Nº 11-633-X au catalogue — Nº 044
ISSN 2371-3437
ISBN 978-0-660-44783-4

Études analytiques : méthodes et références

Exploration de l'utilisation de la technologie des chaînes de blocs pour authentifier les données du site Web de Statistique Canada

Par Kathryn Fedchun, Lillian Klein, et Didem Demirag

Date de diffusion : le 19 septembre 2022

Statistique Canada Statistics Canada

Canada

Comment obtenir d'autres renseignements

Pour toute demande de renseignements au sujet de ce produit ou sur l'ensemble des données et des services de Statistique Canada, visiter notre site Web à www.statcan.gc.ca.

Vous pouvez également communiquer avec nous par :

Courriel à infostats@statcan.gc.ca

Téléphone entre 8 h 30 et 16 h 30 du lundi au vendredi aux numéros suivants :

- Service de renseignements statistiques 1-800-263-1136
- Service national d'appareils de télécommunications pour les malentendants 1-800-363-7629
- Télécopieur 1-514-283-9350

Programme des services de dépôt

- Service de renseignements 1-800-635-7943
- Télécopieur 1-800-565-7757

Normes de service à la clientèle

Statistique Canada s'engage à fournir à ses clients des services rapides, fiables et courtois. À cet égard, notre organisme s'est doté de normes de service à la clientèle que les employés observent. Pour obtenir une copie de ces normes de service, veuillez communiquer avec Statistique Canada au numéro sans frais 1-800-263-1136. Les normes de service sont aussi publiées sur le site www.statcan.gc.ca sous « Contactez-nous » > « Normes de service à la clientèle ».

Note de reconnaissance

Le succès du système statistique du Canada repose sur un partenariat bien établi entre Statistique Canada et la population du Canada, les entreprises, les administrations et les autres organismes. Sans cette collaboration et cette bonne volonté, il serait impossible de produire des statistiques exactes et actuelles.

TABLE DES MATIÈRES

SOMMAIRE

« Savez-vous ce qu'est un jeton non fongible (NFT)? » Cette question a lancé une réaction en chaîne qui a entraîné une enquête menée par une équipe diversifiée visant à savoir comment Statistique Canada (StatCan) pourrait utiliser une technologie de chaînes de blocs, ou la technologie de registre distribué, pour authentifier un document. Cette question a été posée dans le cadre d'une idée plus significative sur la façon dont la Division de la diffusion pourrait utiliser des jetons non fongibles, ou une technologie similaire, afin d'authentifier les produits quittant le site Web de StatCan. Initialement, notre équipe était composée d'employés internes de StatCan : Mathieu Laporte, directeur de la Division de la diffusion, Jacqueline Luffman, chef des Services d'édition, et Lillian Klein, bibliothécaire de recherche. Ces personnes ont discuté de l'idée avec d'autres membres du personnel de StatCan, afin d'évaluer sa faisabilité. Toutefois, reconnaissant des lacunes dans notre expérience en technologie de chaînes de blocs, nous nous sommes adressés à des universitaires menant des recherches sur divers aspects de cette technologie. Dans le cadre de ces réunions, nous sommes entrés en contact avec quatre experts en technologie des chaînes de blocs : Florian Martin-Bariteau de l'Université d'Ottawa, Jeremy Clark de l'Université Concordia, Victoria Lemieux de l'Université de la Colombie-Britannique et Tracey Lauriault de l'Université Carleton. Nous avons rencontré ces spécialistes dans le cadre d'une séance de remue-méninges, au cours de laquelle Jeremy Clark a présenté l'idée d'utiliser des signatures numériques pour authentifier les documents de StatCan. Avec cette idée en tête, une équipe de chercheurs a été formée pour explorer la technologie et les applications cryptographiques les plus récentes, afin de parfaitement comprendre cette technologie et de déterminer si elle serait utile dans le travail de StatCan. Notre équipe de recherche comprend Kathryn Fedchun, doctorante à l'Université Carleton, Didem Demirag, doctorant à l'Université Concordia, et Lillian Klein, bibliothécaire de recherche à StatCan. La présente étude résume plusieurs mois de travail de collaboration de cette équipe.

Ce projet se consacre principalement à mieux comprendre la technologie des chaînes de blocs et à estimer si, à mesure que StatCan étend son site Web, l'organisme pourrait l'utiliser pour permettre aux utilisateurs d'authentifier les données téléchargées du site Web. En comprenant de mieux en mieux ces technologies émergentes, l'objectif de ce projet est d'élaborer un processus d'authentification qui permettrait aux utilisateurs de vérifier que le contenu téléchargé depuis le site Web de StatCan n'a pas été manipulé et a bien été produit par StatCan. Ce processus pourrait accroître la confiance globale envers l'organisme en tant qu'organisme de statistique. En utilisant la technologie des chaînes de blocs pour déterminer l'authenticité de ses données, StatCan a la capacité d'accroître la confiance sociale de ces utilisateurs. Il a été déterminé que la méthode idéale d'authentification des données devrait être facile à utiliser et disponible dans un format en ligne et hors ligne, pour veiller à ce que les utilisateurs ayant divers degrés de connexion à Internet puissent authentifier leurs données.

Notre recherche a défini et expliqué ce qu'est la technologie des chaînes de blocs et relevé la façon dont cette technologie est actuellement utilisée dans un contexte canadien. Nous avons découvert qu'un récent appel à l'action demandait aux organismes gouvernementaux d'adopter la technologie de chaînes de blocs et de prendre des mesures pour la mettre en œuvre dans leurs activités. Pour créer une évaluation suffisamment complète de la technologie, nous avons inclus un examen des préoccupations la concernant. Nous nous sommes principalement concentrés sur les répercussions environnementales, la perception du public quant à cette technologie et toute éventuelle réaction négative que notre équipe a pu anticiper, le manque de réglementation et la potentielle influence du battage médiatique entourant la technologie des chaînes de blocs. Enfin, nous avons brièvement comparé cinq chaînes de blocs qui pourraient être utilisées dans notre solution. Cette comparaison se concentre sur des renseignements généraux relatifs à chaque chaîne, ainsi que le nombre de transactions par seconde, le mécanisme de consensus, la nature privée ou publique de la chaîne et les répercussions environnementales de chaque chaîne de blocs. Cette analyse nous a permis de décider qu'Avalanche était la meilleure option pour nous, à mesure que notre solution technique progresse.

Grâce aux connaissances acquises dans le cadre de cette recherche, notre équipe recommande que ce projet soit l'occasion pour l'organisme de répondre à cet appel à l'action. Nous proposons que StatCan mène un projet pilote fondé sur l'idée de Jeremy Clark d'utiliser des signatures numériques et de créer une application que les utilisateurs puissent télécharger afin d'authentifier leurs données. Nous proposons d'avoir recours à un modèle hybride avec une chaîne de blocs qui permette à la fois aux utilisateurs en ligne et hors ligne d'authentifier leurs données. Les détails techniques de ce projet sont expliqués plus en détail ci-dessous. En résumé :

Dans cette solution hybride, l'authentification se déroulera au moyen d'une application que les utili-

sateurs devront télécharger. La liste de condensés numériques de fichiers sera régulièrement mise à jour, afin de contenir les condensés numériques de nouveaux produits de StatCan. L'authentification d'un fichier se déroulera comme suit : l'utilisateur devra téléverser dans l'application le fichier ayant besoin d'être authentifié. Cette action déclenchera le calcul du condensé numérique du fichier par l'application qui le comparera avec la liste des condensés existants de produits de StatCan. L'application informera ensuite l'utilisateur de la validité du fichier.

Cette solution ajoute une valeur considérable à la transparence de l'organisme et à la confiance que lui accordent les utilisateurs. L'hébergement des valeurs de condensés numériques dans la chaîne de blocs crée un enregistrement inaltérable au fil du temps des produits diffusés par l'organisme et accroît la capacité des utilisateurs de faire confiance aux renseignements téléchargés à partir du site Web de StatCan. Ce projet est l'occasion d'expérimenter avec la technologie des chaînes de blocs sans remanier le système existant de l'organisme.

INTRODUCTION

En cette ère de l'information, il est nécessaire d'admettre le volume croissant d'information numérique à la disposition de la population canadienne et la méfiance croissante de cette dernière envers les sources numériques (Centre for International Governance Innovation d'Ipsos Public Affairs pour le Canada [CIGI-IPSOS], 2019). Selon l'enquête du Centre for International Governance Innovation (2019) d'Ipsos Public Affairs pour le Canada, 36 % des Canadiennes et des Canadiens pensent que le gouvernement contribue à leur sentiment de méfiance envers Internet. Statistique Canada (StatCan) étant l'antenne du gouvernement chargée de diffusion de l'information à la population canadienne, l'organisme ne devrait pas ignorer cette statistique. Au cours de l'exercice financier 2020-2021, le site Web de StatCan a enregistré plus de 28 millions de consultations de pages Web et 766 589 téléchargements de tableaux (Statistique Canada, 2021). StatCan s'enorgueillit de sa transparence et de sa responsabilité envers le public et s'efforce de répondre aux besoins de ses utilisateurs (Statistique Canada, 2018). En tant qu'organisme, StatCan se présente comme « une source fiable de statistiques sur le Canada » (Statistique Canada, 2018). Selon le Centre de confiance de StatCan, « La population peut être confiante que les renseignements recueillis auprès d'elle et à son sujet le sont à son profit, et que les activités sont menées avec intégrité et dans le respect des normes éthiques les plus élevées » (Statistique Canada, 2018). La Loi sur la statistique oriente StatCan, afin de veiller à ce que l'organisme favorise et mette au point « des statistiques sociales et économiques intégrées concernant l'ensemble du Canada » (Loi sur la statistique, 1985).

Les utilisateurs se fient à l'organisme et s'attendent à pouvoir accéder à des données authentiques et fiables et à pouvoir les télécharger lorsqu'ils accèdent au site Web de Statistique Canada. Cependant, après le téléchargement d'un produit, il est difficile de valider qu'il appartient à StatCan et qu'il n'a pas été modifié par un intervenant malveillant. Cela signifie que les utilisateurs peuvent croire qu'ils accèdent à des données non modifiées de StatCan lorsqu'ils téléchargent un fichier .CSV (à valeurs séparées par des virgules) corrompu. Quant à la possibilité que StatCan puisse être victime de cybermenaces aux mains d'intervenants malveillants, le nombre croissant d'attaques auprès d'organisations canadiennes à l'aide de logiciels rançonneurs montre que le pays est une cible potentielle (Centre de la sécurité des télécommunications Canada, 2021). Par conséquent, alors que StatCan commence à planifier l'expansion et l'innovation de son site Web, il est essentiel que l'organisme envisage la façon de fournir aux utilisateurs la capacité de vérifier et d'authentifier les données qu'ils téléchargent depuis ce site Web.

La présente recherche vise à explorer si StatCan pourrait combler les lacunes d'authentification de son site Web en intégrant des technologies émergentes à sa méthodologie de publication existante. Pour répondre à ce questionnement, nous avons commencé par nous familiariser avec les recherches actuelles relatives aux technologies de chaînes de blocs et de registre distribué. Nous avons ensuite exploré l'importance de la tenue de registres, de la confidentialité, de la confiance et de l'authentification. Nous avons étudié de multiples exemples d'autres organisations et organismes du gouvernement du Canada qui utilisent des chaînes de blocs et avons trouvé de nombreux articles encourageant le gouvernement à adopter cette nouvelle technologie. Nous avons toutefois également tenu compte des préoccupations relatives à ces technologies émergentes, notamment les répercussions environnementales, l'image publique et une éventuelle réaction négative du public, le manque de réglementation et la potentielle influence du battage médiatique en la matière. Nous avons étudié cinq chaînes de blocs qui pourraient être utilisées dans la conception de notre système : Ethereum, Avalanche, Cardano, Hyperledger et Solana.

En comprenant mieux la technologie à la disposition de StatCan, nous nous sommes efforcés de conceptualiser un système permettant aux utilisateurs d'authentifier les données qu'ils téléchargent du site Web. Notre objectif est que ce système permette aux utilisateurs de vérifier que le contenu téléchargé depuis le site Web n'a pas été manipulé et a bien été produit par StatCan. Nous pensons que notre méthode d'authentification des données devrait être disponible dans un format en ligne et hors ligne, afin de veiller à ce que les utilisateurs ayant divers degrés de connexion à Internet puissent authentifier les données. Notre équipe a donné la priorité à cet aspect, afin de servir tous les utilisateurs canadiens, sachant qu'une connexion haute vitesse à Internet n'est pas une constante du fait du fossé numérique dans le pays (Forum des politiques publiques du Canada, 2014). De plus, nous avons donné la priorité à l'utilité, en envisageant les options d'une solution devant être aussi simple que possible pour veiller à ce que la technologie soit accessible et facile à comprendre par les utilisateurs.

Avant de pouvoir recommander une solution, il est nécessaire de présenter la technologie qui la sous-tend, afin de fournir le contexte nécessaire pour comprendre comment la technologie peut aider StatCan à atteindre son but. Les principales fonctionnalités devant être comprises sont les signatures numériques et les fonctions de hachage qui appuient notre concept. En plus de l'introduction et de l'analyse documentaire, l'annexe A présente un glossaire terminologique visant à aider les lecteurs à comprendre le contenu plus technique.

