Annexe 1

RAPPORT 1 : REVUE DE LITTÉRATURE

Livrable 1 :

1. Aspects fondamentaux de la technologie de la chaîne de blocs
2. Adéquation de la chaîne de blocs avec le contexte gouvernemental
3. Domaines d'application de la chaîne de blocs dans un contexte gouvernemental

Table des matières

1. Aspects fondamentaux de la technologie de la chaîne de blocs

Dans cette section, nous présentons les aspects fondamentaux de la technologie de la chaîne de blocs. Cette section comprend les définitions, les caractéristiques, le principe de fonctionnement, les types, les générations ainsi que les concepts fondamentaux de la chaîne de blocs, comme le consensus, les contrats intelligents, les applications décentralisées, le portefeuille numérique et la tokenisation.

1.1. Présentation de la technologie de la chaîne de blocs

La chaîne de blocs est définie comme un grand livre public dont toutes les transactions validées sont stockées dans une liste de blocs (Zheng *et al.*, 2017). Chaque bloc stocke un ensemble d'informations composé de données ou transactions horodatées, sécurisées par une cryptographie à clé publique et vérifiées par la communauté du réseau (Seebacher and Schüritz, 2017). Schématiquement, la chaîne de blocs peut être matérialisée comme un ensemble de blocs liés les uns à la suite des autres grâce à un procédé cryptographique (Zheng *et al.*, 2017). En plus de stocker les transactions, chaque bloc contient également l'empreinte du bloc précèdent (sous forme d'un hash) et sa propre empreinte (calculée sur base de l'empreinte du bloc précédent et les informations ou les transactions qu'il contient) formant ainsi une suite de blocs, appelée chaîne de blocs – ou *blockchain* en anglais (cf. figure 1) (Zheng *et al.*, 2017).

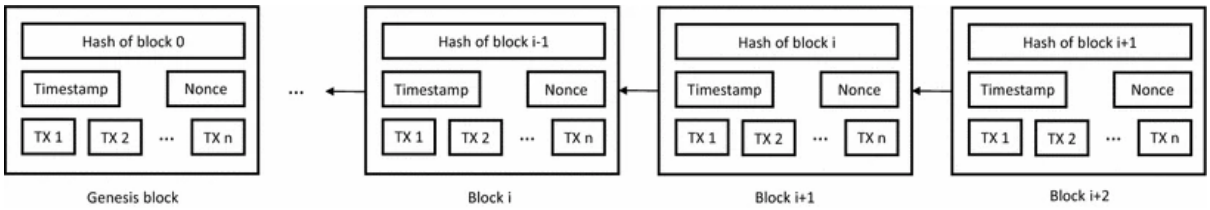

Figure 1. Structure de la chaîne de blocs (Nofer et al. 2017)

La technologie de la chaîne de blocs est également définie comme *« un registre entièrement distribué dans une plate-forme poste à poste qui utilise un protocole de cryptographie avancé pour héberger des applications en toute sécurité* » (Hussien et al., 2019, p. 3, "traduction libre"). Ce registre numérique distribué offre la possibilité d'enregistrer et de partager des informations dans un réseau ou une communauté d'utilisateurs de manière transparente et interrogeable, permettant à tous les membres du réseau d'avoir accès à l'historique de toutes les transactions (Hussien *et al.*, 2019).

Le recours à la cryptographie dans la chaîne de blocs permet de garantir la sécurité et la confidentialité des données (ou transactions) stockées dans la chaîne de blocs étant donné que le contenu des informations stockées dans l'ensemble du réseau est visible et transparent pour tous les utilisateurs (Radanović and Likić, 2018). En effet, la technique de cryptographie utilise

un système à clés publiques et privées qui permet de signer le message, de vérifier l'identité des utilisateurs et l'intégrité des données du réseau sans avoir accès au contenu des données (Roman-Belmonte et al., 2018, Son et al., 2018, Sung and Park, 2021).

D'autres chercheurs définissent la chaîne de blocs comme une plateforme d'échange numérique, où les échanges sont effectués sans impliquer un intermédiaire traditionnel (Pandey and Litoriya, 2020). Ainsi, la technologie de la chaîne de blocs est perçue comme un registre ouvert et distribué qui peut enregistrer les transactions entre deux parties de manière efficace, vérifiable et permanente sans la participation d'une entité intermédiaire (Lakhani and Iansiti, 2017).

1.2.Les caractéristiques de la chaîne de blocs

La technologie de la chaîne de blocs combine à la fois les concepts de cryptographie et des systèmes distribués déjà existants pour garantir l'intégrité des données à travers cinq principales caractéristiques : décentralisation, persistance, anonymat, immuabilité et l'audibilité (Cong et al., 2021, Zheng et al., 2017).

La décentralisation de la chaîne de blocs s'oppose à la centralisation et désigne l'absence d'une entité intermédiaire qui centralise toutes les transactions ou opérations réalisées par les différents membres du réseau de la chaîne de blocs (Zheng *et al.*, 2017). Cette caractéristique suppose également que le registre des transactions de la chaîne de blocs n'est pas tenu par une seule entité du réseau, mais par tous les membres à la fois (Zahed Benisi et al., 2020). En effet, chaque membre du réseau possède une copie validée du registre évitant ainsi le point de défaillance unique, comme c'est le cas dans les systèmes centralisés (Evangelatos et al., 2020, Zahed Benisi et al., 2020). Ceci garantit la sécurité des données du réseau en offrant une protection intrinsèque des données de l'ensemble du réseau. Toutefois, il convient de signaler que la technologie de la chaîne de blocs admet plusieurs niveaux de décentralisation qui permettent de définir les différentes configurations des systèmes de chaîne de blocs (Murray, 2019).

La persistance de la chaîne de blocs désigne l'impossibilité de modifier ou de supprimer les transactions validées de la chaîne de blocs permettant de garantir l'intégrité des données de l'ensemble du réseau (Evangelatos *et al.*, 2020 ; Zheng *et al.*, 2017). Les individus sont généralement susceptibles d'interagir et de traiter avec un système s'ils lui font confiance (Esmaeilzadeh and Mirzaei, 2019). L'intégrité d'un système est donc nécessaire pour répondre aux attentes des utilisateurs et renforcer leur confiance dans le réseau (Hughes et al., 2019). Cette caractéristique permet d'exploiter la chaîne de blocs dans les environnements non

confiants de stockage des données, comme le système de cloud computing, dans lesquels les propriétaires des données ont besoin d'être rassurés de l'intégrité de leurs données stockées chez les prestataires des services cloud (Acquah et al., 2020, Gürsoy et al., 2020, Son et al., 2018) . Le cloud computing est une technologie en ligne qui se caractérise par le service à la demande, ce qui offre la possibilité aux utilisateurs de payer uniquement la quantité de service utilisée (Mayuranathan et al., 2021). Il convient de mentionner que dans les faits, le niveau de persistance est variable d'un type de chaîne de blocs à un autre. Ceci rend possible la modification des données dans un type particulier de la chaîne de blocs.

