is Already Here. What Does That Mean for Records Management and Archives?," Journal of Archival Organization (16:1), pp. 75-84.
Cagigas, D., Clifton, J., Diaz-Fuentes, D., and Fernández-Gutiérrez, M. 2021. "Blockchain for Public Services: A Systematic Literature Review," IEEE Access (9:2021), pp. 13904-13921.
Elisa, N., Yang, L., Chao, F., and Cao, Y. 2018. "A Framework of Blockchain-Based Secure and Privacy-Preserving E-Government System," Wireless networks (29:2023), pp. 1005–1015.
Kamble, S. S., Gunasekaran, A., Subramanian, N., Ghadge, A., Belhadi, A., and Venkatesh, M. 2021. "Blockchain Technology's Impact on Supply Chain Integration and Sustainable Supply Chain Performance: Evidence from the Automotive Industry," Annals of Operations Research), pp. 1-26.
Kassen, M. 2022. "Blockchain and E-Government Innovation: Automation of Public Information Processes," Information Systems (103:2022), pp. 1-11.
Tan, E., Mahula, S., and Crompvoets, J. 2022. "Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management," Government Information Quarterly (39:1), p. 101625.
Taş, R., and Tanrıöver, Ö. Ö. 2020. "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," Symmetry (12:8), pp. 1-24.
Warkentin, M., and Orgeron, C. 2020. "Using the Security Triad to Assess Blockchain Technology in Public Sector Applications," International Journal of Information Management (52:2020), pp. 1-8.
Zahed Benisi, N., Aminian, M., and Javadi, B. 2020. "Blockchain-Based Decentralized Storage Networks: A Survey," Journal of Network and Computer Applications (162), p. 102656.
Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. 2017. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564.

Chaire de recherche sur les contrats intelligents et la chaîne de blocs
Chambre des notaires du Québec

Cas d'utilisation de la chaîne de blocs dans un contexte gouvernemental et Enjeux d'implantation

Wilfried Bazomanza Nzabandora[1]; Martin Tchoukoua[1]

[1] *Chaire de recherche sur les contrats intelligents et la chaîne de blocs, Université Laval, Québec, Canada*

Introduction

L'utilisation de la chaîne de blocs (CB) dans les gouvernements est motivée par le besoin de sécuriser les données des citoyens et d'optimiser par les processus publics (Tan et al., 2022). À travers cette optimisation, les organisations réduisent considérablement la fraude, le gaspillage des ressources et des abus associés, généralement, aux systèmes centralisés. L'utilisation d'un modèle de gouvernance basé sur la CB permet aux utilisateurs des services gouvernementaux et aux gouvernements entre eux de mieux partager les ressources sur un registre décentralisé et sécurisé par la cryptographie (Tan et al., 2022). Cependant, l'implémentation de la CB dans le contexte gouvernemental comprend des défis auxquels les organisations gouvernementales doivent apporter des solutions pour assurer le succès de son implantation(Zheng et al. 2018).

Objectifs

1. Présenter les cas d'utilisation de la CB dans le contexte gouvernemental;
2. Présenter les défis d'implantation de la CB dans le contexte gouvernemental;

Méthodologie

Identification des concepts clés → **Recherche de la littérature** → **Sélection de la littérature pertinente** → **Analyse de la littérature sélectionnée**

Résultats

Cas types d'utilisation de la chaîne de blocs

Vote
Confidentialité, authentification du vote et transparence du processus électoral (**Royaume-Uni, Estonie, Finlande, USA**)

Gestion des actifs
Gestion sécurisée des transactions immobilières (**Ghana, Géorgie, Pays-Bas, Suède, Suisse, Dubaï**)

Énergie
Décentralisation, échange pair-à-pair de l'énergie (**Allemagne, Royaume-Uni et New York**)

Éducation:
Contrefaçon, authenticité des documents universitaires (**France**)

Surveillance et sécurité
Intégrité des données des dispositifs frontaliers, contrôle des identités des voyageurs, sécurité dans les chaînes d'approvisionnement (**USA, Canada**)

Télécommunication:
traçabilité et autorégulation des bandes de fréquences (**USA**)

Identité numérique
Améliorer l'identification et l'accès aux services publics (**Estonie, USA, Canada**)