LACUNES DANS LA DOCUMENTATION

Tout au long du processus de recherche, nous avons relevé quelques lacunes dans la documentation. Les chaînes de blocs étant encore une technologie relativement nouvelle, en particulier dans le cadre d'une utilisation gouvernementale, ces lacunes ne sont pas surprenantes. Il a été difficile de trouver des politiques ou règlements gouvernementaux canadiens concrets portant sur la manière d'intégrer la technologie de chaînes de blocs. Cela signifie que des lignes directrices sur la mise en œuvre de la technologie de chaînes de blocs au sein du gouvernement sont encore en cours d'élaboration. Cette lacune laisse notre équipe avec des questions quant à la façon dont les politiques pourraient changer à l'avenir, en simplifiant ou compliquant la mise en œuvre de ce projet. Une autre lacune relevée est le manque de variété quant à la façon dont les organisations ont publié leur méthode d'intégration d'une chaîne de blocs dans leurs activités quotidiennes. Nous avons trouvé un grand nombre de documents sur la façon dont les chaînes de blocs sont utilisées en cryptomonnaie, en tenue de registres et en technologie financière. Il a cependant été difficile de déterminer comment les organisations utilisent des chaînes de blocs au quotidien. Nous n'avons également pas pu trouver de renseignements significatifs sur la mise en œuvre juridique de l'utilisation de chaînes de blocs aux fins qui nous intéressent. Dans le cas de dossiers médicaux dont il est question ci-dessous, par exemple, il a été difficile de déterminer comment les dossiers des patients étaient téléversés ou suivis dans la chaîne de blocs. Il a en outre été difficile de trouver des recherches sur des projets similaires. Nous n'avons pas pu trouver de recherches publiées cherchant à aborder la question de la façon d'habiliter les utilisateurs à authentifier des données téléchargées d'un site Web. Nous pensons que notre projet comble certaines de ces lacunes dans la documentation et qu'il est un pas précieux dans la direction de l'adoption de nouvelles technologies pour StatCan.

MÉTHODOLOGIE

ANALYSE DOCUMENTAIRE SYSTÉMATIQUE

Dans le cadre de la présente étude, nous avons effectué une analyse documentaire systématique qui nous a permis de comprendre l'étendue et la profondeur du corpus de travaux existant et de relever les lacunes à explorer (Xiao et Watson, 2019, p. 93). Réussir une analyse documentaire systématique comprend trois étapes : la planification, la mise en œuvre et la production d'un rapport (Xiao et Watson, 2019, p. 102). Lors de la première étape (la planification), les chercheurs déterminent le besoin d'un examen, précisent les questions de recherche et élaborent un protocole d'examen (Xiao et Watson, 2019, p. 102). Lors de la deuxième étape, les chercheurs effectuent la recherche, déterminent et sélectionnent les études principales, extraient, analysent et synthétisent les données (Xiao et Watson, 2019, p. 102). Enfin, dans la troisième étape, les chercheurs rédigent le rapport visant à diffuser leurs constats (Xiao et Watson, 2019, p. 102). Dans le cadre du présent projet, nous avions les trois questions de recherche suivantes à l'esprit :

1. **Qu'est-ce que la technologie des chaînes de blocs et comment d'autres agences et organisations gouvernementales l'ont-elles utilisée?**
2. **Comment cette technologie peut-elle être utilisée pour améliorer la tenue de registres,**

la confidentialité, la confiance et l'authentification relativement au site Web de Statistique Canada?

3. **Comment pouvons-nous utiliser cette nouvelle technologie dans notre solution afin d'authentifier les données?**

Lors de l'étape de planification de cette étude, nous avons compilé une liste de mots de recherche axés sur nos domaines d'intérêt dans ce projet. Cette liste de mots de recherche figure en annexe B. Comme l'ont décrit Xiao et Watson (2019) dans leur article sur la façon de mener une analyse documentaire systématique, nous avons utilisé ces mots de recherche pour trouver des articles pertinents. À mesure de la collecte de ces articles de recherches universitaires, notre équipe a ajouté d'autres mots de recherche. Nous avons ensuite en recours à une variété de combinaisons des mots de recherche énumérés en annexe B avec des opérateurs booléens pour limiter nos résultats. Nous avons effectué 15 recherches uniques au total.

Selon le nombre de résultats obtenus dans le cadre d'une recherche, nous avons passé en revue entre 100 et 300 résultats. Si le nombre de résultats obtenus était inférieur à 1 000, nous avons examiné les 100 premiers résultats. Si le nombre de résultats était inférieur à 100 000, nous avons examiné les 200 premiers résultats; en cas de nombre de résultats supérieur à 100 000, nous avons examiné les 300 premiers résultats. Lors du processus d'examen, nous avons évalué les articles universitaires en fonction de leur pertinence relativement à la présente étude, à l'aide du titre de l'article, de son résumé et des mots-clés fournis. Globalement, nous avons rassemblé 59 articles et entré l'information de source dans un tableur, notamment le titre, les auteurs, l'année où l'article ou le livre a été publié, le résumé et une citation complète.

Après la collecte des sources, nous avons commencé à passer en revue chaque article, afin de déterminer sa pertinence par rapport au projet. Nous avons évalué les résumés plus en détail et parcouru les articles pour en évaluer l'utilité. Parmi les 59 articles, nous avons relevé 18 sources présentant une valeur significative pour ce projet. La plupart des articles exclus étaient trop techniques aux fins de cette analyse documentaire. Bien que nous nous efforcions de rendre la présente étude relativement accessible, nous fournissons une liste de termes techniques et leurs définitions en annexe A. Même si certaines de ces définitions sont des paraphrases, elles contiennent un certain nombre de citations pour en maintenir l'intégrité.

De nos 18 sources, nous avons extrait des données et renseignements pertinents et les avons synthétisés dans l'analyse documentaire ci-dessous. À l'aide des questions de recherche ci-dessus, nous avons fourni un aperçu détaillé de la technologie, tenu compte de l'importance de la tenue de registres, de la confidentialité, de la confiance et de l'authentification, ainsi qu'une liste d'exemples d'autres organisations et agences gouvernementales qui utilisent des chaînes de blocs. Nous avons en outre été surpris de trouver de multiples articles encourageant le gouvernement à utiliser ces nouvelles technologies et nous avons également inclus cela comme thème ci-dessous.

Outre les articles universitaires, nous avons examiné de nombreux articles concernant les aspects préoccupants de la technologie de chaînes de blocs dans les domaines des répercussions environnementales, de l'image publique et d'une éventuelle réaction négative du public, du manque de réglementation et de la potentielle influence du battage médiatique relatif à cette technologie. Nous avons également effectué des recherches sur cinq chaînes de blocs en particulier : Ethereum, Avalanche, Cardano, Hyperledger et Solana. Le nombre de chaînes de blocs disponibles augmente chaque jour, mais notre équipe a choisi d'explorer ces cinq-là. Ethereum est une chaîne de blocs de pair-à-pair extrêmement populaire consommant une assez grande quantité d'énergie. Avalanche est une chaîne de blocs à preuve d'enjeu plus écologique, comme Cardano, qui est également une chaîne de blocs à preuve d'enjeu plus respectueuse de l'environnement qu'Ethereum. Hyperledger est un projet global de chaînes de blocs en source ouverte ainsi que des outils connexes et Solana est une chaîne de blocs à preuve d'enjeu neutre en carbone. De plus amples détails sur ces cinq chaînes de blocs et leurs différences sont fournis ci-dessous. Cette analyse documentaire systématique a renforcé nos connaissances sur cette technologie et nous a aidés à formuler des solutions recommandées et les étapes suivantes de ce projet, présentées ci-dessous.

ANALYSE DOCUMENTAIRE

Ce projet vise à explorer la façon dont la technologie peut aider les utilisateurs à vérifier et à authentifier des données provenant du site Web de StatCan. La présente analyse documentaire commence par un aperçu de la technologie cryptographique. Nous considérons ensuite l'importance de la tenue de registres, de la confidentialité, de la confiance et de l'authentification. Nous fournissons des exemples d'organisations, d'agences et d'entreprises au Canada utilisant cette technologie. Nous dressons ensuite une liste de nombreuses sources demandant au gouvernement d'adopter de nouvelles technologies, comme celle des chaînes de blocs. Nous examinons ensuite d'éventuelles préoccupations relatives à l'utilisation des chaînes de blocs, comme les répercussions environnementales, l'image publique et une éventuelle réaction négative du public, le manque de réglementation et la potentielle influence du battage médiatique relatif à la technologie des chaînes de blocs. Enfin, nous comparons cinq chaînes de blocs : Ethereum, Avalanche, Cardano, Hyperledger et Solana. Ce projet est une petite avancée de StatCan vers de nouvelles technologies pouvant mieux protéger ses données.

APERÇU DE LA TECHNOLOGIE

Au début des années 1990, les cryptographes Scott Stornetta et Stuart Haber ont conçu l'idée de relier des blocs par données hachées (condensées) (Treiblmaier et Clohessy, 2020, p. v). Près de 20 ans plus tard, le 31 octobre 2008 :

> **Une mystérieuse personne (ou un groupe de personnes), connue uniquement sous le pseudonyme de Satoshi Nakamoto, a publié un lien vers un livre blanc intitulé Bitcoin: A Peer-to-Peer Electronic Cash System (Bitcoin: système de monnaie électronique de pair-à-pair) sur une obscure liste de diffusion appelée Cryptography List. Dans ce livre blanc, Nakamoto proposait la création de ce qui prendrait le nom de chaîne de blocs comme moyen d'établir un système de paiement électronique ne nécessitant pas d'intermédiaire tiers de confiance (Urban et Pineda, 2018, p. 5).**

Une chaîne de blocs est un registre numérique, décentralisé et distribué dans lequel des transactions sont enregistrées et ajoutées dans leur ordre chronologique, afin de créer des enregistrements permanents infalsifiables (Treiblmaier, 2018, p. 547). L'idée de registre existait depuis longtemps; il s'agit d'une collection permanente de transactions enregistrées, inscrites historiquement dans un livre physique. La chaîne de blocs prend son origine dans cette idée en déplaçant le registre en ligne dans le cadre d'une monnaie numérique. Depuis lors, l'idée de la chaîne de blocs s'est élargie pour inclure la sécurité numérique au-delà d'une monnaie numérique comme Bitcoin.

La majeure partie de cette technologie prend ses racines dans la cryptographie. Le terme « cryptographie » est dérivé du mot grec kryptos, utilisé pour décrire tout ce qui est caché, voilé, secret ou mystérieux (Mohamed, 2020, s.p). La cryptographie permet de sécuriser la communication et l'information à l'aide de technologies et de codes. Il est bien connu que les données sont précieuses et souvent vulnérables. Dans le monde d'aujourd'hui, produire de faux documents est de plus en plus courant. Puisque les faux documents ressemblent exactement aux originaux, il est difficile pour tout un chacun de distinguer le vrai de sa copie (Prathibha et Krishna, 2021, p. 71). En sachant cela, la technologie ayant recours à la cryptographie et aux chaînes de blocs peut protéger l'information, en rendant un document infalsifiable et exceptionnellement difficile à modifier ou à supprimer (De Filippi, 2018, p. 34–35). À mesure que les gens commencent à reconnaître la valeur significative et intrinsèque des données, les technologies de chaînes de blocs et de registre distribué peuvent forcer des organisations à repenser de façon fondamentale leurs relations avec les utilisateurs et les approches en matière de protection de la vie privée (Maull et coll., 2017, p. 484). Avant de fournir des exemples de chaînes de blocs utilisées au Canada, nous allons discuter de l'importance de la tenue de registres, de la confidentialité, de la confiance et de l'authentification dans le cadre de notre projet.

TENUE DE REGISTRES

Victoria Lemieux, an archival studies scholar, claims that "Victoria Lemieux, chercheure en archivistique, déclare que la majorité des discussions sur les enregistrements ou les systèmes de confiance se résument en deux concepts interreliés : la fiabilité et l'authenticité (2016a, p. 112). Lorsque des utilisateurs accèdent à des enregistrements, ils tiennent compte de tout risque potentiel associé aux données (Lemieux, 2016a). Les utilisateurs déterminent la fiabilité des données en fonction de la façon dont ils accèdent aux données et de la création des enregistrements, notamment la personne ayant créé l'enregistrement et la façon dont ce dernier a été créé (Lemieux, 2016a). Mme Lemieux avance que la préservation de l'information à long terme au format numérique nécessite

d'aborder les dangers techniques auxquels est confrontée la longévité de l'information authentique (2016a, p. 114). Dans notre cas, l'objectif de ce qui est réellement enregistré dans la chaîne n'est pas l'archivage, mais plutôt l'établissement de l'authenticité de l'enregistrement initial de la transaction (Lemieux, 2016b, p. 15). Le but du présent projet est de protéger de façon proactive les données de StatCan grâce à la valeur ajoutée de la technologie de chaînes de blocs.

CONFIDENTIALITÉ

Le présent projet démontre que StatCan reconnaît l'importance de la confidentialité. En matière de données, la confidentialité désigne la protection de l'information (telle que des fichiers informatiques ou des éléments de base de données), de sorte que seules des personnes autorisées peuvent y accéder de façon contrôlée (Mohamed, 2020, s.p). Les données de StatCan doivent être protégées contre des menaces ou attaques potentielles. Pour ce faire, nous devons déterminer la vulnérabilité ou la faiblesse du système actuel de StatCan (Mohamed, 2020). Il est possible que les données du site Web de StatCan puissent être modifiées sans que l'utilisateur ne le sache. Ce projet tente d'éviter ce potentiel risque en abordant la confidentialité et en veillant à ce que l'information puisse être authentifiée par l'utilisateur.

CONFIANCE

Selon un chapitre sur la manière dont l'authenticité peut transformer la confiance sociale, Batista et coll. illustrent les trois aspects les plus importants de la confiance : l'exactitude, la fiabilité et l'authenticité (2021, p. 112). Ils argumentent que des enregistrements exacts [et fiables] sont précis, corrects, fidèles..., cohérents, complets et objectifs (Batista et coll., 2021, p. 114). Pour susciter la confiance, les auteurs décrivent que des enregistrements authentiques doivent préserver leur identité et leur intégrité tout au long de la période de conservation à long terme (Batista et coll., 2021, p. 116). Dans le cas d'archives numériques, les auteurs décrivent la difficulté de maintenir la confiance dans un document numérique. Supposons, par exemple, qu'un document statistique ait été modifié. Dans ce cas, il peut être difficile de détecter les variances entre l'original et la copie modifiée; cela peut avoir une incidence négative sur la confiance sociale, du fait de ce qu'ils appellent une « authenticité incertaine » (Batista et coll., 2021, p. 117). Le présent projet cherche à améliorer la confiance entre StatCan et ses utilisateurs en fournissant une façon d'authentifier les données du site Web de StatCan et d'éliminer l'incertitude.