L'échange des données poste à poste fait référence au fonctionnement *poste à poste* non structuré du réseau chaîne de blocs dans lequel il n'existe ni d'autorité centrale ni de hiérarchie, et où tous les nœuds ont le même statut et peuvent communiquer librement les uns avec les autres (Murray, 2019). Cette configuration du réseau de la chaîne de blocs permet d'éviter d'avoir à la fois des nœuds qui contrôlent le réseau et le point de défaillance unique, car plusieurs nœuds détiennent des copies exactes de la chaîne de blocs complète (Murray, 2019).

L'anonymat dans la chaîne de blocs fait référence à la manière dont les utilisateurs de la chaîne de blocs interagissent avec cette technologie (Zheng *et al.*, 2017). En effet, chaque utilisateur interagit avec la chaîne de blocs en utilisant les adresses générées dans le système, permettant ainsi de masquer l'identité réelle de chaque utilisateur du réseau (Leeming et al., 2019). L'anonymat permet également d'assurer la confidentialité des données sensibles stockées dans la chaîne de blocs, car elle ne donne pas la possibilité aux membres du réseau d'accéder aux identités des propriétaires des données stockées dans le réseau (Zheng *et al.*, 2017). C'est d'ailleurs en se servant de cette caractéristique que certains individus utilisent la technologie chaîne de blocs pour des activités ou transactions illégales. En effet, grâce à l'anonymat offert par la chaîne de blocs les cybercriminels utilisent cette technologie pour demander le versement en cryptomonnaies à travers leurs ransomwares (logiciel informatique malveillant qui prend en otage les données d'un système) (Hussien et al., 2019).

Enfin, l'audibilité est une caractéristique importante de la chaîne de blocs qui permet à chaque membre du réseau de suivre en temps réel toutes les transactions réalisées dans le réseau de la chaîne de blocs (Zheng *et al.*, 2017). Il convient de noter que l'établissement des pistes d'audit des transactions du réseau de la chaîne de blocs a été rendu possible grâce à la persistance de la chaîne de blocs qui prévient toute modification apportée aux données ou aux transactions déjà validées par le réseau de la chaîne de blocs (Upadhyay, 2020).

1.3. Génération des chaînes de blocs

Depuis la première utilisation de la chaîne de blocs dans les cryptomonnaies (version 1.0), cette technologie connaît plusieurs autres cas d'utilisation qui expliquent son passage de la version 1.0 à la version 4.0 (Casino et al., 2019, Zubaydi et al., 2019a, Daraghmi et al., 2019a, Angelis and Ribeiro da Silva, 2019). La chaîne de blocs 1.0 inclut des applications qui permettent uniquement les transactions numériques de cryptomonnaie comme le Bitcoin ou l'Ether (Casino et al., 2019). La chaîne de blocs 2.0 permet l'intégration des contrats intelligents et comprend un ensemble d'applications allant au-delà des transactions de cryptomonnaie (Casino et al. 2019). Dans la version 2.0, la chaîne de blocs est utilisée principalement dans la gestion des actifs et des accords de confiance (Zubaydi et al., 2019b). La chaîne de blocs 3.0 inclut des applications dans des domaines au-delà des deux versions précédentes, tels que l'administration publique, la santé, la science et l'internet des objets (Casino et al., 2019, Xu et al., 2019, Ellervee et al., 2017). La version 3.0 de la chaîne de blocs fait référence aux applications de la chaîne de blocs en dehors des activités économiques, des marchés financiers, du commerce ou de l'argent (Zubaydi et al., 2019b). Enfin, la version 4.0 concerne l'utilisation combinée de la chaîne de blocs et de l'intelligence artificielle (Angelis and Ribeiro da Silva, 2019).

1.4. Types des systèmes de chaîne de blocs

La littérature sur la chaîne de blocs présente trois types ou catégories des systèmes de chaîne de blocs: la chaîne de blocs publique, la chaîne de blocs privée et la chaîne de blocs en consortium (Zahed Benisi *et al.*, 2020).

Dans une chaîne de blocs publique, tout le registre des transactions est visible au public et tout utilisateur peut joindre le réseau (Zheng *et al.*, 2017). Dans ce type de chaîne de blocs, tous les utilisateurs ont le même niveau d'autorité et peuvent y participer au même degré, soit comme mineurs (producteurs des blocs) soit simples utilisateurs (Zahed Benisi *et al.*, 2020). Comme exemples de chaîne de blocs publique, nous citons entre autres le Bitcoin et l'Ethereum (Hussien *et al.*, 2019). Ces deux types de chaînes de blocs sont les plus utilisés dans les différentes applications de la technologie de la chaîne de blocs (Zahed Benisi *et al.*, 2020).

Différemment de la chaîne de blocs publique, la chaîne de blocs privée appartient généralement à une organisation et les autorisations d'accès au registre et de participation au réseau peuvent être publiques ou restreintes (Zahed Benisi *et al.*, 2020). Ce type de chaîne de blocs est considéré comme un réseau centralisé, car elle est entièrement sous le contrôle d'une seule

organisation (Zheng *et al.*, 2017). Dans ce type de chaîne de blocs, nous retrouvons les chaînes de blocs Hyperledger Fabric, et Ripple (Holbl et al., 2018).

Enfin, la chaîne de blocs en consortium désigne un type de chaîne de blocs composé d'un groupe présélectionné de participants (ou organisations) autorisés à participer au processus de consensus lors de la validation des transactions effectuées à l'intérieur du réseau de la chaîne de blocs (Zahed Benisi *et al.*, 2020). La chaîne de blocs en consortium est considérée comme une chaîne de blocs partiellement décentralisée, car seule une partie des utilisateurs du réseau est sélectionnée pour déterminer le consensus dans la validation des transactions du réseau, et les autres utilisateurs participent uniquement pour consulter ou proposer de nouvelles informations à stocker dans le réseau (Zheng *et al.*, 2017).

Les trois types de chaînes de blocs présentés ci-dessus permettent de définir deux principales familles de chaînes de blocs à savoir les chaînes de blocs avec autorisation et les chaînes de blocs sans autorisation. Les chaînes de blocs avec autorisation comprennent les chaînes de blocs privées et en consortium, et les chaînes de blocs sans autorisation comprennent la chaîne de blocs publique (Helliar et al., 2020).