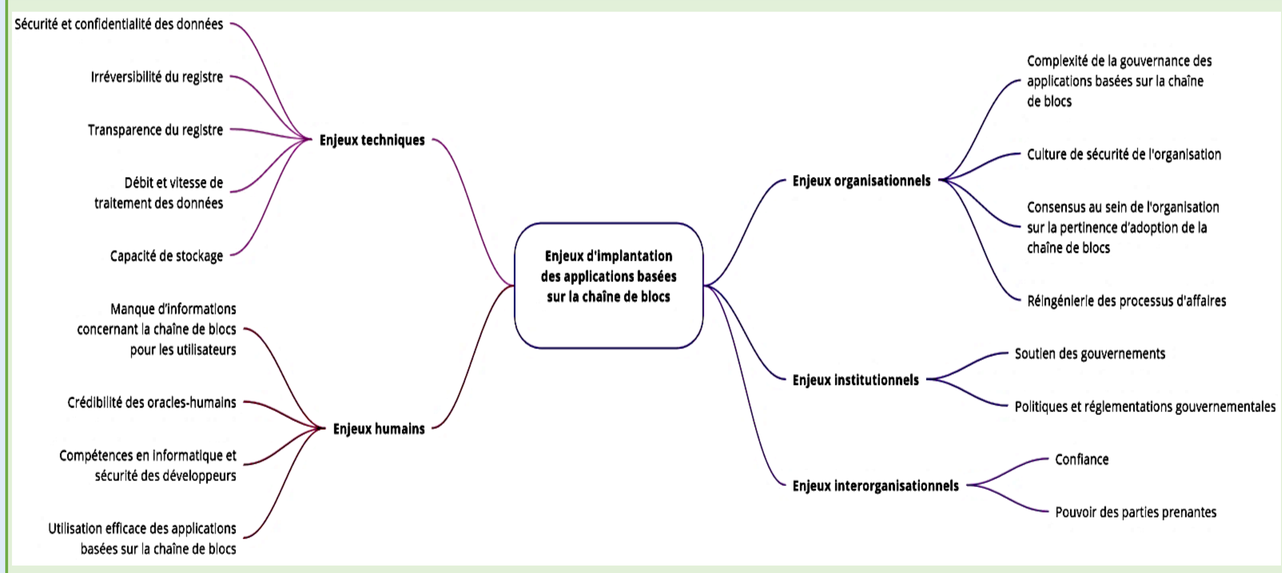
Identité agroalimentaire:
Amélioration de la traçabilité, de l'efficacité et la transparence (**Estonie, Suisse**)

Dossiers de santé:
Sécurisation des dossiers médicaux des patients, transparence des services de santé (**USA**)

Impôts: Transparence, asymétrie d'information, collecte des taxes (**USA**)

Santé publique:
Suivie des crises, optimisation du développement des médicaments, orientation des politiques publiques (**Chine**)

Enjeux d'implantation de la chaîne de blocs



Recommandations aux organisations

- Mettre en place des stratégies pour lutter contre les attaques à 51%.
- S'assurer de la correction des codes des applications basées sur la chaîne de blocs
- Identifier les données hautement sensibles à stocker sur-chaîne et les moins sensibles hors-chaîne
- 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.
- Tenir compte des capacités de traitement des données des chaînes de blocs que les organisations souhaitent adopter en fonction de la vitesse de traitement de leurs données.
- Recourir aux applications basées sur la chaîne de blocs disponibles dans le cloud computing lorsque l'organisation ne dispose pas de l'infrastructure requise.
- Choisir des solutions interopérables qui sont basées sur la chaîne de blocs.
- Adopter une approche graduelle d'implantation de la chaîne de blocs
- Instaurer une culture de sécurité pour éviter certains risques de sécurité qui pourraient provenir de la mauvaise utilisation des applications basées sur la chaîne de blocs.
- S'assurer que les données saisies par les utilisateurs sont valides,
- Veiller à la performance des applications basées sur la chaîne de blocs (Tests de sécurité, de fiabilité et d'intégration avec les systèmes existants)
- Privilégier l'utilisation des chaînes de blocs écologiques et environnementales.

Conclusion

- Le secteur public utilise de plus en plus la CB pour la sécurité des données et l'optimisation des services publics
- L'implémentation des applications basées sur la CB comprend des défis
- Quatre types de défis: techniques, humains, organisationnels et inter organisationnels
- La mauvaise gestion de ces défis conduit à l'échec des projets d'implantation de la CB
- Nécessité de développer des stratégies pour surmonter les défis liés à l'implantation de la CB et assurer le succès de leur implantation

Remerciements

Cette recherche a été rendue possible grâce au projet de recherche réalisé entre l'Université Laval, Revenu Québec et le Ministère de la cybersécurité et du numérique.