AUTHENTIFICATION

L'authentification désigne la capacité de déterminer la validité d'une source. Cette notion répond à la question, Comment un destinataire peut-il savoir que l'entité de communication distante est bien qui elle prétend être? (Mohamed, 2020, s.p). Dans le cadre du présent projet, StatCan souhaite aider les utilisateurs à déterminer la validité d'une source au moyen d'un processus d'authentification. Des algorithmes cryptographiques soutiennent le chiffrement authentifié; ce qui signifie que les utilisateurs peuvent être certains que la source est authentique (Mohamed, 2020). La notion d'intégrité découle également de cette vérification; les utilisateurs peuvent savoir que l'information n'a pas été modifiée, sauf si des employés de StatCan la modifient en suivant le processus adéquat d'autorisation (Mohamed, 2020). Manifestement, la tenue de registres, la confidentialité, la confiance et l'authentification sont des facteurs importants du présent projet. Nous allons maintenant présenter des exemples démontrant l'utilisation de cette technologie au Canada.

ÉLÉMENTS CLÉES

- La cryptographie est le processus de sécuriser la communication et l'information avec des moyens technologiques.
- Une chaîne de blocs est un registre numérique, décentralisé et distribué.
- Une chaîne de blocs peut soutenir la tenue de registres au moyen de l'archivage des données, accroître la confidentialité et atténuer la vulnérabilité, susciter la confiance entre l'utilisateur et StatCan et aider les utilisateurs à authentifier les données du site Web de StatCan.

EXEMPLES AU CANADA

Nous avons relevé de nombreux exemples au cours de nos recherches auprès d'instances du gouvernement canadien ayant intégré la technologie de chaînes de blocs dans des projets particuliers. Dans un énoncé de politique publié par le Mowat Centre for Policy Innovation de l'Université de Toronto, Urban et Pineda (2018, p. 61-62) ont énuméré de nombreux organismes gouvernementaux canadiens expérimentant dans le domaine des chaînes de bloc, comme Innovation, Sciences et Développement économique Canada, le Secrétariat du Conseil du Trésor du Canada et le Conseil national de recherches Canada (CNRC). En janvier 2018, le Programme d'aide à la recherche industrielle du CNRC a utilisé une chaîne de blocs Ethereum pour publier de façon proactive des données de subventions et contributions en temps réel (Programme d'aide à la recherche industrielle,

2019). Ce projet était une expérience d'un an et a pris fin le 1er mars 2019. Même si cette expérience n'est plus en cours, ce travail a fourni des informations constructives sur le potentiel de cette technologie et la façon dont elle peut permettre des opérations plus ouvertes et transparentes pour des programmes publics (Conseil national de recherches Canada, 2018).

De nombreux ordres gouvernementaux ont commencé à utiliser des chaînes de blocs en matière de permis, notamment le gouvernement de l'Ontario, la ville de Toronto et le gouvernement de la Colombie-Britannique (Urban et Pineda, 2018, p. 62). Un article énumère diverses façons dont les administrations publiques utilisent des chaînes de blocs, notamment en matière d'identité numérique, de stockage de décisions judiciaires, de financement d'établissements d'enseignement et de traçage d'argent, d'état matrimonial, de vote électronique, de permis d'exploitation d'entreprise, de passeports, de casier judiciaire et même de dossiers fiscaux (Ølnes, Ubacht et Janssen, 2017, p. 357). Le gouvernement de l'Ontario a également organisé un marathon de programmation de chaînes de blocs ayant généré un certain nombre d'idées pour d'autres applications de chaînes de blocs au sein d'administrations publiques (Urban et Pineda, 2018, p. 62). Soutenir des projets pilotes ayant recours à la technologie de chaînes de blocs est une manière efficace pour le gouvernement de commencer à utiliser ces nouvelles technologies avec succès (Urban et Pineda, 2018, p. 67). Les administrations publiques ont recours à des chaînes de blocs dans de nombreux domaines et StatCan peut utiliser ces connaissances et ce travail dans le cadre du présent projet.

Outre les organismes gouvernementaux qui mettent en œuvre les technologies de chaînes de blocs et de registre distribué, le domaine des soins de santé avance rapidement vers l'utilisation de chaînes de blocs et de dossiers médicaux numériques. Enregistrer des dossiers médicaux électroniques dans une chaîne de blocs améliore non seulement la tenue des registres, mais fournit en outre aux patients un plus grand contrôle sur leur propre santé et leurs traitements médicaux (Urban et Pineda, 2018, p. 42). Les médecins, les infirmiers et infirmières, les hôpitaux et d'autres établissements de soins de santé ont recours à des chaînes de blocs pour certifier la santé de patients (De Filippi, 2018, p. 112). Ces chaînes servent à stocker les dossiers médicaux personnels chiffrés (Zheng, Zhu, et Si, 2019, p. 17). Une chaîne de blocs peut fournir l'accès à des personnes particulières, de sorte que le dossier médical d'une personne demeure sécurisé et confidentiel lorsqu'il est enregistré dans un registre distribué (Zheng, Zhu et Si, 2019). Mme Lemieux explique que les conditions sous-jacentes au Canada sont particulièrement bien adaptées pour mener la recherche et la mise en œuvre de la technologie de chaînes de blocs; le Canada disposant d'un espace technologique relatif aux chaînes de blocs dynamique et hautement actif, comptant diverses entreprises émergentes et divers cabinets-conseils faisant un travail innovateur (2016b, p. 5). C'est avec grand enthousiasme que nous contribuons à ce travail dans le cadre du présent projet.

ÉLÉMENTS CLÉES

- De nombreux ordres gouvernementaux au Canada utilisent la technologie de chaînes de blocs, notamment le gouvernement de l'Ontario, la ville de Toronto et le gouvernement de la Colombie-Britannique.
- Le domaine des soins de santé au Canada a également commencé à utiliser les technologies de chaînes de blocs et de registre distribué pour stocker de façon sécurisée des dossiers médicaux numériques.

APPEL À L'ACTION

Dans de multiples articles, il a été demandé aux administrations publiques d'adopter de nouvelles technologies pour mieux sécuriser leurs données. Urban et Pineda argumentent que la technologie de chaînes de blocs peut offrir aux administrations publiques la possibilité d'améliorer la transparence, l'efficience et l'efficacité (2018, p. 42). Alors que les chaînes de blocs ne sont pas une nouvelle technologie, leur utilisation au sein d'administrations publiques est relativement nouvelle, de sorte que le niveau d'expertise dans ce domaine et les capacités au sein des administrations publiques et des organismes de réglementation du Canada sont actuellement limités (Urban et Pineda, 2018, p. 61). Ils déclarent que l'une des premières mesures que devrait entreprendre le gouvernement canadien est ce que nous faisons actuellement dans le cadre du présent projet : établir des groupes de technologues et de décideurs au sein des administrations publiques qui comprennent la technologie, ses conséquences ainsi que les possibilités et défis potentiels en découlant (Urban et Pineda, 2018, p. 61). Alors qu'Urban et Pineda (2018) encouragent le recours aux chaînes de blocs au sein du gouvernement, Ølnes, Ubacht et Janssen soulignent que le gouvernement devrait passer d'une approche axée sur la technologie à une approche axée sur les besoins dans le cadre d'applications de chaînes de blocs (2017, p. 355). Ils argumentent que la technologie de chaînes de blocs entraînera l'innovation et la transformation des proces-

sus gouvernementaux (Ølnes, Ubacht et Janssen, 2017, p. 355). Étant donné la facilité avec laquelle des fichiers numériques peuvent être modifiés (Bell et coll., 2019, p. 6), nous soutenons que le présent projet est motivé par un besoin d'authentification des données du site Web de StatCan.

Selon De Filippi, les administrations publiques ont établi et assuré l'intendance de divers systèmes et institutions visant à améliorer le bien-être social et à fournir l'infrastructure de base de la croissance économique et politique tout au long de l'histoire (2018, p. 107). Dans un article sur la cryptographie et les administrations publiques, Aljeaid et coll. argumentent que le gouvernement électronique devrait agir comme un pont en matière de communication entre les administrations publiques et les citoyens, entre les administrations publiques elles-mêmes ou entre les administrations publiques et les entreprises, de façons efficientes et fiables (2014, p. 581). Les auteurs soulignent l'importance de la sécurité des données au sein des administrations publiques quant à une vulnérabilité potentielle en l'absence de mesures de sécurité. Ils déclarent que les utilisateurs finaux ont besoin de solutions de sécurité robustes, afin d'atteindre l'assurance lorsqu'ils utilisent les systèmes d'un gouvernement électronique (Aljeaid et coll., 2014, p. 581). Créer un répertoire d'enregistrements publics infalsifiables et résilients (De Filippi, 2018, p. 107-108) à l'aide de la cryptographie et de chaînes de blocs peut aider les administrations publiques à éviter la fuite de données, la perte de données et d'autres vulnérabilités. Nous sommes d'accord avec cet appel à l'action et pensons que le présent projet améliorera la confiance du public envers StatCan et le gouvernement du Canada.

ÉLÉMENTS CLÉES

- De nombreux auteurs demandent aux administrations publiques canadiennes d'adopter de nouvelles technologies, comme les chaînes de blocs, pour mieux sécuriser leurs données.
- Cette technologie peut aider les administrations publiques à éviter les vulnérabilités en matière de données et améliorer la transparence, la sécurité, l'efficience et l'efficacité.

PRÉOCCUPATIONS

Alors que cet appel à l'action est important, nous souhaitons également prendre le temps d'explorer toute préoccupation éventuelle relative à la technologie de chaînes de blocs. Nous avons résumé nos constats en quatre catégories : les répercussions environnementales, l'image publique et une éventuelle réaction du public, le manque de réglementation et la possibilité d'une influence du battage médiatique relatif à la technologie des chaînes de blocs.

RÉPERCUSSIONS ENVIRONNEMENTALES

Il existe de nombreuses allégations quant aux répercussions environnementales de la nouvelle technologie de chaînes de blocs. En novembre 2021, un projet de chaîne de blocs intitulé Solana a engagé Robert Murphy, conseiller en matière climatique et énergétique, dans le but de publier un rapport sur la consommation d'énergie (Solana, 2021). Il a comparé les activités courantes entraînant une consommation d'énergie d'une transaction Solana, d'une transaction Ethereum et d'une transaction Bitcoin (Solana, 2021). Même s'il n'a pas inclus toutes les options de chaînes de blocs que nous avons choisi d'explorer, il est utile de tenir compte de la comparaison entre les transactions de chaîne de blocs et les activités quotidiennes. Effectuer une seule recherche avec Google consomme 1 080 joules d'énergie, travailler avec un ordinateur doté d'un moniteur pendant une heure consomme 46 800 joules et utiliser un gallon (3 785 litres) d'essence consomme 121 320 000 joules (Solana, 2021). En comparaison, une transaction Solana consomme 1 837 joules d'énergie, une transaction Ethereum consomme 692 820 000 joules et une transaction Bitcoin consomme 6 995 592 000 joules (Solana, 2021). Selon Huang, O'Neill et Tabuchi pour The New York Times, le processus de création de bitcoins aux fins de dépense ou d'échange consomme environ 91 térawatts-heure d'électricité chaque année; plus que n'utilise la Finlande, nation comptant 5,5 millions d'habitants (2021). Même si nous n'utilisons pas Bitcoin pour notre projet, ces chiffres sont stupéfiants.

Bon nombre des importants acteurs de la technologie de chaînes de blocs, y compris Ethereum, consomment une quantité étonnante d'énergie, du fait de leur mécanisme de consensus de preuve de travail. La preuve de travail nécessite que les participants au réseau de la chaîne de blocs consomment de vastes quantités de ressources informatiques et d'énergie lors de la génération de nouveaux blocs valides (Chandler, 2021). En comparaison, la preuve d'enjeu nécessite que les participants du réseau de la chaîne de blocs misent un montant de cryptomonnaie en garantie du nouveau bloc qui devrait être, selon eux, ajouté à la chaîne (Chandler, 2021). Chandler argumente

que la preuve de travail, comme l'utilise Ethereum, peut être plus sécuritaire et décentralisée, mais consomme également une immense quantité d'électricité, est plus lente et moins évolutive (Chandler, 2021). En revanche, la preuve d'enjeu, comme l'utilisent Avalanche, Cardano et Solana, présente de moindres répercussions environnementales et permet des transactions plus rapides et une meilleure évolutivité, mais est une forme plus récente de technologie et peut ne pas être aussi sûre ou infalsifiable que la preuve de travail (Chandler, 2021). Il est évident que la preuve de travail et la preuve d'enjeu présentent des avantages et des inconvénients et nous explorons les répercussions environnementales particulières de cinq chaînes de blocs (Ethereum, Avalanche, Cardano, Hyperledger et Solana) dans le tableau ci-dessous.

IMAGE PUBLIQUE ET ÉVENTUELLE RÉACTION NÉGATIVE

De nombreuses entreprises et organisations ont suscité une réaction négative lors de leur tentative d'utilisation de la technologie de chaînes de blocs. En décembre 2021, Kickstarter a annoncé que l'entreprise adoptait la technologie de chaînes de blocs (Plunkett, 2021). Le billet de blogue, intitulé « Let's Build What's Next for Crowdfunding Creative Projects » (Construisons la nouvelle étape des projets créatifs de financement participatif) a reçu de nombreuses critiques et plaintes de créateurs (Plunkett, 2021). Kickstarter a répondu en produisant une section de questions fréquemment posées, dans laquelle l'entreprise déclarait être confiante qu'un protocole de financement participatif établi sur Celo n'aurait pas d'effets négatifs significatifs sur les émissions de carbone de l'entreprise du fait de son architecture sous-jacente (Kickstarter, 2022). De nombreux créateurs et commanditaires ont tout de même affirmé qu'ils n'utiliseraient plus Kickstarter, à la suite de cette annonce (Morse, 2021).