Une chaîne de blocs avec autorisation permet deux types d'accès : public ou privé. L'accès est public lorsque tout utilisateur peut consulter le registre, mais seul un ensemble prédéfini d'utilisateurs peut participer au consensus (Dubovitskaya et al., 2020). L'accès est privé lorsque le droit de consulter le registre est contrôlé au niveau de l'identité des utilisateurs (Dubovitskaya et al., 2020, Esmaeilzadeh and Mirzaei, 2019).

Pour Helliar *et al.* (2020), les chaînes de blocs sans autorisation sont devenues une solution axée sur le marché pour la négociation de devises, et les chaînes de blocs avec autorisation offrent une solution institutionnelle à la conduite des affaires avec une efficacité transactionnelle et une réduction des coûts des transactions. Cette efficacité transactionnelle permet, par exemple, la traçabilité des marchandises dans les chaînes d'approvisionnement mondiales telles que l'industrie alimentaire (Helliar *et al.*, 2020).

Les facteurs d'adoption et les barrières à l'adoption des chaînes de blocs avec autorisation (privées et en consortium) et sans autorisation (publiques) ne sont pas les mêmes et dépendent des besoins des utilisateurs (Wei et al., 2019). Ainsi, les barrières à l'adoption d'un type peuvent constituer les facteurs d'adoption de l'autre type (Helliar *et al.*, 2020). À titre d'exemple, au niveau légal et réglementaire, l'absence des normes universelles pour les chaînes de blocs constitue un obstacle pour l'adoption des chaînes de blocs sans autorisation qui les rendent non interopérables, mais constitue un facteur d'adoption pour les chaînes de blocs avec autorisation,

car les organisations qui adoptent la chaîne de blocs privée ou en consortium peuvent définir leurs propres standards d'échange des données (Helliar *et al.*, 2020).

Le **tableau 1** résume la différence entre les trois types de chaînes de blocs en fonction de six principaux critères à savoir : la détermination du consensus, l'autorisation de lecture du registre, la persistance de la chaîne de blocs, l'efficacité, le caractère centralisé de la chaîne de blocs et enfin, le processus de consensus (Zheng *et al.*, 2017).

Tableau 1. Comparaison des types des chaînes de blocs (public, privé et de consortium)

Propriétés (critères)	**Chaîne de blocs sans autorisation**	**Chaîne de blocs avec autorisation**	
	Chaîne de blocs publique	**Chaîne de blocs en consortium**	**Chaîne de blocs privée**
Détermination du consensus	Tous les nœuds du réseau	Groupe sélectionné des nœuds	Une seule organisation
Autorisation de lecture du registre	Public	Public ou restreint	Public ou restreint
Persistance	Modifications impossibles	Modifications possibles	Modifications possibles
Efficacité	Faible	Élevée	Élevée
Centralisation	Non	Partiel	Oui
Processus de consensus	Sans autorisation	Avec autorisation	Avec autorisation
Exemples	Bitcoin, Ethereum	Hyperledger Fabric, Tendermint, R3 Corda, and Multi-Chain	

Source : Zheng et al. (2017)

1.5. Fonctionnement d'une transaction : algorithmes de consensus

Les algorithmes de consensus sont au cœur du fonctionnement du réseau de la chaîne de blocs (Zheng *et al.*, 2017). Ces algorithmes vérifient et valident les transactions créées par les nœuds du réseau avant d'être ajoutées comme des blocs dans la chaîne de blocs existante (cf. *Figure 4*) (Murray, 2019).

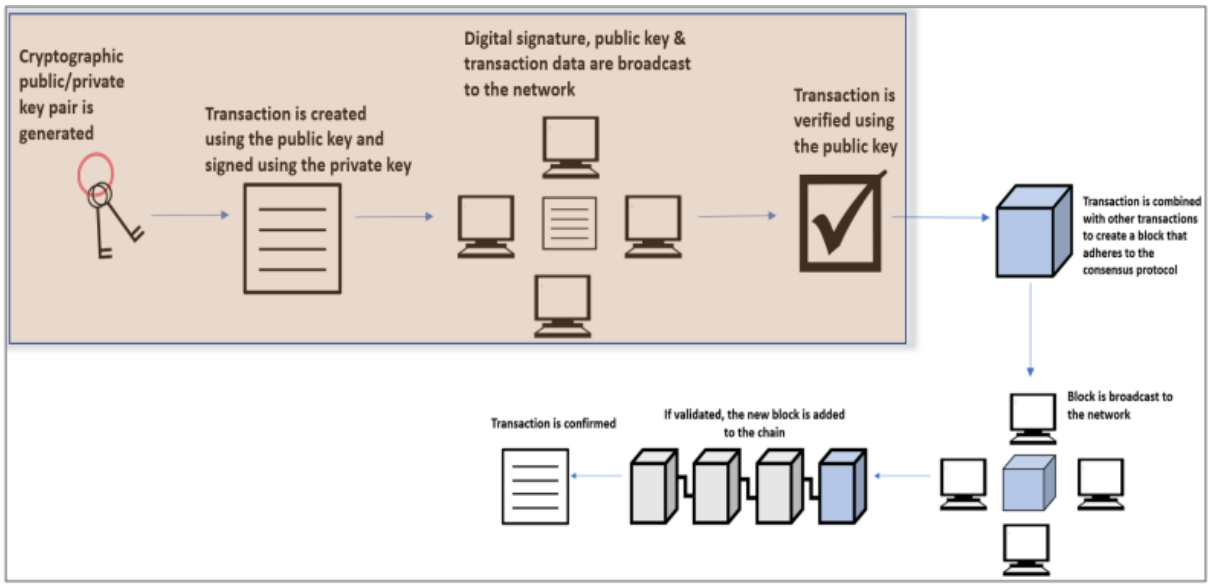

Figure 2. Fonctionnement de la chaîne de blocs (Murray, 2019)

Étant donné le caractère décentralisé et non confiant du réseau de la chaîne de blocs, la validation des transactions se fait grâce aux algorithmes de consensus (Zheng *et al.*, 2017). Ces algorithmes désignent un ensemble de vérifications des transactions réalisées par des nœuds particuliers du réseau chaîne de blocs appelés les mineurs (Zheng *et al.*, 2017). En d'autres termes, les algorithmes de consensus permettent aux différents nœuds du réseau de la chaîne de blocs de se mettre d'accord sur le principe de fonctionnement du réseau en ce qui concerne la création et la validation de nouveaux blocs du réseau chaîne de blocs (Upadhyay, 2020). Il existe plusieurs algorithmes de consensus (Zubaydi *et al.*, 2019), mais les plus utilisés sont la preuve de travail, la preuve d'enjeu, la preuve d'enjeu par délégation (Aste *et al.*, 2017).