Références

Tan, E., Mahula, S., and Crompvoets, J. 2022. "Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management," Government Information Quarterly (39:1), p. 101625.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. 2018. "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services (14:4), pp. 352-375.

Université Laval | Chaire de recherche sur les contrats intelligents et la chaîne de blocs
Chambre des notaires du Québec

Revenu Québec

Gouvernance de la chaîne de blocs et enjeux techniques avec les systèmes existants

Wilfried Bazomanza Nzabandora[1]; Martin Tchoukoua[1]

[1] *Chaire de recherche sur les contrats intelligents et la chaîne de blocs, Université Laval, Québec, Canada*

Introduction

Bien que les applications basées sur la chaîne de blocs (CB) soient des systèmes destinés à fonctionner de manière autonome, elles peuvent néanmoins nécessiter une intervention humaine (Dursun & Üstündağ, 2021). Les raisons de cette intervention se justifient par le besoin d'assurer un bon fonctionnement de ces applications, à travers des modèles de gouvernance. Cette dernière fait référence à l'ensemble des processus et des règles adoptées sur la plate-forme de la CB qui régissent son fonctionnement (Dursun & Üstündağ, 2021). En plus de la gouvernance, les applications basées sur la CB comprennent également des défis techniques de sécurité et d'intégration avec les systèmes existants (Homoliak et al., 2021;Janssen et al., 2020).

Objectifs

1. Présenter les modèles et les défis de gouvernance des applications basées sur la CB
2. Présenter les défis de sécurité des applications basées sur la CB;
3. Présenter les défis techniques de la CB avec les systèmes existants.

Méthodologie

Identification des concepts clés → Recherche de la littérature → Sélection de la littérature pertinente → Analyse de la littérature sélectionnée

Résultats

Gouvernance de la chaîne de blocs

➢ **Gouvernance sur-chaîne** (Reijers et al., 2021).

- Règles et processus décisionnels encodés directement dans l'infrastructure sous-jacente d'une application basée sur la chaîne de blocs

➢ **Gouvernance hors-chaîne** (Dursun & Üstündağ, 2021)

- Processus de décision basé sur des interactions humaines pour obtenir un consensus (Similaire aux structures de gouvernance sociale traditionnelles)

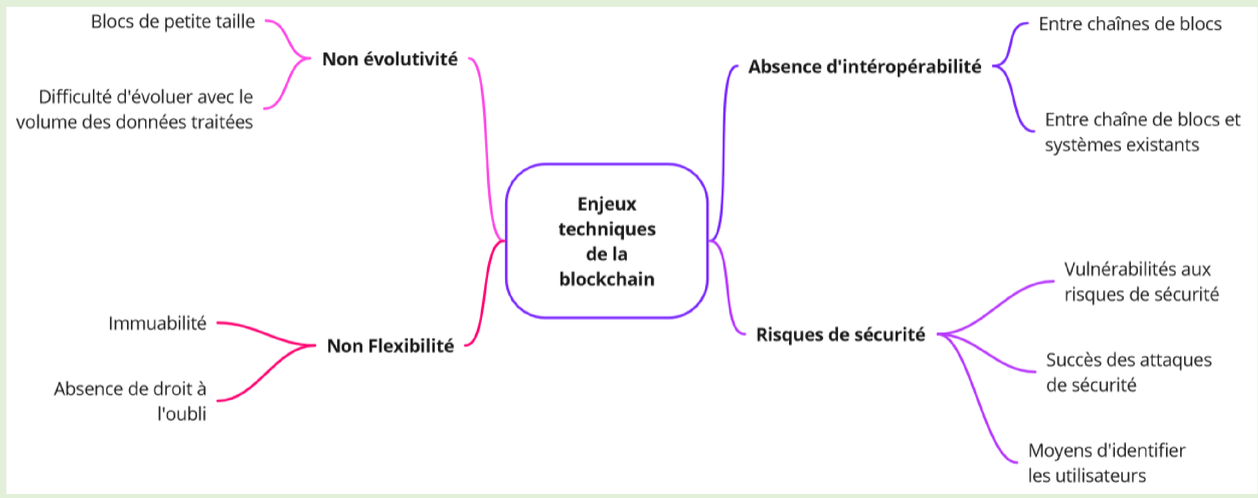
➢ **Défis de gouvernance** (Schmeiss et al., 2019)