De façon similaire à Kickstarter, la plateforme de communication numérique Discord a envoyé un gazouillis signalant l'intégration d'Ethereum à sa plateforme en novembre 2021 (Pearson, 2021). Le fondateur et directeur général de Discord, Jason Citron, a, deux jours plus tard, rapidement abandonné le projet étant donné la réaction négative du public (Pearson, 2021). M. Pearson commente que les gens de l'industrie du jeu détestent la technologie des chaînes de blocs, soit du fait des répercussions environnementales des jetons de preuve de travail dans Ethereum, soit selon l'idée que les chaînes de blocs collectionnables sont une arnaque fondée sur un mythe, voir les deux (2021). Bon nombre d'utilisateurs se sont désinscrits du service payant à supplément Nitro de la plateforme ou ont menacé de le faire (Jiang, 2021). Étant donné que ces deux exemples ont eu lieu récemment, en novembre et décembre 2021, il est difficile d'envisager ce que pourrait être l'opinion publique quant à StatCan et au présent projet. Toutefois, il est important de tenir compte de ces exemples et de reconnaître qu'une réaction négative est une conséquence potentielle.

MANQUE DE RÉGLEMENTATION

Une autre préoccupation est la nature décentralisée et non réglementée de la technologie de chaînes de blocs. Le contrôle et la prise de décisions en matière de chaînes de blocs ne sont pas effectués par une entité unique; il s'agit d'un domaine de préoccupation pour StatCan. Plutôt que de faire confiance à une entité, la confiance est placée dans des algorithmes mathématiques. D'autres projets de chaînes de blocs existant au sein des administrations publiques canadiennes devraient être utilisés pour orienter les politiques de StatCan quant à ce projet. Parmi les cinq chaînes de blocs que nous étudions ci-dessous, chacune dispose de différents règlements, objectifs et capacités. La mise à l'échelle peut également être difficile selon la chaîne de blocs choisie. Cela peut être une préoccupation, car le nombre de produits de StatCan disponibles à l'authentification n'a pas encore été décidé. Puisque nous avons considéré la confiance et la confidentialité plus tôt dans cette analyse documentaire, le manque de réglementation est moins inquiétant que les répercussions sur l'environnement et l'image publique. En fait, le présent projet est l'occasion de fournir un exemple préliminaire et d'être le chef de file en matière de réglementation relative à la mise en œuvre de chaînes de blocs et nous espérons pouvoir intégrer de nouvelles politiques à notre projet.

INFLUENCE DU BATTAGE MÉDIATIQUE

Il convient d'aborder le battage médiatique général relatif à la technologie de chaînes de blocs. Selon Victoria Lemieux, nous devons faire face aux faiblesses de conception et de mise en œuvre de la tenue de registres par chaînes de blocs, afin de pouvoir mieux réaliser la vision louable de cette technologie (Lemieux, 2019). Elle commente que les allégations associées à l'utilisation de la technologie de chaînes de blocs aux fins de tenue de registre sont, dans plusieurs cas, surestimées. Les solutions de chaînes de blocs qui revendiquent, par exemple, de fournir des solutions « archivistiques » ne fournissent en fait pas d'accessibilité à long terme aux enregistrements ni ne les préservent (Lemieux, 2016b, p. 4). Elle déclare que le plus grand danger des chaînes de blocs réside dans une confiance aveugle en leur endroit (2016b, p. 23). Toutefois, explorer ces limites de façon critique est la clé d'une utilisation réussie d'innovations technologiques, comme les chaînes de blocs, au profit de l'ensemble de la population canadienne (Lemieux, 2016b, p. 8). Alors que

la technologie de chaînes de blocs ne résout pas tous les problèmes qu'elle a été annoncée pouvoir résoudre, il s'agit d'une technologie utile qui continuera à être utilisée dans l'industrie et mérite de plus amples recherches et expérimentations (Ruoti et coll., 2020, p. 53). Même si cette technologie relativement nouvelle est palpitante et que les risques peuvent susciter la peur d'étouffer l'innovation (Lemieux, 2016b, p. 5), il est impératif d'adopter une attitude critique quant aux limites et préoccupations potentielles relatives à cette technologie blocs pour que ce projet présente le meilleur résultat possible.

ÉLÉMENTS CLÉES

- Le recours à la technologie de chaînes de blocs présente quatre préoccupations :

  1. les répercussions environnementales liées à la consommation d'énergie; différentes chaînes de blocs consommant différentes quantités d'énergie;
  2. une éventuelle réaction négative selon les expériences d'entreprises ayant tenté d'adopter les chaînes de blocs et ayant été critiquées par leurs utilisateurs;
  3. un manque général de réglementation du fait de la nature décentralisée de la technologie de chaînes de blocs;
  4. un aveuglement dû au battage médiatique entourant cette technologie.

CINQ CHAÎNES DE BLOCS : ETHEREUM, AVALANCHE, CARDANO, HYPERLEDGER ET SOLANA

Dans le cadre du présent projet, nous avons choisi d'évaluer et de comparer cinq chaînes de blocs différentes en tenant compte de points particuliers. Nous avons décidé d'étudier les chaînes de blocs Ethereum, Avalanche, Cardano, Hyperledger et Solana. Ethereum est l'une des chaînes de blocs les plus populaires, même si elle effectue le moins grand nombre de transactions par seconde et présente une consommation d'énergie significative par rapport aux autres options, du fait de son utilisation du mécanisme de preuve de travail. La preuve de travail signifie que la majorité des utilisateurs doivent voter sur chaque nouvelle chaîne de blocs et cela prend davantage de temps et d'efforts que les chaînes de blocs à preuve d'enjeu. Nous avons également inclus Avalanche et Cardano, qui sont toutes deux des chaînes de blocs publiques à preuve d'enjeu. Alors que les répercussions environnementales d'Avalanche sont neutres en carbone, son taux de transactions par seconde est le plus élevé, par rapport aux quatre autres chaînes de blocs analysées. Parallèlement, Cardano est moins écoénergétique et plus lente qu'Avalanche. Nous avons également choisi d'inclure Hyperledger, car il s'agit d'une chaîne de blocs privée utilisant la tolérance pratique au problème des généraux byzantins comme mécanisme de consensus. Il s'agit d'une chaîne de blocs privée; ce qui signifie qu'elle est centralisée. Cela peut influer sur la confiance, puisqu'un moins grand nombre de nœuds peut diminuer la sécurité du réseau. Enfin, nous avons inclus Solana, car il s'agit d'une chaîne de blocs neutre en carbone, qui utilise la preuve d'enjeu et a fourni un rapport sur la consommation d'énergie en la comparant avec des chaînes de blocs comme Ethereum. Toutes les chaînes de blocs résumées ci-dessous présentent des avantages et des inconvénients. À l'issue de leur examen, nous avons décidé d'utiliser Avalanche dans le cadre du présent projet. Avalanche est une chaîne de blocs en source ouverte à preuve d'enjeu présentant le taux de transactions par seconde le plus élevé (4 500). Il s'agit, en outre, d'un réseau public neutre en carbone; considération importante pour nous.

ÉLÉMENTS CLÉES

- Dans le cadre du présent projet, nous avons choisi Avalanche, qui est une chaîne de blocs en source ouverte à preuve d'enjeu présentant le taux de transactions par seconde le plus élevé (4 500).
- Il s'agit d'un réseau public neutre en carbone, résolvant l'une de nos préoccupations susmentionnées en matière de répercussions environnementales.

FIGURE 1:

Aperçu des chaînes de blocs Ethereum, Avalanche, Cardano, Hyperledger et Solana

Points à prendre en considération	Ethereum	Avalanche	Cardano	Hyperledger	Solana
Renseignements généraux	Ethereum est une technologie qui permet d'envoyer de la cryptomonnaie à toute personne moyennant de faibles frais. Elle alimente en outre des applications que tout le monde peut utiliser et que personne ne peut endommager	Avalanche est une plateforme ouverte et programmable de contrats intelligents visant des applications décentralisées.	Cardano est une plateforme de chaîne de blocs à preuve d'enjeu; la première à être fondée sur une recherche revue par les pairs et élaborée au moyen de méthodes fondées sur des données probantes.	Hyperledger est une collaboration mondiale, hébergée par la Fondation Linux et qui comprend des chefs de file en finance, banque, Internet des objets, chaînes d'approvisionnement, fabrication et technologies.	Solana est une chaîne de blocs décentralisée créée pour permettre l'utilisation d'applications évolutives et conviviales dans le monde entier.
Transactions par second	14	4 500	257	3 000	2 295
Mécanisme de consensus	Preuve de travail	Preuve d'enjeu	Preuve d'enjeu	Tolérance au problème pratique des généraux byzantins	Preuve d'enjeu et preuve d'historique
Publique ou privée	Publique	Publique	Publique	Privée	Publique
Répercussions environnementales	Consommation d'énergie significative	Zéro CO2 (carboneutralité)	Efficacité énergétique	Efficacité énergétique	Zéro CO2 (carboneutralité)
Site Web	www.ethereum.org	www.avax.network	www.cardano.org	www.hyperledger.org	www.solana.com

SOLUTION TECHNIQUE

Notre équipe de recherche a conçu une solution qui intègre la technologie de chaîne de blocs à partir des connaissances acquises de notre analyse documentaire et de l'expérience technique préexistante. Cette section présente le système en détail ainsi que la solution recommandée permettant aux utilisateurs d'authentifier des documents téléchargés à partir du site Web de StatCan. Nous allons commencer en présentant trois éléments techniques qui sont les piliers de notre solution : les signatures numériques, les fonctions de hachage et les tunnels sécurisés. Ces trois éléments techniques interagissent comme suit : un condensé numérique (hash) calculé pour le fichier appartenant à StatCan sert à veiller à ce que le fichier ne soit pas modifié; une signature numérique sur ce condensé numérique prouve que le fichier appartient à StatCan; le tunnel sécurisé assure une communication sécurisée entre l'utilisateur et le site Web de StatCan. Dans la présente section, nous expliquons comment ces blocs élémentaires fonctionnent et comment ils sont intégrés aux solutions que nous proposons..

SIGNATURES NUMÉRIQUES

Lorsque les utilisateurs téléchargent un fichier depuis le site Web de StatCan, ils peuvent se poser deux questions. Tout d'abord : les données appartiennent-elles réellement à StatCan? Ensuite, les données ont-elles été modifiées?

QUESTION 1 : LES DONNÉES APPARTIENNENT-ELLES RÉELLEMENT À STATCAN?

Pour répondre à cette question, nous proposons d'avoir recours à une signature numérique. Cette idée est similaire à la signature d'un document au stylo; si vous recevez une lettre ou un document signé(e) par « x »,

vous pouvez vérifier si la signature du document est celle de « x » et si le document est par conséquent bien le sien. Dans un système de signature numérique, une paire de clés privée-publique est utilisée pour signer un document et vérifier la signature par rapport au condensé numérique du document. Un système de signature numérique comprend trois étapes : StatCan doit 1) générer une paire de clés publique-privée; afin 2) de pouvoir signer le condensé numérique du document avec sa clé privée et 3) que tout utilisateur possédant la clé publique puisse vérifier la signature.

1re étape : Génération de la clé

À l'aide d'une fonction de génération de clés, StatCan peut obtenir une paire de clés publique-privée. La clé publique est partagée sur le site Web; les utilisateurs peuvent la télécharger et l'utiliser au cours de la vérification de la signature. StatCan ne partage pas la clé privée, puisqu'un intervenant malveillant pourrait utiliser cette clé privée pour falsifier la signature de StatCan sur les documents. Il est important de noter que la génération de clés est une fonction unidirectionnelle; ce qui signifie qu'il est impossible de calculer la clé privée à partir de la clé publique. StatCan utiliserait sa clé privée pour générer la signature du condensé numérique d'un document plutôt que le document lui-même, puisque cela est plus rapide et plus efficace, et la signature ainsi obtenue est plus courte. On peut considérer que la génération de signature est une fonction demandant à l'utilisateur de fournir sa clé privée et le condensé numérique du document, afin de générer un fichier contenant cette signature

2e étape : Signature du condensé numérique d'un document

Pour créer la signature, StatCan a besoin de sa clé privée et du condensé numérique du document. Il est impossible de calculer une signature pour le condensé numérique d'un document si la clé privée n'est pas connue. La signature créée est conservée dans un fichier distinct. StatCan téléverserait le fichier de signature et sa clé publique sur son site Web, afin que les utilisateurs puissent télécharger 1) le fichier qu'ils souhaitent utiliser, 2) le fichier de signature créé pour le condensé numérique de ce document et 3) la clé publique de StatCan. On peut considérer que la vérification de signature est une fonction demandant à l'utilisateur de fournir les trois fichiers téléchargés depuis le site Web.

3e étape : Vérification d'une signature

Tout utilisateur peut vérifier la validité de la signature en fournissant 1) le fichier qu'il souhaite vérifier, 2) le fichier de signature créé pour le condensé numérique de ce document et 3) la clé publique de StatCan. Si la signature est confirmée, l'utilisateur peut être certain que le fichier appartient réellement à StatCan

ÉLÉMENTS CLÉES

- Une signature numérique est une signature électronique générée et vérifiée par chiffrage de clé publique.
- Dans un système de signature numérique, StatCan doit 1) générer une paire de clés publique-privée; afin 2) de pouvoir signer le condensé numérique du document avec sa clé privée et 3) que tout utilisateur possédant la clé publique puisse vérifier la signature.

COMMENT LES UTILISATEURS PEUVENT-ILS S'ASSURER D'UTILISER UNE CLÉ STATCAN?