La preuve de travail (Proof of Work - en anglais) est l'algorithme de consensus le plus ancien utilisé dans le réseau Bitcoin (Nakamoto, 2008). Cet algorithme de consensus est basé sur la compétition entre les pairs du réseau pour la création de nouveaux blocs de transactions validées du réseau. Pour y arriver, les nœuds doivent faire preuve de la production d'une énorme quantité de travail en résolvant un problème mathématique complexe (Holbl *et al.*, 2018). Comme le montre la *figure 4*, le premier nœud à résoudre ce problème diffuse le bloc créé dans le réseau pour être vérifié par les différents pairs et ajouté dans la chaîne des blocs existante (Holbl *et al.*, 2018). Étant donné que l'algorithme de consensus de la preuve de travail exige une forte consommation d'énergie électrique, à travers la puissance de calcul exigée à tous les mineurs du réseau lors de la création des blocs de transactions valides, il est souvent moins préféré à d'autres algorithmes de consensus (Zheng *et al.*, 2017). Il est important de mentionner que dans l'algorithme de consensus de la preuve de travail, tous les nœuds du réseau sont actifs dans le processus de création de nouveaux blocs valides, car c'est un algorithme qui s'appuie sur la

compétition à créer des blocs valides des transactions (Zheng *et al.*, 2017). Le plus grand désavantage de cet algorithme est sa vulnérabilité à l'attaque par la majorité ou attaque par le 51 %. À travers cette attaque, un nœud qui possède plus de 51 % de la puissance de calcul de tous les nœuds du réseau est capable de falsifier les données déjà stockées dans la chaîne de blocs. L'autre désavantage de cet algorithme concerne l'empreinte écologique causée par la production de la chaleur par les mineurs du réseau pendant la production de nouveaux blocs (Zheng *et al.*, 2017).

La preuve d'enjeu (Proof of Stake - en anglais), différemment de l'algorithme de consensus de la preuve de travail, est basée non pas sur une compétition entre les nœuds du réseau, mais sur le portefeuille en cryptomonnaies des nœuds du réseau (Holbl *et al.*, 2018). En effet, les nœuds du réseau qui possèdent plus de cryptomonnaies dans leur portefeuille ont plus de probabilité d'être sélectionnés comme futurs producteurs de nouveaux blocs des transactions (Holbl *et al.*, 2018). Cet algorithme se base sur le principe selon lequel un nœud qui possède plus de cryptomonnaies dans son portefeuille est moins disposé à tricher dans le réseau (Zheng *et al.*, 2017). Dans ce type d'algorithme, tous les nœuds sont passifs étant donné l'absence de la compétition pour la production de nouveaux blocs des transactions. Chaque nœud du réseau attend tout simplement d'être sélectionné pour la production de nouveaux blocs.

L'algorithme de la preuve d'enjeu existe en plusieurs versions selon le procédé choisi pour sélectionner les futurs producteurs de nouveaux blocs du réseau (Holbl *et al.*, 2018). La preuve d'enjeu par délégation (Delegated Proof of Stake – en anglais) est l'une des versions de la preuve d'enjeu qui repose sur une démocratie représentative (contrairement à l'algorithme de la preuve d'enjeu qui s'appuie sur une démocratie directe) dans laquelle les nœuds du réseau votent à l'unanimité le futur nœud responsable de la production de nouveaux blocs des transactions (Holbl *et al.*, 2018). Dans l'algorithme de la preuve d'enjeu par délégation, les nœuds sont à la fois actifs (ils doivent manifester leur intérêt pour la production de nouveaux blocs) et passifs (ils attendent d'être choisis par les autres nœuds du réseau pour la production de nouveaux blocs).

Le **tableau 2** présente les propriétés des différents algorithmes et les types de chaînes de blocs qui les supportent.

Tableau 2. Comparaison des algorithmes de consensus

Propriétés	**Preuve de travail**	**Preuve d'enjeu**	**Preuve d'enjeu par délégation**
Gestion de l'identité des nœuds	Ouvert	Ouvert	Ouvert
Économie d'énergie	Non	Partiel	Partiel

Exemples d'application	Bitcoin, Ethereum, Litecoin	NXT, Tezos, soon Ethereum, Peercoin	EOS, BitShares

Source : Holbl et al. (2018)

1.6. Contrats intelligents (Smart Contracts)

Une des nouveautés apportées par la chaîne de blocs Ethereum est les contrats intelligents (Zahed Benisi *et al.*, 2020). Le développement des contrats intelligents dans la chaîne de blocs Ethereum a permis d'étendre l'utilisation de la chaîne de blocs dans plusieurs domaines d'activités et d'automatiser certains traitements dans les applications basées sur la chaîne de blocs (Daraghmi et al., 2019b). Par exemple, dans le cas des dossiers de santé électroniques, les contrats intelligents permettent la création des conditions d'accès et d'utilisation des données médicales, de modalités et de règles pour échanger et partager les dossiers médicaux en toute sécurité (Daraghmi *et al.*, 2019).

« Les contrats intelligents sont des contrats auto-exécutables qui se composent d'un groupe de codes définissant les règles régissant les transactions et sont construits sur une plate-forme de cryptomonnaie sous-jacente » (Zahed Benisi et al., 2020, p.4, "traduction libre"). En d'autres termes, les contrats intelligents permettent de figer les règles d'un contrat traditionnel dans la chaîne de blocs et qui doit s'exécuter à chaque fois que les conditions liées aux règles du contrat sont respectées (Evangelatos et al., 2020).

Les contrats intelligents permettent de réduire le niveau d'intervention humaine dans un processus en automatisant certaines tâches (Casino *et al.*, 2019), facilitant ainsi l'augmentation du niveau de désintermédiation dans une transaction (Shermin, 2017). Étant donné que le contrat intelligent est un protocole de transaction informatisé qui exécute les termes d'un contrat (Zheng *et al.*, 2017), il devient maintenant possible d'engager deux parties inconnues dans une transaction basée sur la confiance (Rashideh, 2020).

En plus de l'automatisation des traitements d'un contrat entre deux parties, les contrats intelligents donnent la possibilité à la technologie de la chaîne de blocs d'assurer l'interopérabilité des systèmes autonomes (Khezr et al., 2019). Par exemple, pour faciliter l'interopérabilité entre deux systèmes autonomes à travers la chaîne de blocs, il est nécessaire que les données de ces deux systèmes soient organisées rigoureusement avec des champs prédéfinis. Ensuite, cette vérification des données standardisées est continuellement réalisée par les contrats intelligents pour permettre à ces deux systèmes autonomes de s'échanger des données (Khezr *et al.*, 2019).