- Défis analysés sur dix facteurs :
  - Consensus des parties prenantes, sécurité de la gouvernance, risque de centralisation, équité, mauvais alignement des incitations, efficacité, complexité, flexibilité de la gouvernance, réponse lente dans les cas problématiques et dépendances inter-propositions

➢ **Considérations de sécurité** (Homoliak et al. 2021)

- Facteurs de risques :
  - Technologie: Couches de la CB et ses caractéristiques
  - Humains: Développeurs et utilisateurs
  - Oracles

Enjeux d'implantation de la chaîne de blocs



Recommandations aux organisations

Gouvernance

➢Gouvernance hors-chaîne est beaucoup plus utile pour les réseaux qui ont tendance à prendre moins de décisions
➢Gouvernance sur-chaîne réduit le fork dans un réseau chaîne de blocs
➢Règles de gouvernance doivent atteindre les intérêts divergents des membres pour favoriser un taux de participation élevé (sécurité)
➢ Règles de gouvernance doivent réduire au maximum la vulnérabilité des applications basées sur la chaîne de blocs aux risques de sécurité.
➢Améliorer la compréhension de la chaîne de blocs par les adoptants pour augmenter leur intérêt à participer au processus de décision sur les règles du protocole.
➢Gouvernance de la chaîne de blocs doit être dynamique

Enjeux technique d'implantation

➢Normes d'interopérabilité doivent d'abord être soutenues par une grande communauté open source basée sur un « middelware » sécurisé.
➢Normes doivent être prises en charge par la plupart des réseaux de chaîne de blocs et de systèmes existants à l'échelle mondiale.
➢Intégration des normes dans les protocoles pour l'intégrité des données.
➢Intégration dans les normes d'un «middelware» généralisé susceptibles d'améliorer la sécurité et la performance des systèmes basés sur la chaîne de blocs
➢Optimisation des stockages à partir des opérations de transactions hors chaîne
➢Refonte de la chaîne de blocs pour des fins d'évolutivité

Conclusion

Les organisations qui souhaitent adopter la chaîne de blocs doivent procéder au préalable à une bonne compréhension de cette technologie en ce qui concerne, dans un premier temps, ses différents modèles de gouvernance et ses vulnérabilités aux attaques de sécurité. Dans un deuxième temps, elles doivent définir des stratégies pour surmonter les défis techniques liés à l'implantation de cette technologie, comme l'interopérabilité avec les systèmes existants ou l'évolutivité de la technologie. Le choix d'un modèle de gouvernance qui est adapté à une application basés sur la chaîne de blocs réduit au maximum les attaques de sécurité contre ces applications.

Remerciements

Cette recherche a été rendue possible grâce au projet de recherche réalisé entre l'Université Laval, Revenu Québec et le Ministère de la cybersécurité et du numérique.

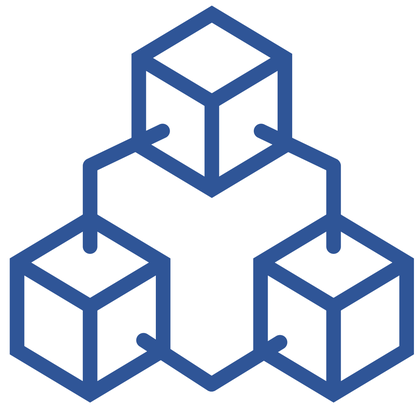
Références

Dursun, T., and Üstündağ, B. B. 2021. "A Novel Framework for Policy Based on-Chain Governance of Blockchain Networks," Information Processing & Management (58:4), p. 1.
Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., and Szalachowski, P. 2021. "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses," IEEE Communications Surveys & Tutorials (23:1), pp. 341-390.
Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., and Irani, Z. 2020. "A Framework for Analysing Blockchain Technology Adoption: Integrating Institutional, Market and Technical Factors," International Journal of Information Management (50), pp. 302-309.
Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Cubillos Vélez, A., and Orgad, L. 2021. "Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies," Topoi (40:4), pp. 821-831.
Schmeiss, J., Hoelzle, K., and Tech Robin, P. G. 2019. "Designing Governance Mechanisms in Platform Ecosystems: Addressing the Paradox of Openness through Blockchain Technology," California Management Review (62:1), pp. 121-143.