L'infrastructure de clés publiques couple les clés publiques à des identités. Cela a lieu par processus d'inscription selon lequel une autorité de certification délivre des certificats en signant la clé publique de StatCan. Ainsi, une autorité de certification vérifie que la clé publique appartient réellement à StatCan. Les autorités de certification sont des entités délivrant des certificats servant à vérifier la propriété d'une clé publique. Tout utilisateur ayant accès à la clé publique de l'autorité de certification peut vérifier le certificat délivré pour la clé publique de StatCan. Ces certificats sont valides pendant une période précise.

FONCTIONS DE HACHAGE

QUESTION 2 : LES DONNÉES ONT-ELLES ÉTÉ MODIFIÉES?

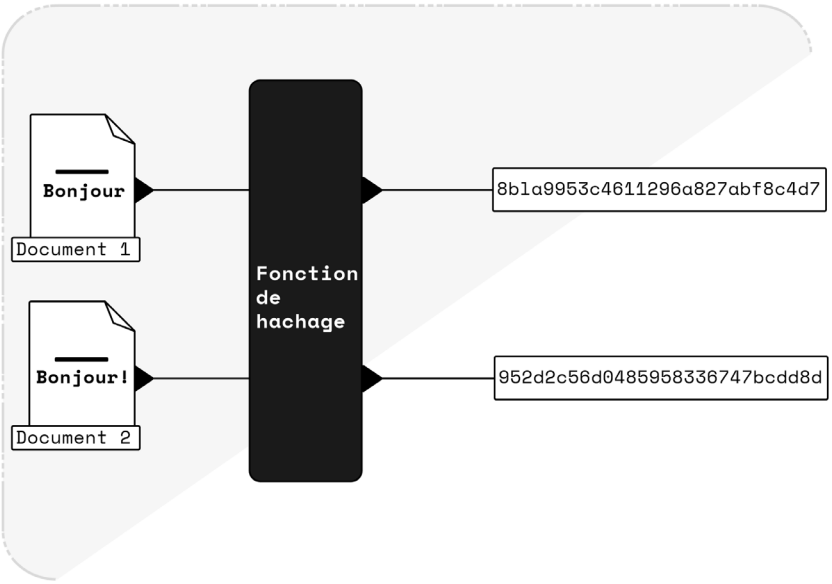
Des fonctions de hachage sont utilisées pour créer une empreinte unique du message d'entrée. Cette technologie fournit à StatCan la capacité de hacher (condenser) un document (tel qu'un fichier .CSV) et d'en créer une « empreinte » unique sous la forme d'un condensé numérique (ou digest) de taille fixe. Après avoir calculé le condensé numérique du fichier, StatCan le téléverse sur le site Web. Lorsque les utilisateurs téléchargent un fichier, le document est haché (ou condensé). Le condensé numérique obtenu est comparé à la valeur téléversée pour vérifier que le fichier n'a pas été modifié. Cette partie du processus est gérée par l'application elle-même. Nous expliquerons cela plus en détail dans les solutions proposées..

ÉLÉMENTS CLÉES

- Le hachage est un terme désignant l'utilisation d'un algorithme, appelé fonction de hachage (ou condensé numérique), pour convertir un renseignement en chaîne de caractères alpha-numériques.

Pour répondre à la préoccupation des utilisateurs relative à l'authentification de leur fichier téléchargé, ainsi que des signatures numériques, nous devons employer des fonctions de hachage dans notre solution. Il s'agit d'une pratique courante en cryptographie, puisque les fonctions de hachage sont réputées être sûres (Al-Kuwari, Davenport et Bradford, 2011). Elles sont utilisées comme protection contre les parties malveillantes qui peuvent essayer de modifier volontairement des données. Utiliser des fonctions de hachage comble une demande dans le système que nous proposons, car l'attaquant ne devrait pas pouvoir créer de fichier doté d'un condensé numérique particulier et le remplacer par un fichier de StatCan. Pour que les fonctions de hachage fonctionnent de façon efficace, elles doivent respecter certaines propriétés. Lorsque deux personnes condensent le même document à l'aide de la même fonction de hachage, par exemple, elles obtiennent la même valeur de condensé numérique. La fonction de hachage produit le même résultat pour un intrant donné (également appelé « préimage"); cela signifie que les fonctions de hachage sont déterministes. Même dans le cas de l'ajout d'une seule lettre à une seule cellule d'un document, le condensé numérique obtenu est différent (voir la figure 2). La propriété de déterminisme est pertinente dans le contexte de deviner la préimage. Une entrée dans la fonction de hachage ne peut pas être calculée en considérant seulement la valeur de hachage. Toutefois, on peut tenter de deviner la préimage, la hacher et la comparer à la valeur de hachage. Considérons l'authentification d'utilisateurs; les mots de passe sont généralement enregistrés sous forme de condensé numérique. Si un attaquant peut accéder à cette base de données de condensés numériques, il peut choisir un mot de passe (l'un des mots de passe les plus couramment utilisés, par exemple), le hacher et le comparer à la base de données pour essayer de trouver une correspondance.

FIGURE 2: Illustration du fonctionnement du hachage



Note : Cette image présente le fonctionnement du hachage. Le document 1 contient le mot « Bonjour » et la fonction de hachage crée le condensé numérique « Hash 1 » pour ce document. Le deuxième document diffère du document 1 d'un caractère : « Bonjour! » La fonction de hachage crée le condensé numérique « Hash 2 » pour le document 2. Les condensés numériques Hash 1 et Hash 2 ont des valeurs différentes, puisque le document 1 et le document 2 sont différents. Les condensés numériques Hash 1 et Hash 2 sont de même taille, puisque la fonction de hachage produit des extrants de taille fixe.

Ce qui est plus pertinent pour notre projet, c'est qu'il est impératif de noter que nous attendons de la fonction de hachage qu'elle possède une propriété de résistance à la collision; c'est-à-dire, qu'il soit impossible de trouver deux messages différents ayant le même condensé numérique. En d'autres termes, un adversaire ne peut pas trouver d'autre fichier .CSV ayant un contenu différent, mais le même condensé numérique que le document initial, et ne peut pas remplacer le document initial par un autre.

Pour assurer une compréhension complète, nous devons également mentionner les deux autres propriétés que devrait présenter une fonction de hachage. Aux fins de clarté, notez qu'un message à hacher est appelé la préimage et le condensé numérique obtenu est appelé l'image. La « résistance à la préimage » signifie que pour

un condensé numérique donné pour un message, il est impossible de trouver un message correspondant. Une « faible résistance à la collision » indique que pour un message donné, il est impossible de trouver un autre message ayant le même condensé numérique. Comme nous l'avons mentionné précédemment, la fonction de hachage est également nécessaire pour l'opération de signature. StatCan signe le condensé numérique du document, plutôt que le document lui-même, afin de créer une signature plus courte. Cela accroît l'efficacité, puisque la signature du condensé numérique est bien plus rapide. Puisque le condensé numérique sert dans la fonction de signature, la propriété de résistance à la collision est nécessaire.

Certaines fonctions de hachage sont bien connues, comme MD 5, SHA1, SHA2 et SHA3. Toutefois, elles ne garantissent pas toutes le même degré de sécurité. MD 5 et SHA1 se sont avérées ne pas fournir une parfaite sécurité, car elles ne sont pas dotées de la propriété de résistance à la collision. Alors qu'il faut plus de temps pour attaquer SHA1 que MD 5, les deux sont actuellement jugées faibles. La sécurité des fonctions de hachage peut ne pas perdurer au fil du temps, mais elles sont remplacées par des versions sécurisées. Pour l'instant, nous savons que SHA2 et SHA3 sont sûres (National Institute of Standards and Technology, 2015). Puisque SHA3 est plus sûre que SHA2, nous proposons d'utiliser SHA3 dans notre solution.

POURQUOI NE PAS UTILISER DE SOMME DE CONTRÔLE OU DES CODES CORRECTEURS D'ERREURS?

- Une somme de contrôle ne devrait-elle pas être utilisée plutôt que des fonctions de hachage? Les sommes de contrôle sont des condensés numériques tronqués. Elles ne sont pas principalement sécurisées et servent à détecter des erreurs aléatoires. Un adversaire peut manipuler des sommes de contrôle pour modifier les données tout en veillant à ce que la somme de contrôle ne change pas. Contrairement aux condensés numériques, il n'est pas difficile de créer des données (comme un fichier) présentant une somme de contrôle particulière. Cette propriété évite la détection des erreurs. Pour ces deux raisons, les sommes de contrôle ne peuvent pas offrir de protection contre les adversaires malveillants.

- Un code correcteur d'erreurs sert à détecter des erreurs au cours de la transmission de données à travers un canal non fiable. Le message est chiffré avec des renseignements redondants. Le destinataire utilise ces renseignements redondants pour détecter un nombre limité d'erreurs. Ces erreurs peuvent être corrigées selon certaines limites. Ces erreurs peuvent être corrigées du côté du destinataire (c.-à-d. la retransmission des données n'est pas nécessaire).

TUNNELS SÉCURISÉS

Les solutions proposées nécessitent un tunnel sécurisé entre l'utilisateur et le site Web de StatCan aux fins de communication. Dans les deux solutions hors ligne et hybrides mentionnées ci-dessous, l'utilisateur doit télécharger une application à partir du site Web de StatCan. L'utilisateur doit veiller à obtenir l'application pertinente; un tunnel sécurisé est nécessaire entre l'utilisateur et StatCan à cette fin. De plus, dans le cas de la solution en ligne, l'utilisateur communique avec le site Web de StatCan au moyen du tunnel sécurisé. Le protocole « Https » fournit un tunnel sécurisé; ce qui signifie que si un attaquant observe le routage dans le tunnel, il ne connaît pas le contenu du message transmis. Tout ce qu'un attaquant peut observer est qu'un routage a lieu entre deux parties.

Le tunnel sécurisé assure :

1. la confidentialité des messages : les messages transmis étant chiffrés, un attaquant ne peut pas les déchiffrer pour en lire le contenu (il sait uniquement que la transmission d'un message a lieu entre deux parties);

2. l'intégrité des messages : un attaquant se trouvant sur le chemin de transmission ne peut pas modifier le routage;

3. l'authentification du serveur : la fin du tunnel est connue et ne mène pas à l'adversaire.

TROIS SOLUTIONS POTENTIELLES

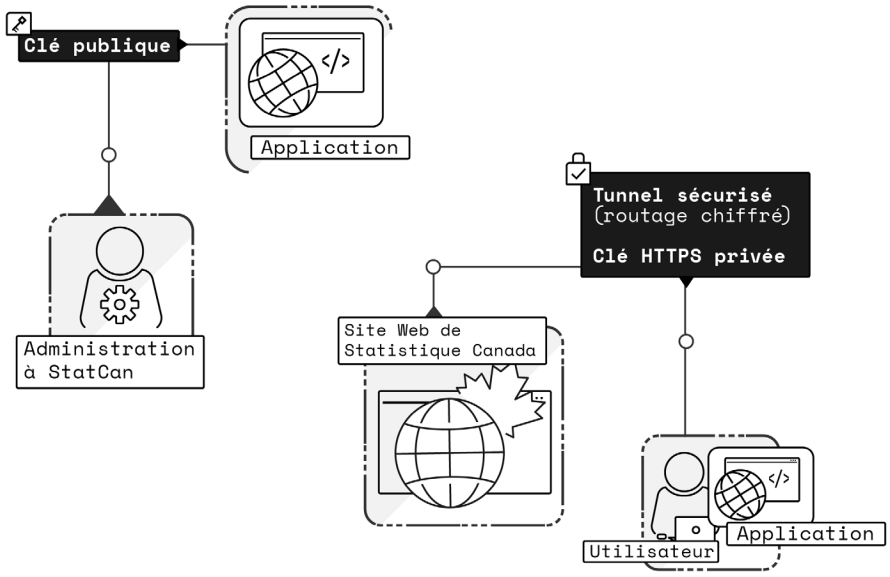
Trois solutions peuvent être mises en œuvre à l'aide de la technologie mentionnée précédemment pour répondre aux besoins des utilisateurs d'authentifier un document de StatCan. Des solutions hors ligne et hybrides nécessitent la création d'une application que télécharge l'utilisateur. Dans le cadre de ces solutions, l'utilisateur interagit avec l'application pour vérifier la validité d'un document.

1. SOLUTION HORS LIGNE

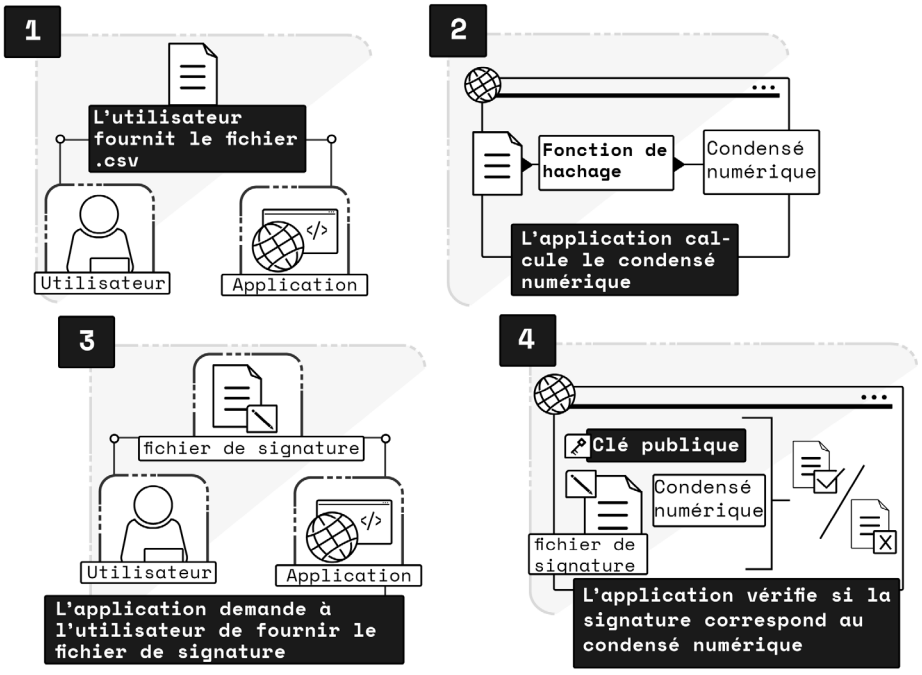
Dans le cadre de cette solution, l'utilisateur télécharge une application depuis le site Web de StatCan au moyen d'un tunnel sécurisé. Cela permet à l'utilisateur de veiller à ce que l'application qu'il télécharge appartienne bien à StatCan. Cette application vise à vérifier la validité du document qui intéresse l'utilisateur. L'utilisateur télécharge, ensemble, le fichier .CSV et le fichier de signature à partir du site Web; il fait glisser le fichier .CSV vers l'application. L'application calcule le condensé numérique pour le fichier, puis demande à l'utilisateur de fournir le fichier de signature correspondant calculé pour le condensé numérique du fichier .CSV. L'application vérifie si la signature correspond au condensé numérique. Pour ce faire, les clés de StatCan doivent être codées en dur dans l'application (phase de configuration à la figure 3). La clé est nécessaire pour vérifier la signature pour un fichier.