Les contrats intelligents sont des codes informatiques figés dans la chaîne de blocs qui peuvent être écrits dans différents langages de programmation dont les plus connus et utilisés sont : Solidity (proche de JavaScript), LLL (proche de Lisp) et Serpent (proche de Python). Parmi ces trois langages de programmation, le langage Solidity est le plus populaire (Dubovitskaya et al., 2020, Solaiman et al., 2020).

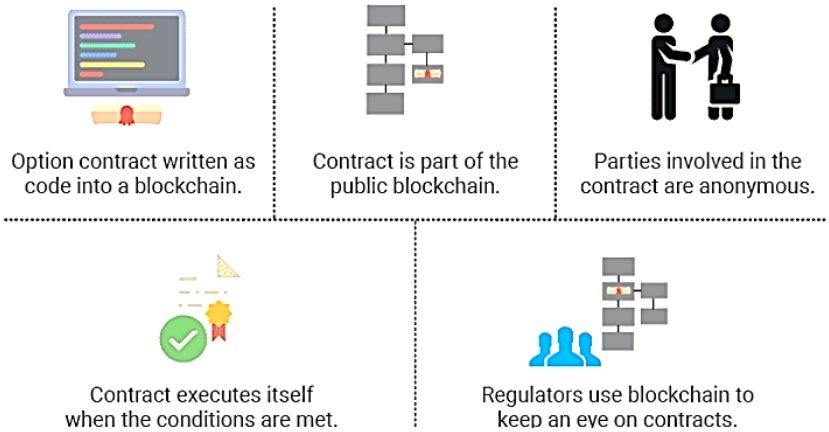

Figure 3. Fonctionnement des contrats intelligents (https://codebrahma.com)

La *figure 5* illustre l'exécution d'un contrat intelligent. Dans l'exécution d'un contrat intelligent, l'événement joue un rôle important étant donné qu'il conditionne l'exécution du contrat. Les termes du contrat signé entre les parties prenantes sont figés dans la chaîne de blocs et à la suite de l'occurrence d'un événement particulier, le contrat intelligent s'exécute automatiquement en faisant les actions initialement définies dans le contrat traditionnel correspondant à l'occurrence de l'événement (Hylock and Zeng, 2019).

1.7. Les applications décentralisées

Une application décentralisée est une application exécutée sur un réseau distribué (Subramanian et al., 2020). Les participants partagent des informations protégées en toute sécurité et les opérations s'exécutent de manière décentralisée à travers les différents nœuds du réseau (Leporcher et al., 2019). Les applications décentralisées, appelées également organisations décentralisées sont les manifestations techniques des contrats intelligents (Leporcher et al., 2019). Dans la littérature, quatre types d'applications décentralisées sont identifiées : Applications décentralisées (Dapp), Organisations Décentralisées (DAO), Entreprises Autonomes Décentralisées (DAC), et Société Autonome Décentralisée (DAS). Ces applications décentralisées sont des contrats intelligents qui se comportent comme des entités à part entière préprogrammées, voire autoprogrammées, réalisant des opérations liées à une chaîne de blocs.

Les applications décentralisées fonctionnent tant que la plate-forme sur laquelle elles sont déployées fonctionne et ne s'active que lorsqu'elles sont appelées et alimentées en tokens ou

cryptomonnaies. Les applications décentralisées possèdent quatre principales propriétés essentielles. Premièrement, elles sont totalement open source et fonctionnent de manière autonome avec aucune contrepartie contrôlant l'essentiel de leurs jetons. Ainsi, ces applications peuvent adapter leurs protocoles en fonction des améliorations proposées et des retours du marché. Deuxièmement, les données et les enregistrements des opérations effectuées par ces applications doivent être cryptés et stockés dans une chaîne de blocs publique et décentralisée. Ceci pour éviter qu'elles soient altérées à la suite d'une défaillance sur le point unique où opèrent ces applications. Troisièmement, les applications décentralisées doivent utiliser un token crypté qui est requis pour y accéder. Toute contribution de valeur faite par les mineurs doit être rémunérée avec des tokens de l'application. Enfin, les applications décentralisées doivent générer des tokens en fonction d'un algorithme de cryptographie standard. Ces tokens sont des preuves qu'un travail ayant une valeur a été effectué sur l'application au niveau d'un nœud donné.

1.8.Portefeuille numérique de cryptomonnaie

Un portefeuille de cryptomonnaie ou « crypto wallet » est un support matériel ou immatériel qui permet de stocker, d'envoyer et de recevoir des cryptomonnaies (Leporcher et al., 2019). Les portefeuilles de cryptomonnaie interagissent avec les chaînes de blocs pour les différentes transactions étant donné que les actifs créés et échangés sur la chaîne de blocs sont numériques[1]. Il ne stocke pas directement la cryptomonnaie d'un utilisateur, qui est enregistrée directement sur la chaîne de blocs publique, mais fournit plutôt une interface permettant de visualiser, de recevoir et d'envoyer les cryptomonnaies[2]. Le portefeuille de cryptomonnaie ne contient pas les cryptomonnaies, mais les clés primaires et publiques nécessaires pour la gestion des actifs numériques stockés sur la chaîne de blocs.

La clé publique du portefeuille représente une adresse électronique composée d'une série de chiffres et de lettres. La valeur de hash cette clé publique représente l'adresse du portefeuille sur la chaîne de blocs et permet de recevoir des paiements provenant d'autres portefeuilles de cryptomonnaie. La clé privée (ou secrète) du portefeuille, quant à elle, permet d'accéder aux

[1] https://www.ig.com/fr/strategies-de-trading/qu_est-ce-qu_un-portefeuille-de-crypto-monnaie--wallet-crypto--e-210917 consulté le 27/02/2022

[2] https://hardbacon.ca/fr/cryptomonnaies/les-meilleurs-portefeuilles-de-cryptomonnaies-pour-les-canadiens/#:~:text=Il%20ne%20stocke%20pas%20directement,peut%2D%C3%AAtre%20bien%20plus%20encore. Consulté le 27/02/2022

fonds conservés dans la chaîne de blocs, de faire des transactions sur le portefeuille et de confirmer les transactions.