LA CHAÎNE DE BLOCS AU REGARD DU RESPECT DE LA CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS AU SEIN DE REVENU QUÉBEC ET DE SES PARTENAIRES INSTITUTIONNELS

Joey Blais, Thania Vallières-Racine et Vincent Morin

Chaire de recherche sur les contrats intelligents et la chaîne de blocs



INTRODUCTION

- L'implantation de la technologie de chaîne de blocs par les organismes publics a le potentiel de révolutionner la manière dont s'effectue la collaboration entre le secteur privé et les entités gouvernementales. Les organismes souhaitant intégrer la technologie de la chaîne de blocs au sein de leur organisation doivent s'assurer de la **conformité de leur projet avec le cadre règlementaire et législatif** des organismes publics portant sur la **gestion et la confidentialité des données et des renseignements personnels.**

OBJECTIFS

1. Identifier les **ENJEUX sur l'environnement légal et législatif** lors de l'adoption d'une chaîne de blocs par un organisme public
2. Identifier l'**IMPACT** d'une pareille adoption sur la **sécurité et la confidentialité des données** et la **gestion des renseignements personnels.**

MÉTHODES

1. **Identification des concepts clés**
2. **Identification des lois applicables au cas étudié**
3. **Recherche dans la littérature scientifique**
4. **Analyse de la littérature pertinente**
5. **Application de l'analyse aux ententes interinstitutionnelles particulières présentées par revenu Québec**

RÉSULTATS ET DISCUSSIONS

- Un organisme public souhaitant utiliser la technologie de la chaîne de blocs pour collecter et stocker les données et les renseignements personnels des citoyens du Québec devra identifier la **NATURE** de ces renseignements soit:
  1. renseignements **personnels**;
  2. renseignements **personnels sensibles;**
  3. renseignements **dépersonnalisés**;
  4. renseignements **anonymisés**.
- Les organismes publics devront respecter les **normes légales applicables à la collecte** de ces différents types de renseignements.

➢ **Exemple fictif de dépersonnalisation et d'anonymisation des données**

Répartition des participants de l'étude selon leur intention de vote			
RENSEIGNEMENTS DÉPERSONNALISÉS		**RENSEIGNEMENTS ANONYMISÉS**	
Code utilisateur	**Parti politique**	**Participant**	**Parti politique**
5MJ609	Parti mauve	A	Parti mauve
9HG198	Parti brun	B	Parti brun
7KD032	Parti mauve	C	Parti mauve
6MN569	Ne sait pas	D	Ne sait pas
3TH678	Parti jaune	E	Parti jaune

- **L'adoption d'une technologie de chaîne de blocs publique par revenu Québec et un partenaire institutionnel contreviendrait aux obligations des organismes publics en matière de sécurité et de confidentialité des données.** L'inscription d'un renseignement au registre distribué d'une chaîne de blocs publique aurait pour effet de publiciser cette donnée à l'ensemble du réseau, représentant une faille béante de sécurité (voire l'absence de sécurité) du système en matière de protection des renseignements personnels.
- Qu'elle soit publique ou privée, une chaîne de blocs peut **constituer un obstacle important au respect des exigences des organismes publics relatives à la destruction des données** puisqu'il est impossible de supprimer définitivement une entrée dans son registre. Cette entrée peut constituer un renseignement au regard de la *Loi*.
- L'anonymisation est une alternative à la destruction des données, rendu impossible par le registre immuable (art 73 *Loi sur l'accès*). Cependant, **nous croyons plutôt que la chaîne de blocs, dont le fonctionnement repose sur l'utilisation de clefs personnelles appartenant à chaque utilisateur, ne permet que l'atteinte d'un renseignement personnel dépersonnalisé.**

CONCLUSION

- Il ne faut pas envisager **la technologie de la chaîne de blocs** comme une cassure et un remplacement intégral du système préexistant, mais plutôt comme un **outil complémentaire** permettant d'effectuer des **gains en efficience et faciliter le traitement de certaines données** par l'administration publique.
- Cela étant dit, les **législations québécoise et canadienne** actuelles portant sur les enjeux de gestion et de confidentialité des données semblent **INADAPTÉES à la technologie de la chaîne de blocs.**
- Le recours de la chaîne de blocs par des organismes publics présente donc **des difficultés pratiques et techniques parfois INSURMONTABLES** quant au respect de leurs **obligations légales** en matière de SÉCURITÉ et de CONFIDENTIALITÉ des renseignements personnels.

REMERCIEMENTS

Cette recherche a été rendue possible grâce au projet de recherche réalisé entre l'Université Laval et revenu Québec

RÉFÉRENCES

Code civil du Québec, RLRQ c C-1991.

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021 c 25.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1.

Loi sur l'administration fiscale, RLRQ c A-6.002.

Loi sur l'Agence du revenu du Québec, RLRQ c A-7.003.