FIGURE 3: Illustration de notre solution hors ligne

CONFIGURATION :



UTILISATION :

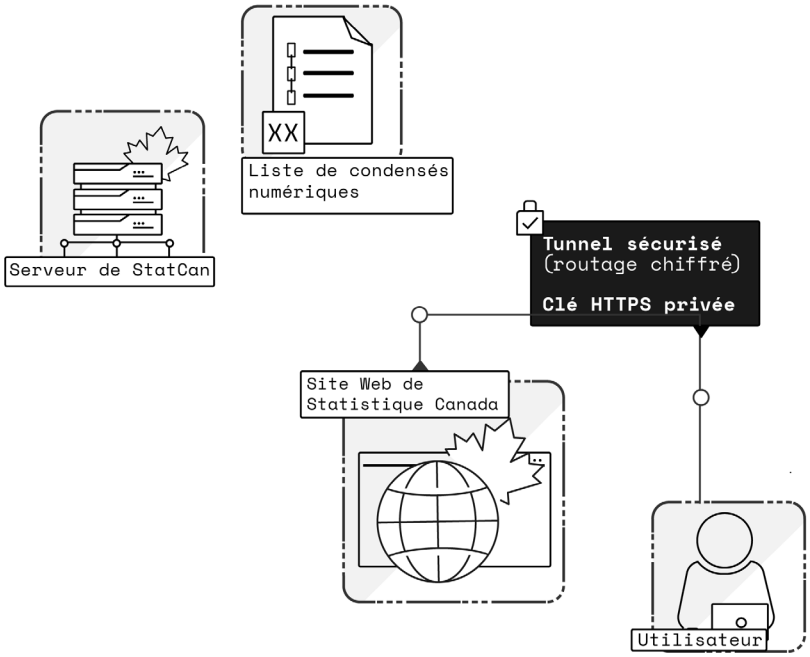


2. SOLUTION EN LIGNE

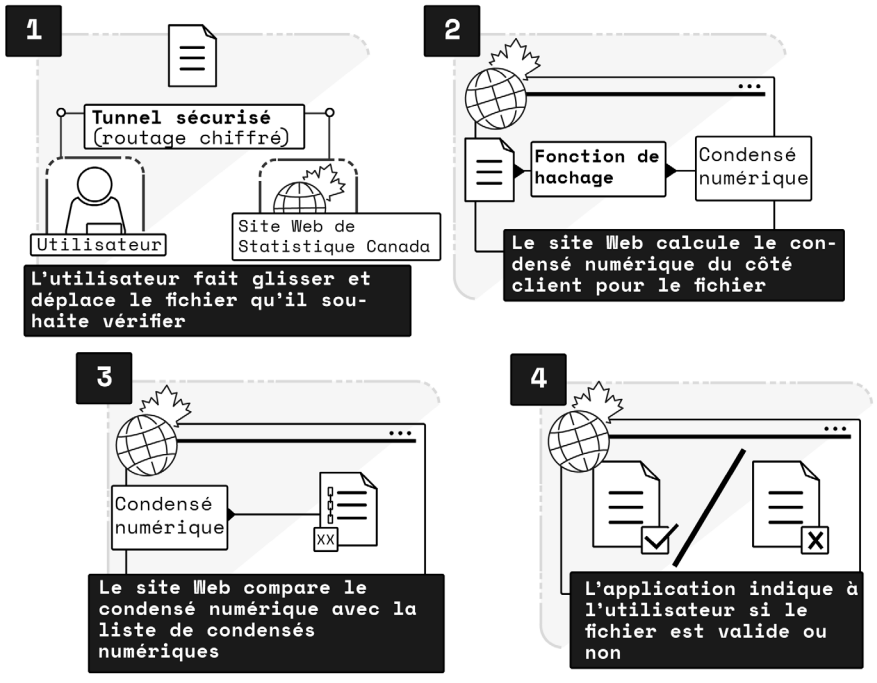
Dans le cadre de cette solution, StatCan maintient à jour une page sur son site Web où l'utilisateur peut vérifier la validité des documents. L'utilisateur communique avec le site Web de StatCan au moyen du tunnel sécurisé; puis y fait glisser le fichier qu'il souhaite vérifier. Puisque le site Web connaît la liste des condensés numériques de tous les fichiers, il peut calculer le condensé numérique du côté client pour le fichier fourni par l'utilisateur et le comparer avec la liste; StatCan maintient à jour un serveur où est conservée la liste de condensés numériques. L'utilisateur peut alors savoir si le fichier téléversé est valide. Si tel est le cas, cela signifie que le fichier n'a pas été modifié et qu'il appartient bien à StatCan. Par rapport à la solution hors ligne, cette approche offre une expérience plus simple à l'utilisateur, puisqu'il doit seulement fournir le fichier du produit. Toutefois, cette solution exige que l'utilisateur soit en ligne, contrairement à l'application mentionnée précédemment qui fonctionne hors ligne.

FIGURE 4: Illustration de notre solution en ligne

CONFIGURATION :



UTILISATION :

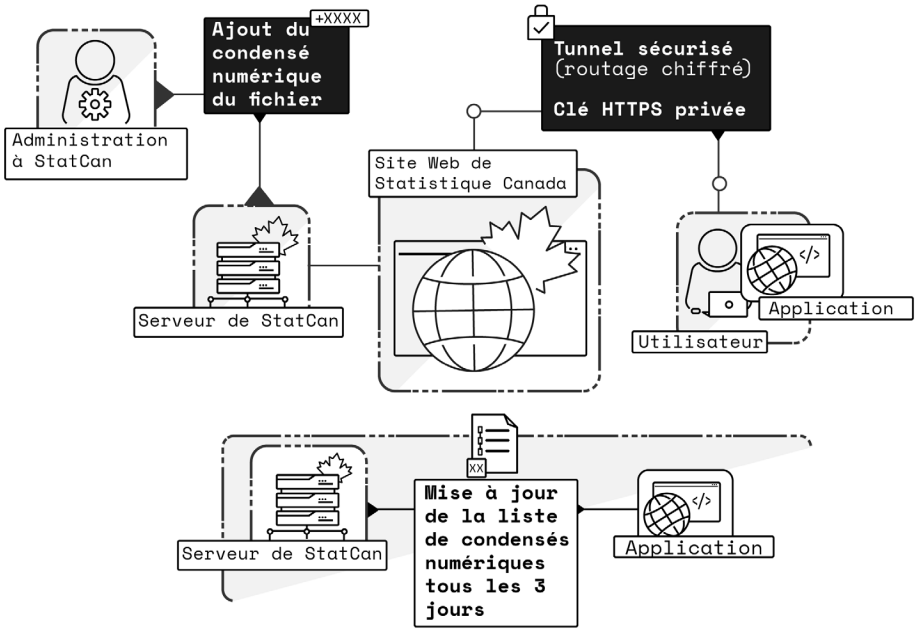


3. SOLUTION HYBRIDE

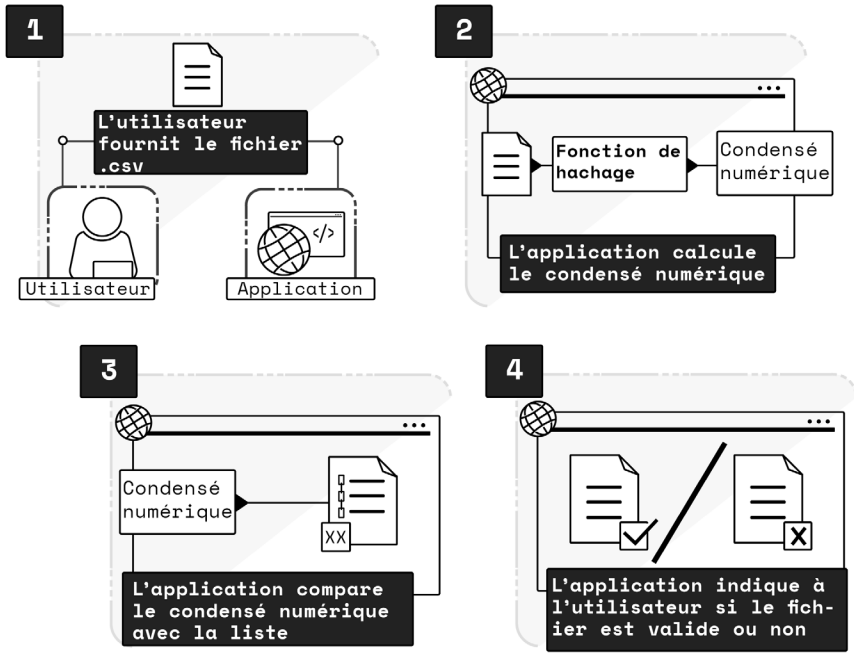
Dans le cadre de la solution hybride, l'utilisateur doit télécharger une application (similaire à la solution hors ligne) au moyen du tunnel sécurisé. L'application contient une liste de condensés numériques de fichiers appartenant à StatCan. Pour authentifier le document, l'utilisateur téléverse le fichier dans l'application, qui calcule le condensé numérique et le compare avec la liste. L'application informe ensuite l'utilisateur de la validité ou non du fichier. L'application se connecte à l'occasion au site Web de StatCan pour mettre à jour la liste de condensés numériques; StatCan maintient à jour un serveur où est conservée cette liste. Alors que nous suggérons que l'application se connecte tous les trois jours, ce délai peut être plus long ou plus court, en fonction de la fréquence de partage de fichiers de StatCan. Tous les trois jours, l'application reçoit la liste mise à jour des condensés numériques conservée sur le serveur, afin de disposer de la liste la plus récente. Une signature pour un condensé numérique prouve la propriété du fichier. Recevoir la liste de condensés numériques par la connexion sécurisée signifie que StatCan est le propriétaire des condensés numériques. Cette solution élimine l'étape de fourniture du fichier de signature, si le condensé numérique du fichier que l'utilisateur présente figure dans la liste de condensés. S'il n'y figure pas, l'application demande à l'utilisateur de fournir le fichier de signature pour le condensé, afin que l'application puisse calculer le condensé et vérifier la signature pour le fichier. Cette situation peut se produire si l'utilisateur tente d'authentifier un fichier avant que l'application n'ait eu l'occasion de se connecter au site Web de StatCan et de mettre à jour la liste de condensés numériques.

FIGURE 5: Illustration de notre solution hybride

CONFIGURATION :



UTILISATION :



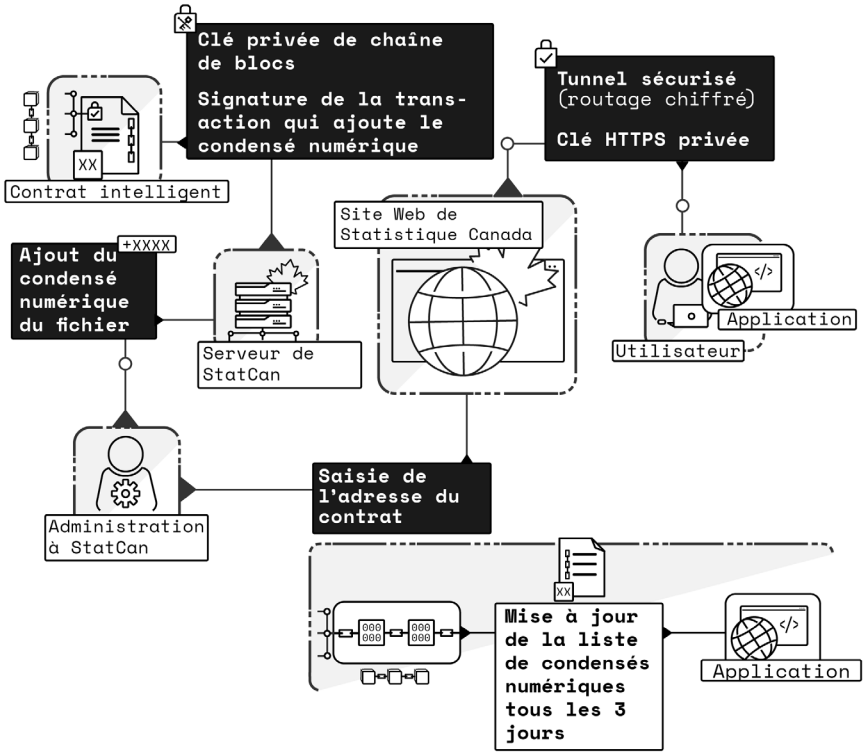
SOLUTION RECOMMANDÉE: HYBRID + CHAÎNE DE BLOCS

Ces trois solutions offrent aux utilisateurs l'occasion d'authentifier des données provenant du site Web de StatCan. Toutefois, elles ne respectent pas toutes de façon égale les normes fixées dans nos objectifs relatifs à ce projet. Alors que la solution hors ligne répond à notre objectif de permettre aux utilisateurs de part et d'autre du fossé numérique d'authentifier des données, elle exige de l'utilisateur qu'il soumette le fichier de signature correspondant dans l'application. Relativement à la solution en ligne, l'utilisateur a uniquement besoin de fournir un fichier .CSV; ce qui réduit au minimum le nombre de téléchargements que doit effectuer l'utilisateur. Par conséquent, la solution en ligne présente une meilleure utilité que la solution hors ligne. La solution en ligne ne respecte en revanche pas l'exigence de fournir une méthode d'authentification accessible, quel que soit l'accès à Internet dont dispose l'utilisateur.