En combinant la clé publique et la clé privée, l'utilisateur crée une signature numérique qui interagit avec la chaîne de blocs de différentes cryptomonnaies. Ainsi, grâce au portefeuille numérique, il est possible d'interagir avec la chaîne de blocs sans avoir besoin de télécharger la chaîne de blocs[3]. À ce jour, il existe plusieurs types de portefeuilles de cryptomonnaies utilisés dans différentes chaînes de blocs pour la gestion des actifs numériques stockées sur ces chaînes de blocs. Ces différents types de portefeuilles de cryptomonnaies sont illustrés dans le tableau 3.

Type de portefeuille	**Caractéristiques**	**Avantages/Risques**	**Exemples**
Portefeuille mobile	Application mobile	Facile à utiliser, moins de fonctionnalités, achat en ligne ou physique/ exposé au piratage, vol de smartphone	Jaxx, Edge, Breadwallet, Exodus et Electrum
Portefeuille Desktop	Logiciel sur ordinateur personnel Intermédiaire entre online et offline	Sécurité élevée, restauration possible en cas de défaillance du système/Risque piratage, logiciels malveillants	Electrum, Jaxx, Exode et Wasabi Wallet
Portefeuille en ligne	Stockage cloud	Facile à utiliser, transactions quotidiennes rapides /peu sécurisé (panne serveur ou attaques)	Coinbase, MyEtherWallet, Rahakott et Blockchain.com.
Portefeuille matériel ou physique	Système de stockage hors ligne, stockage sur périphériques de stockage	Facile à utiliser, grande sécurité/ coût élevé et moins pratique pour l'accès rapide aux fonds	Ledger Nano S, Trezor, BitLox et KeepKey
Portefeuille chaud	Stockage en ligne, accès par Smartphone, ordinateur ou tablette connectée à internet	Pratique à utiliser et facile d'accès/Contrôlé par un tiers, vulnérable aux piratages	
Portefeuille froid/ Portefeuille hors ligne	Stockage hors ligne, portefeuille papier ou d'un hardware wallet	Sécurité/ coût élevé, impossible d'utilisation hors ligne	
Portefeuille papier	Impression des clés publiques et les clés privées sous la forme d'un code QR sur un papier	Sécurisé (non exposé aux logiciels malveillants et pirates) / Risque de perte, vol ou dégradation	

[3] https://www.pensezblockchain.ca/portefeuille-numerique-bitcoin consulté le 27/02/2022

Tableau 3. Types de Portefeuilles de cryptomonnaies (https://www.ig.com/fr/strategies-de-trading/qu_est-ce-qu_un-portefeuille-de-crypto-monnaie--wallet-crypto--e-210917)

1.9. La tokenisation

La tokenisation est définie par *Blockchain France* comme « la création de la représentation numérique d'un actif sur une chaîne de blocs » (Blockchain France, 2018). Elle permet l'inscription d'un actif et de ses droits sur un token afin d'en permettre la gestion et l'échange en pair-à-pair sur une chaîne de blocs, de façon instantanée et sécurisée. Un token ou jeton est un concept largement utilisé dans l'écosystème des applications basées sur la chaîne de blocs. Il est défini comme "*un actif numérique émis et échangeable sur une chaîne de blocs*"[4]. Ainsi, dans l'écosystème de la chaîne de blocs, tout actif transférable numériquement entre deux personnes est appelé token (Tönnissen et al., 2020). Ce dernier peut être une cryptomonnaie ou tout autre actif numérique ayant une valeur dans toute application basée sur la chaîne de blocs. Dans l'écosystème des cryptomonnaies, un token désigne une cryptomonnaie basée sur la chaîne de blocs d'une autre cryptomonnaie, contrairement à un coin qui est une cryptomonnaie basée sur sa propre chaîne de blocs (comme le bitcoin-Bitcoin, l'ether-Ethereum, XRP-Ripple, etc.) (Tönnissen et al., 2020). D'autres auteurs définissent le token comme une unité de mesure qui est générée au moment où un calcul a été réalisé par l'intermédiaire d'une machine via une application décentralisée. D'un point de vue technique, la valeur d'un token est tributaire de la difficulté de sa génération, du nombre de tokens actuellement sur le marché ou du potentiel maximal de génération de ces tokens. D'un point de vue du marché, la loi de l'offre et de la demande agit comme une surcouche dans l'établissement de son cours de change avec d'autres cryptomonnaies.

Dans l'écosystème des cryptomonnaies, les tokens sont classés en quatre principaux types : les tokens d'utilité, les tokens de sécurité, les tokens d'actifs et les tokens non fongibles (Blockchain France, 2018). Les tokens d'utilité représentent les tokens achetés auprès d'une entreprise permettant d'accéder à ses services ou produits. Ces tokens permettent à l'entreprise émettrice de lever les fonds pour le développement de son produit et aussi faire fonctionner l'écosystème qui a développé ce token. Les tokens de sécurité représentent des tokens liés à une offre de titres et représentent la propriété légale d'un actif numérique ou physique. En tant que preuve de propriété d'un actif, il est impossible de le modifier ou de le supprimer. Les Tokens d'actifs représentent des actifs numériques qui peuvent être interchangeables, comme les cryptomonnaies (ZDNet, 2022). À l'inverse, les Tokens Non Fongibles (TNF ou Non Fongible

[4] https://www.leblogdudirigeant.com/quest-ce-que-la-tokenisation/ consulté le 27/02/2022

Token-NFT) associés aux actifs numériques représentent des objets physiques ou virtuels auxquels sont rattachés des identités numériques et sur base de leurs caractéristiques intrinsèques ne peuvent pas être interchangeables (ZDNet, 2022). Le TNF constitue ainsi un jeton avec une couche de cryptographie spécifique basée sur une chaîne de blocs ERC (Ethereum Request for Comment). Grâce à ce cryptage unique et aux métadonnées incluses, le jeton peut alors servir de certificat d'identification pour n'importe quel objet digital (une œuvre d'art, un tweet, un objet de jeu vidéo, etc.) (ZDNet, 2022).

2. Adéquation de la chaîne de blocs avec le contexte gouvernemental

Il convient dans cette partie de montrer l'utilité de la technologie chaîne de blocs pour les gouvernements en passant par une brève description du gouvernement électronique et des problèmes généraux rencontrés par les bases de données traditionnelles pour ensuite présenter ses avantages pour les organisations gouvernementales.

2.1. L'e-government et la chaîne de blocs

Le gouvernement électronique (e-government) se définit comme « l'utilisation des technologies de communication électronique pour améliorer les processus démocratiques dans un pays. » (Stoica et al, 2020, p. 5, traduction libre). À ce titre, l'administration en ligne apparait comme l'un des systèmes les plus complexes qui nécessite d'être distribué, sécurisé et qui doit préserver la vie privée. Car l'échec de ces paramètres peut être très coûteux à la fois sur le plan économique et social (Elisa et al., 2018). Raison pour laquelle on note le cas par exemple du Danemark qui a créé une infrastructure centrale de technologies de l'information et de la communication (TIC) pour fournir des services partagés dans des domaines tels que la sécurité des données, le bien-être numérique et les solutions commerciales numériques (Sung & Park, 2021).