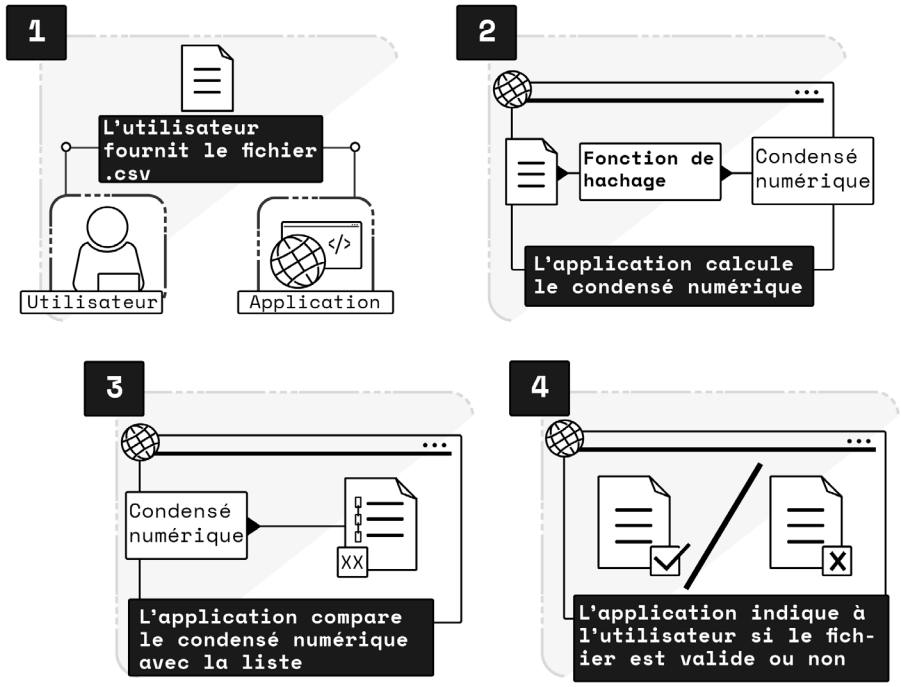
Pour ces raisons, nous avons décidé que la solution hybride était idéale, car elle fournit un niveau d'utilité comparable à la solution en ligne et n'exige pas de l'utilisateur qu'il soit en ligne pour vérifier le fichier souhaité. Cette solution tient donc compte des obstacles dont il a été question ci-dessus quant à un accès constant à Internet. L'ajout de la technologie de chaînes de blocs à la solution hybride fournit des améliorations à une sous-composante de la solution proposée : le stockage du condensé numérique d'un fichier. StatCan crée le condensé numérique d'un fichier et l'inscrit au registre. Par comparaison avec la figure 5, les condensés numériques sont inscrits dans la chaîne de blocs et l'application en reçoit la liste des condensés mise à jour. L'élément

FIGURE 6: Illustration de la solution que nous recommandons

CONFIGURATION :



UTILISATION :



ajouté de la chaîne de blocs accroît la confiance entre StatCan et le public : StatCan ne peut pas modifier les données une fois qu'elles sont publiées. Si StatCan modifie les données, une preuve de cette modification est enregistrée. Un autre avantage d'inclure la technologie de chaînes de blocs est que les condensés numériques sont toujours accessibles, même si le site Web de StatCan est en panne, puisqu'ils sont enregistrés dans la chaîne de blocs. La chaîne de blocs offre également de meilleures propriétés d'archivage, car elle veille à ce que les données enregistrées soient accessibles sur une plus longue période que si les données étaient stockées sur un serveur. Le serveur peut tomber en panne ou ne pas être continuellement tenu à jour, rendant les données inaccessibles. La technologie de chaînes de blocs permet de vérifier la provenance des données (par le condensé numérique du fichier) pendant une longue période, sans pour autant archiver les fichiers. Un éventuel inconvénient d'intégrer une chaîne de blocs à la solution hybride est que StatCan ne peut rien faire si les nœuds de registre manipulent la liste des condensés numériques; c.-à-d. lorsqu'un réseau mondial dispose du contrôle sur les données. Les nœuds de registre sont les entités au sein de ce réseau qui acceptent ou refusent un bloc de transactions en fonction de leur validité; ils diffusent ces transactions afin que tous les nœuds demeurent à jour. Dans la solution hybride sans chaîne de blocs, en revanche, StatCan conserve un contrôle exclusif.

ÉLÉMENTS CLÉES

- La solution que nous recommandons est une solution hybride avec chaîne de blocs.
- Dans la solution hybride avec chaîne de blocs, l'authentification se déroulerait au moyen d'une application que les utilisateurs devront télécharger, tout comme dans la solution hybride. La différence est que la liste de condensés numériques de fichiers serait inscrite dans la chaîne de blocs. Cette liste serait régulièrement mise à jour avec les condensés numériques des nouveaux produits de StatCan. L'authentification d'un fichier se déroulerait comme suit : l'utilisateur devrait téléverser dans l'application le fichier ayant besoin d'être authentifié. Cette action déclencherait le calcul du condensé numérique du fichier par l'application qui le comparerait avec la liste des condensés existants de produits de StatCan. L'application recevrait cette liste de condensés numériques de la chaîne de blocs. L'application informerait ensuite l'utilisateur de la validité du fichier.

ANNEXE A : TERMINOLOGIE

CHAÎNE DE BLOCS

- Système distribué de pair-à-pair permettant de valider, d'horodater et de stocker de façon permanente des transactions dans un registre distribué ayant recours à la cryptographie pour authentifier la propriété d'un actif numérique et son authenticité, et algorithmes de consensus permettant d'ajouter des transactions validées au registre et d'assurer l'intégrité continue de l'historique complet du registre (Lacity, 2018, p. 41).
- La chaîne de blocs est numérique et décentralisée; son objectif est de créer des enregistrements permanents et inaltérables (Treiblmaier, 2018, p. 547).
- Selon A. Welfare (2019), la technologie de chaîne de blocs comprend cinq caractéristiques importantes : la vérité et la confiance, la transparence, la sécurité, la certitude et l'efficacité.
- En informatique, une chaîne de blocs est une séquence d'enregistrements numériques ou « blocs » reliés au moyen de la cryptographie, de sorte que chaque bloc soit vérifiable et virtuellement inaltérable; ce qui est généralement distribué et géré au sein d'un réseau de pair-à-pair (OED, n.d.a).

AUTORITÉ DE CERTIFICATION

- Le Computer Security Resource Center (CSRC) définit une autorité de certification comme étant une entité autorisée à créer, signer, délivrer et révoquer des certificats de clés publiques (s.d.a)

CLÉ PUBLIQUE

- L'Oxford English Dictionary définit une clé publique comme une clé cryptographique pouvant être obtenue et utilisée par quiconque pour chiffrer des messages, de telle sorte que les messages chiffrés puissent être seulement déchiffrés à l'aide d'une deuxième clé « privée » uniquement connue du destinataire (OED, n.d.g).

CODE CORRECTEUR D'ERREURS

- Katz et Dash décrivent les codes correcteurs d'erreurs comme un système de codage qui transmet des messages sous forme de nombres binaires, de telle sorte que le message puisse être récupéré même si certains bits sont inversés par erreur. Ils sont utilisés dans pratiquement tous les cas de transmission de messages, en particulier le stockage de données lorsque ces codes offrent une protection contre la corruption de données (s. d.)

COLLISION

- Le CSRC explique que, dans le contexte de fonctions de hachage, il y a collision lorsque deux intrants distincts ou plus produisent le même extrant (s.d.b)

EMPREINTE D'UN MESSAGE

- L'empreinte d'un message peut désigner la chaîne de bits de longueur fixe que produit une fonction de hachage selon le CSRC (s.d.e) Des synonymes de ce terme sont empreinte numérique, valeur de hachage ou haché (CSRC, s.d.e)

FAIBLE RÉSISTANCE À LA COLLISION

- Hirose définit la faible résistance à la collision comme la probabilité non négligeable de ne pas trouver de collision (2004, p. 88).

GÉNÉRATION DE CLÉ

- Le processus de génération de clé peut se dérouler soit comme un processus simple ayant recours à un générateur de bits aléatoires et à un ensemble de règles approuvées, soit en le créant lors de l'entente ou de la dérivation de clé (CSRC, s.d.d)

HACHAGE

- Le hachage est un terme désignant l'utilisation d'un algorithme, appelé fonction de hachage (ou condensé numérique), pour convertir un renseignement en chaîne de caractères alphanumériques comme celle-ci : e9ffc424b79f4f6ab42d11c81156d3a17228d6b1edf4139be78e948a9332d7d8. Le hachage est une technique couramment utilisée en informatique et en cryptographie (Urban et Pineda, 2018, p. 16).

- La manipulation de fichiers journaux peut s'exprimer de nombreuses façons; les possibilités de reconnaître de telles manipulations varient également grandement. Les mécanismes de vérification de fichiers cherchent à vérifier qu'un fichier n'a pas été modifié. Les techniques de somme de contrôle ou de hachage, par exemple, peuvent permettre de vérifier le contenu, les auteurs ou la propriété numérique (Radinger-Peer et Kolm, 2020, p. 134).
- En informatique, le hachage désigne l'attribution d'une chaîne numérique ou alphanumérique à une donnée, en appliquant une fonction dont les valeurs de résultat ont toutes le même nombre de bits de longueur (OED, n.d.e).

INFRASTRUCTURE DE CLÉS PUBLIQUES

- Le CSRC explique qu'une infrastructure de clés publiques est l'architecture, l'organisation, les techniques, les pratiques et les procédures qui soutiennent collectivement la mise en œuvre et l'exploitation d'un système cryptographique de clés publiques fondé sur des certificats. Cadre établi pour émettre, maintenir à jour et révoquer des certificats de clés publiques (s.d.i)

INTÉGRITÉ D'UN MESSAGE

- L'intégrité d'un message désigne la validité d'un message transmis. L'intégrité d'un message signifie qu'un message n'a pas été modifié ni altéré (PCmag Encyclopedia, s.d.)

JETON NON FONGIBLE (NFT)

- Selon le Merriam-Webster, des jetons non fongibles (NFTs en anglais) sont un identifiant numérique unique ne pouvant pas être copié, substitué ou subdivisé, qui est enregistré dans une chaîne de blocs et utilisé pour certifier l'authenticité et la propriété (p. ex. d'un actif numérique particulier ainsi que les droits particuliers afférents) (s.d.)

NŒUD

- Le CSRC définit un nœud comme étant un système individuel au sein d'un réseau de chaîne de blocs (s.d.f)

PRÉIMAGE

- Le CSRC définit une préimage comme un message X produisant une empreinte numérique de message donnée lors de son traitement par une fonction de hachage (s.d.g)

PREUVE DE TRAVAIL

- Chowdhury explique que la preuve de travail est une mesure économique visant à éviter les attaques de déni de service ou d'autres abus de service (comme le pourriel sur un réseau), exigeant du demandeur de service qu'il effectue une tâche; ce qui signifie généralement du temps de traitement par un ordinateur (2019, p. 56).

PREUVE D'ENJEU

- Chowdhury compare la preuve d'enjeu avec la preuve de travail, en expliquant qu'au lieu de rendre les opérations dispendieuses du fait d'une consommation d'électricité, ce système demande aux mineurs de déposer des pièces que les intervenants malveillants perdraient s'ils essayaient de contourner les règles (2019, p. 19).

PROPRIÉTÉ DE DÉTERMINISME

- Les fonctions de hachage sont toujours de nature déterministe; en effet, la valeur du condensé numérique est purement déterminée par ses intrants et aucun facteur aléatoire ne participe au modèle (Techopedia, 2019). Les fonctions de hachage produisent toujours le même résultat à partir du même intrant (Techopedia, 2019).

PROPRIÉTÉ DE RÉSISTANCE AUX COLLISIONS

- Le CSRC énonce que la propriété de résistance aux collisions est une propriété attendue d'une fonction de hachage cryptographique, selon laquelle il est informatiquement impossible de trouver une collision (s.d.c)

PROVENANCE

- Selon l'Oxford English Dictionary, la provenance est le fait de provenir d'une source en particulier; l'origine, la dérivation; relativement à la notion établie par le domaine des arts, il s'agit de l'historique de propriété d'une œuvre d'art ou d'une antiquité, utilisé comme guide de

l'authenticité ou de la qualité; enregistrement documenté de cela (n.d.f).

- La provenance de données effectue le suivi de l'origine de l'information dans le but d'améliorer la confiance entre les parties intéressées. La provenance de données est une exigence importante pour un éventail d'applications, comme la sécurité alimentaire, la chaîne d'approvisionnement et le traçage de flambées épidémiques. Bon nombre de ces applications sont intrinsèquement distribuées et nécessitent des niveaux élevés de protection de la vie privée et de confiance (Lautert, Pigatto et Gomes 2020, p. 1).
- La provenance est le processus ou les techniques utilisés pour retracer l'origine, identifier l'auteur et déterminer l'historique d'un objet donné. Elle a été initialement utilisée dans le contexte des œuvres d'art pour vérifier qu'un objet a bien été créé par l'auteur annoncé (Lautert, Pigatto et Gomes 2020, p. 1).

RÉSISTANCE À LA PRÉIMAGE

- Cette propriété de fonctions de hachage est définie par le CSRC comme une propriété attendue d'une fonction de hachage cryptographique de telle sorte que, pour une empreinte de message sélectionné aléatoirement (empreinte_message), il est informatiquement impossible de trouver une préimage d'empreinte_message (s.d.h). Voir empreinte de message et préimage pour une plus grande clarté.