Selon Stoica et al. (2020), le (G2C) et le (G2E) sont des composantes du e-government dont les rôles respectifs sont : la modernisation des services publics fournis aux citoyens et l'utilisation des moyens électroniques pour les communications avec les employés du gouvernement ou des applications qui facilitent l'exécution des tâches. À cet égard, on distingue quatre principales composantes qui permettent de décrire le e-government : les interactions « gouvernement et citoyens (G2C) » ; « gouvernement et environnement d'affaires (G2B) » ; « gouvernement et fonctionnaires(G2E) » ainsi que les interactions entre institutions gouvernementales (G2G) (Stoica et al., 2020). Se faisant, on peut déduire que les technologies de l'information (TI) sont d'une importance capitale pour les gouvernements en ce sens qu'elles permettent à l'administration électronique de fournir des services publics aux individus ainsi

qu'aux organisations de manière performante et transparente (Elisa et al., 2018). Par exemple, le développement de l'administration électronique est considéré en Chine comme un élément important de la stratégie nationale d'informatisation (Hou, 2017).

Nombres sont les gouvernements qui sont confrontés de nos jours à de nombreux problèmes et dans divers domaines. Par exemple, à la fin de l'année 2020, la chaîne publique CBC faisait mention des comptes de services gouvernementaux canadiens piratés par des personnes véreuses qui se donnaient le luxe de modifier les informations bancaires de leurs victimes à leur guise (Monde, 2020). En 2015 également, le gouvernement américain avait connu une grande attaque causant la fuite d'informations confidentielles de plus de 4 millions de ses employés y compris la sécurité (Elisa et al., 2018). Par ailleurs, plusieurs problèmes ont été recensés dans de nombreux gouvernements à l'occurrence l'absence dans la gestion administrative, la mauvaise gestion des actifs et des identités numériques des citoyens. (p. ex., Alammary et al., 2019 ; Upadhyay, 2020 ; Carter & Ubacht, 2018 ; Clavin et al., 2020)

De nos jours, les administrations fonctionnent toujours avec des systèmes hypercentralisés qui ne permettent pas à toutes les parties prenantes d'avoir accès à toutes les informations (Alammary et al., 2019). Les vidéos, les images, les documents et d'autres bases de données traditionnelles constituent généralement les applications auxquelles les organisations gouvernementales font recours pour le stockage de leur grande très grande quantité de données. Ce qui ne garantit aucune véritable satisfaction en termes d'intégrité et d'immuabilité (Berryhill et al., 2018). De ce fait, seule une unité organisationnelle a la possibilité de manipuler les informations à sa guise avec des risques élevés de pertes d'intégrité des données (Alammary et al., 2019). C'est ainsi qu'on peut citer les phénomènes de multiples ventes d'actifs immobiliers (titres fonciers), de contentieux électoraux et l'usage de nombreux documents administratifs y compris l'usage des faux diplômes ou actes de naissance (p. ex., Alammary et al., 2019 ; Upadhyay, 2020).

Tout compte fait, les premières recherches sur le gouvernement électronique ont fait allusion à des préoccupations concernant la confidentialité et la sécurité (Warkentin & Orgeron, 2020). Comme le suggérait une enquête de 2003 menée par le Conseil pour l'excellence du gouvernement, il a été noté que la protection de la vie privée et la sécurité étaient des problèmes récurrents dans la recherche sur le commerce électronique et le gouvernement électronique (Warkentin & Orgeron, 2020). Cependant, McPhee et Ljutic (2017) soutiennent par ailleurs que les contrats intelligents et les signatures numériques, qui sont des applications qui utilisent la chaîne de blocs, peuvent contribuer au fonctionnement efficace de divers services du secteur

public tout en assurant l'intégrité des transactions concernées. À cet effet, Ølnes et al. (2017) soutiennent qu'une expérimentation par les gouvernements, de l'application de la chaîne de blocs dans ses propres services lui permettrait de mieux la cerner et de redéfinir ses propres rôles ainsi que ses fonctions dans un environnement institutionnel. Par exemple, les États-Unis d'Amérique utilisent la chaîne de blocs dans les services de santé pour suivre les épidémies de santé publique et pour gérer les identités dans les services publics à travers des agences telles que les douanes américaines et la protection des frontières (Sung & Park, 2021). De même, l'utilisation de cette technologie a également été utile dans le secteur de l'énergie, de l'industrie de la musique ainsi que le stockage des informations et des documents gouvernementaux de haute importance (Sanka et al. 2021; Ølnes et al., 2017).

2.2. Avantages de la chaîne de blocs pour les organisations gouvernementales

Devant la complexité de demandes des services publics, la chaîne de blocs apparaît comme l'une des technologies les plus importantes qui influencera et transformera les entreprises et la société dans les années à venir (Wang et al., 2018). C'est ainsi que le parlement français envisageait déjà en 2018, le lancement de plusieurs projets visant à faire de la France une « Chaîne de blocs Nation ». Tel est le cas par exemple des projets portant sur la chaîne de blocs ainsi que sur le lancement par les administrations et l'expérimentation d'une monnaie numérique émise par une banque centrale de France (Contexte Numérique, 2018). De même, la chaîne de blocs est considérée par le gouvernement chinois comme une solution potentielle pour relever de nombreux défis gouvernementaux, car il s'agit d'une technologie qui est sécurisée contre les attaques en ligne, ses registres pouvant être vérifiés par n'importe qui et elle résiste à toute tentative de falsification de son historique (Hou, 2017).

La structure décentralisée de la chaîne de blocs contribue à garantir une plus grande sécurité des données gouvernementales, car elle réduit leur dépendance vis-à-vis des silos d'informations. De plus, elle limite les risques et les dommages des points de défaillance unique (Cagigas et al., 2021). Contrairement à un réseau d'un système centralisé, la chaîne de blocs ne dispose pas de points de défaillance unique et répond également aux défis de cybersécurité (Jimoh et al., 2019). Par ailleurs, il s'est avéré dans le cadre de l'utilisation des référentiels des données de l'Organisation de Coopération et de développement Economique que la chaîne de blocs regorge plusieurs potentiels qui répondent aux préoccupations sociétales actuelles telles que la transparence, l'accessibilité aux données et l'amélioration de l'efficacité de la prise de décision fondée sur des données probantes de politique (Sicilia & Visvizi, 2018).