SIGNATURE NUMÉRIQUE

- Selon l'Oxford English Dictionary, une signature numérique est une signature électronique générée et vérifiée par chiffrage de clé publique (OED, n.d.c).

SOMME DE CONTRÔLE

- Selon l'Oxford English Dictionary, une somme de contrôle est une somme calculée à partir des chiffres d'un ensemble de données et transmise ou stockée avec les données pour fournir un moyen de vérifier automatiquement toute corruption subséquente (OED, n.d.b)

TECHNOLOGIE DE REGISTRE DISTRIBUÉ

- Un registre est un livre ou cahier demeurant de façon permanente à un certain endroit et généralement utilisé pour enregistrer des transactions commerciales (OED, n.d.d).
- Des plateformes fondées sur la technologie de registre distribué désignent un ensemble de technologies et divers domaines scientifiques (comme l'algèbre et les statistiques) qui, regroupés, permettent le stockage et l'échange de données de façon décentralisée et sécurisée sans qu'un organisme de réglementation central ne soit nécessaire (Lesmes, 2019, s.p.)
- Cette technologie facilite le stockage, le traitement et l'échange de données, permettant des vitesses supérieures de traitement ainsi qu'une transparence et une fiabilité supérieures à celles des anciens systèmes traditionnels (Lesmes, 2019, s.p.)

ANNEXE B : MÉTHODES

MOTS-CLÉS

- Authentication (Authentification)
- Certification
- Verification (Vérification)
- Applied (Appliquée)
- Distributed ledger technology (Technologie de registre distribué)
- DLT
- Cryptography (Cryptographie)
- Data (Données)
- Government (Gouvernement)
- Blockchain (Chaîne de blocs)
- Cryptographic key (Clé cryptographique)
- Hash function (Fonction de hachage)
- Digital signature (Signature numérique)
- Data flow (Flux de données)
- Tool (Outil)
- Checksum (Somme de contrôle)
- Data provenance (Provenance de données)
- Digital fingerprint (Empreinte numérique)
- Data security (Sécurité de données)
- Unique identifiers (Identifiants uniques)
- Error-correcting codes (Codes correcteurs d'erreurs)

RECHERCHES

1. ("Distributed ledger technology") OR (DLT)
2. ("Blockchain") AND ("Authent*) OR (Certif*) OR (Verif*)
3. ("Digital signature")
4. ("Hash function") AND ("Cryptography")
5. ("Government") AND ("Applied") AND ("Cryptographic key")
6. ("Government") AND ("Applied") AND ("Distributed ledger technology") OR ("DLT")
7. ("Government") AND ("Applied") AND ("Digital fingerprint")
8. ("Error-correcting codes") AND ("Applied") NOT ("Algebra")
9. ("Error-correcting codes") AND ("Applied") AND ("Government")
10. ("Checksum") AND ("Verif*) AND ("Applied")
11. ("Data provenance") AND ("Blockchain")
12. ("Data flow") AND ("Data provenance")
13. ("Digital signature") OR ("Digital fingerprint") AND ("Data security")
14. ("Unique identifiers") AND ("Data security")
15. ("Error-correcting codes")

RÉFÉRENCES

Al-Kuwari, S., Davenport, J. H., and Bradford, R. J. (2011). Cryptographic Hash Functions: Recent Design Trends and Security Notions. Short Paper Proceedings of Inscrypt '10, 1–37. Retrieved 2022, from https://eprint.iacr.org/2011/565.pdf.

Aljeaid, D., Ma, X., and Langensiepen, C. (2014). Biometric identity-based cryptography for e-Government environment. Proceedings of 2014 Science and Information Conference, SAI 2014. 581-588. https://doi.org/10.1109/SAI.2014.6918245.

Batista, D., Kim, H., Lemieux, V. L., Stancic, H., and Unnithan, C. (2021). Block and provenance: How a technical system for tracing origins, ownership and authenticity can transform social trust. In V. Lemieux and C. Feng (eds.) Building decentralized trust: Multidisciplinary perspectives on the design of blockchains and distributed ledgers (First ed., pp. 111–128). Springer. https://doi.org/10.1007/978-3-030-54414-0.

Bell, M., Green, A., Sheridan, J., Collomosse, J., Cooper, D., Bui, T., Thereaux, O., & Higgins, J. (2019). Underscoring archival authenticity with blockchain technology. Insights: The UKSG Journal, 32. https://link.gale.com/apps/doc/A594619025/AONE?u=anon~eafb9693&sid=googleScholar&xid=e1544e71

Canada's Public Policy Forum. (2014). Northern Connections: Broadband and Canada's Digital Divide. Public Policy Forum: Reports. Retrieved January 27, 2022, from https://ucarecdn.com/68b98fff-32c9-4904-904c-09b1d98cdd2e/

Chandler, S. (2021, December 22). Proof of stake vs. proof of work: Key differences between these methods of verifying cryptocurrency transactions. Business Insider. https://www.businessinsider.com/personal-finance/proof-of-stake-vs-proof-of-work

Chowdhury, N. (2019). Inside blockchain, Bitcoin, and cryptocurrencies. Auerbach.

Communications Security Establishment Canada. (2021, December 6). Ministers urge Canadian organizations to take action against Ransomware. Canada.ca. Retrieved January 26, 2022, https://www.canada.ca/en/communications-security/news/2021/12/ministers-urge-canadian-organizations-to-take-action-against-ransomware.html

Computer Security Resource Center. (n.d.a). Certification authority. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/certification_authority

Computer Security Resource Center. (n.d.b). Collision. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/collision

Computer Security Resource Center. (n.d.c). Collision resistance. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/collision_resistance

Computer Security Resource Center. (n.d.d). Key generation. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/key_generation

Computer Security Resource Center. (n.d.e). Message digest. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/message_digest

Computer Security Resource Center. (n.d.f). Node. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/node

Computer Security Resource Center. (n.d.g). Preimage. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/preimage

Computer Security Resource Center. (n.d.h). Preimage resistance. In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/preimage_resistance

Computer Security Resource Center. (n.d.i). Public key infrastructure (PKI). In Computer Security Resource Center: Glossary. Retrieved from, https://csrc.nist.gov/glossary/term/public_key_infrastructure.

De Filippi, P. D. F. (2018). Blockchain and the law: The rule of code. Harvard University Press. https://doi.org/10.4159/9780674985933

Hirose, S. (2004). Yet another definition of weak collision resistance and its analysis. In Lim JI., Lee DH. (eds) Information Security and Cryptology - ICISC 2003. ICISC 2003. Lecture Notes in Computer Science, vol. 2971. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24691-6_8

Huang, J., O'Neill, C., and Tabuchi, H. (2021, September 3). Bitcoin uses more electricity than many countries. How is that possible? The New York Times. https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

Industrial Research Assistance Program. (2019). Blockchain publishing prototype. National Research Council of Canada. Government of Canada. https://nrc-cnrc.explorecatena.com/en

Ipsos Public Affairs for Canada's Centre for International Governance Innovation. (2019). Global Survey Internet Security & Trust. CIGI-Ipsos Global Survey Internet Security Trust Part I & II: Internet security, online privacy & trust. Retrieved from, https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%201%20%26%202%20Internet%20Security%2C%20Online%20Privacy%20%26%20Trust.pdf

Jiang, S. (2021, November 9). Discord's hints about crypto, NFTs are tearing its community apart. Kotaku. https://kotaku.com/discords-hints-about-crypto-nfts-are-tearing-its-commu-1848023955

Katz, A., & Dash, S. (n.d.). Error correcting codes. Brilliant Math & Science Wiki. Retrieved January 27, 2022, from https://brilliant.org/wiki/error-correcting-codes/

Kickstarter. (2022). Let's build what's next for crowdfunding creative projects. Kickstarter. https://www.kickstarter.com/articles/lets-build-whats-next-for-crowdfunding-creative-projects?ref=section-homepage-promo-the-future-of-crowdfunding-creative-projects

Lacity, M. (2018). A manager's guide to blockchains for business: From knowing what to knowing how. SB Publishing.

Lautert, F., Pigatto, D. F., and Gomes, L. (2020). A fog architecture for privacy-preserving data provenance using blockchains. Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC). https://doi.org/10.1109/ISCC50000.2020.9219724

Lemieux, V. (2016a). Trusting records: Is Blockchain technology the answer? Records Management Journal, 26(2), 110–139. https://doi.org/10.1108/RMJ-12-2015-0042

Lemieux, V. (2016b). Blockchain for recordkeeping: Help or hype? SSHRC Technical Report, p. 1–31.

Lemieux, V. (2019). Blockchain and public record keeping: Of temples, prisons, and the (re) configuration of power. Frontiers Blockchain, 2, n.p. https://doi.org/10.3389/fbloc.2019.00005

Lesmes, J. (2019). The internet of value: How distributed ledger technologies will reshape the financial services industry (First ed.). O'Reilly Media.

Maull, R., Godsiff, P., Mulligan, C., Brown, A., & Kewell, B. (2017). Distributed ledger technology: Applications and implications. Strategic Change, 26(5), 481–489. https://doi.org/10.1002/jsc.2148

Merriam-Webster. (n.d.). Non-fungible token. In Merriam-Webster.com dictionary. Retrieved January 26, 2022, from https://www.merriam-webster.com/dictionary/non-fungible%20token

Mohamed, K. S. (2020). New frontiers in cryptography: Quantum, blockchain, lightweight, chaotic and DNA (1st ed.). Springer. https://doi.org/10.1007/978-3-030-58996-7

Morse, J. (2021, December 16). Kickstarter said it's moving to the blockchain, and creators are pissed: Decentralized frustration. Mashable. https://mashable.com/article/kickstarter-protocol-blockchain-creator-reaction

National Institute of Standards and Technology. (2015, August 5). NIST releases SHA-3 Cryptographic Hash Standard. NIST: News. Retrieved January 27, 2022, from https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

National Research Council Canada. (2018). Exploring blockchain for better business. Government of Canada. https://nrc.canada.ca/en/stories/exploring-blockchain-better-business

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Oxford English Dictionary. (n.d.a). Blockchain. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.b). Checksum. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.c). Digital Signature. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.d). Distributed Ledger Technology. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.e). Hashing. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.f). Provenance. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

Oxford English Dictionary. (n.d.g). Public Key. In Oxford English Dictionary. Retrieved from https://www-oed-com.proxy.library.carleton.ca

PCmag Encyclopedia. (n.d.). Message Integrity. PCmag. Retrieved January 27, 2022, from https://www.pcmag.com/encyclopedia/term/message-integrity#:~:text=Message%20integrity%20means%20that%20a,been%20tampered%20with%20or%20altered.& text=Integrity%20checking%20is%20one%20component, Parkerian%20Hexad%20and%20data%20integrity.

Pearson, J. (2021, November 11). Discord backs off of crypto after entire internet yells at CEO. Vice. https://www.vice.com/en/article/7kb9dg/discord-backs-off-of-crypto-after-entire-internet-yells-at-ceo

Plunkett, L. (2021, December 17). Kickstarter announces blockchain future, doubles down after users say "no thank you." Kotaku. https://kotaku.com/kickstarter-announces-blockchain-future-doubles-down-a-1848231993

Prathibha, Sona, T. R., & Krishna Priya, J. (2021). Secured Storage and Verification of Documents Using Blockchain Technology. In Transforming Cybersecurity Solutions using Blockchain (pp. 71–90). Springer Singapore. https://doi.org/10.1007/978-981-33-6858-3_5

Radinger-Peer, W. and Kolm, B. (2020). A blockchain-driven approach to fulfill the GDPR recording requirements. In Treiblmaier, H. and Clohessy, T. (Eds.), Blockchain and distributed ledger technology use cases: Applications and lessons learned (pp. 133-148). Springer. https://doi.org/10.1007/978-3-030-44337-5

Ruoti, S., Kaiser, B., Yerukhimovich, A., Clark, J., and Cunningham, R. (2020). Blockchain Technology: What is it good for? Communications of the ACM, 63(1), 46–53. https://doi.org/10.1145/3369752

Solana. (2021, November 24). Solana's energy use report: November 2021. Solana. https://solana.com/news/solana-energy-usage-report-november-2021

Statistics Act, Revised Statutes of Canada (1985, c. S-19). Retrieved from the Justice Laws website: https://laws.justice.gc.ca/eng/acts/S-19/

Statistics Canada. (2018, October 5). Acts and regulations. Statistics Canada. Retrieved January 26, 2022, from https://www.statcan.gc.ca/en/about/frp/frp?MM=as

Statistics Canada. (2021). Departmental Results Report (Catalogue no. 11-628-X). Retrieved from, https://www.statcan.gc.ca/en/about/drr/2020-2021/index

Techopedia. (2019, August 29). What is deterministic algorithm?—definition from Techopedia. Techopedia.com. Retrieved January 28, 2022, from https://www.techopedia.com/definition/18830/deterministic-algorithm

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Management, 23(6), 545–559. https://doi.org/10.1108/SCM-01-2018-0029

Treiblmaier, H., & Clohessy, T. (2020). Preface. In H. Treiblmaier and T. Clohessy (eds.), Blockchain and distributed ledger technology use cases: Applications and lessons learned (1st ed., pp. v-vii). Springer International Publishing. https://doi.org/10.1007/978-3-030-44337-5

Urban, M. C. and Pineda, D. (2018). Inside the black blocks: A policymaker's introduction to blockchain, distributed ledger technology and the "internet of value." Mowat Centre for Policy Innovation, University of Toronto.

Welfare, A. (2019). Commercializing blockchain: Strategic applications in the real world. Wiley.

Xiao, Y. and Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of Planning Education and Research, 39(1), 93–112. https://doi.org/10.1177/0739456X17723971

Zheng, X., Zhu, Y., & Si, X. (2019). A survey on challenges and progresses in blockchain technologies: A performance and security perspective. Applied Sciences, 9(22), 1–24. https://doi.org/10.3390/app9224731