Considérée comme l'une des plus grandes caractéristiques de la technologie chaîne de blocs, sinon la plus importante en termes de sécurité (Warkentin & Orgeron, 2020), l'immuabilité permet à cette technologie d'assurer l'intégrité des données ou des informations. En tant que base de données, la possession de cette caractéristique par la chaîne de blocs lui confère une propriété qui la différencie de certaines bases de données dites traditionnelles et utilisables dans le secteur public (Berryhill et al., 2018). Cette immuabilité inhérente de la chaîne de blocs donne aux données enregistrées un caractère d'inviolabilité permettant à tout professionnel de ce secteur et à toute autorité gouvernementale d'approuver lesdites données (Chamola et al., 2020). En effet, il est impossible pour un utilisateur de supprimer une donnée sur la chaîne de blocs une fois que celle-ci est inscrite, contrairement aux autres bases de données existantes (Berryhill et al., 2018). Cependant, fort du constat selon lequel la chaîne de blocs ne permet pas le droit à l'oubli, l'association de la chaîne de blocs avec une base de données externe, donne ainsi lieu à une application hybride qui constitue une solution idéale en termes de confidentialité, de stockage et de partage des données massives des gouvernements (Berryhill et al., 2018).

La conservation des informations communes aux différents services gouvernementaux ainsi que le partage de ces informations entre eux améliorent le succès de l'efficacité des opérations, la transparence, la responsabilité et la prise de décision (Upadhyay, 2020). Sous cette réserve, plusieurs avantages potentiels de la chaîne de blocs ont alors attiré l'attention des gouvernements de nombreux pays pour l'amélioration de la transparence et l'élimination de la corruption (Carter & Ubacht, 2018). À titre d'exemple, la Corée du Sud suit une stratégie de mise en œuvre gouvernementale intelligente qui comprend l'IA et l'analyse de données pour les services axés sur les citoyens et la chaîne de blocs pour l'innovation dans l'administration publique (Sung & Park, 2021). Dans la même lancée, on dénombre plusieurs pays tels que les États-Unis, le Royaume-Uni, les Pays-Bas, les Émirats arabes unis, l'Estonie, la Suède et la Chine, qui ont annoncé des initiatives en matière de chaîne de blocs pour explorer activement ses utilisations dans le secteur public (Carter & Ubacht, 2018).

En plus de la courbe représentative du nombre de projets et d'applications de la chaîne de blocs qui semble croissante au niveau des gouvernements du monde entier, ses propriétés d'immuabilité et de traçabilité font d'elle un élément essentiel en termes d'authenticité, d'efficacité, de sécurité et de transparence dans la gestion des données (Cagigas et al., 2021). Par exemple, une fois l'adoption de la chaîne de blocs effectuée dans les organisations gouvernementales, si l'on considère le cas de la gestion d'un registre donné, on pourrait concevoir le fait que l'ensemble des parties impliquées dans cette gestion se chargerait de consulter le registre à n'importe quel moment étant donné l'égalité de droit d'accès. Ce qui

rendrait ainsi le système de gestion plus transparent. Par ailleurs, l'autorisation ou l'ajout d'une information ou d'une quelconque modification pourrait se faire de manière consensuelle avec toutes les parties concernées. Ce qui donnerait ainsi lieu à une authentification et une mise à jour régulière dudit registre (Gosselin, 2019). L'on pourrait également confirmer cette totale transparence qui est reconnue à la chaîne de blocs à partir de l'utilisation d'une chaîne de blocs sans permission, qui donne l'opportunité à tous ses utilisateurs de consulter toutes les données qui sont enregistrées sur les blocs (Berryhill et al., 2018). En réponse aux nombreuses préoccupations sociétales actuelles, on peut dire que la chaîne de blocs offre de nombreuses opportunités d'amélioration de prise de décision au niveau des organisations gouvernementales à travers ses propriétés de transparence et d'accessibilité aux données (Sicilia & Visvizi, 2018). Donc la chaîne de blocs possède ainsi de nombreuses propriétés qui sont capitales pour la majorité de services publics et surtout pour la tenue de l'enregistrement des registres fonciers (Upadhyay, 2020).

3. Domaines d'application de la chaîne de blocs dans un contexte gouvernemental

La chaîne de blocs est appliquée dans de nombreux domaines parmi lesquels : le foncier, l'éducation, la gestion de la chaîne d'approvisionnement (ou Supply Chain Management), la finance, le vote électronique et la santé.

3.1. Domaine du notariat

Il s'avère que la confiance du public envers les services gouvernementaux est le plus souvent menacée par la corruption (Shang & Price, 2019). Dès lors, la confiance qui est un élément essentiel dans la validité d'un enregistrement de registre foncier trouve un champ favorable avec la technologie de la chaîne de blocs (Bhatia & Wright de Hernandez, 2019). En effet, étant donné qu'il est quasiment impossible de falsifier les documents dans une chaîne de blocs pour des raisons d'immuabilité, la désintermédiation dans les échanges, induite par cette technologie élimine la corruption lorsque la plupart des participants sont honnêtes (Przytarski et al., 2021). À cet égard, la confiance induite qui dérive de la mise en œuvre de cette technologie fait d'elle une base sur laquelle les populations marginalisées et victimes d'abus potentiels du pouvoir institutionnel pourront désormais obtenir des preuves d'authenticité et d'intégrité de leurs dossiers (Bhatia & Wright de Hernandez, 2019). Cette clarté et cette sécurité qui semblent dériver de l'implication de la chaîne de blocs dans la gestion de la propriété foncière sont des facteurs importants dans l'atteinte des objectifs de développement durable, de gestion des cessions de terres et de renforcement d'une justice pour la paix (Thakur et al., 2020). C'est ainsi que la Suède par exemple héberge non seulement des portails d'e-gouvernement qui offrent aux

citoyens un accès numérique à tous les services publics, mais utilise des applications basées sur la chaîne de blocs pour les transactions immobilières et l'enregistrement foncier (Sung & Park, 2021). Donc la gestion et la préservation des informations fiables relatives aux individus, aux organisations, aux actifs et aux activités par les gouvernements peuvent être amplifiées par l'adoption de la chaîne de blocs (Fan et al., 2019). Un autre exemple est celui de la réussite d'un projet d'implémentation de la chaîne de blocs en Géorgie, qui a permis de constater que la chaîne de blocs est une technologie qui peut contribuer à la restauration de la confiance publique dans les agences gouvernementales tout en luttant contre la corruption, la possession illégale des registres fonciers (Shang & Price, 2019).

3.2. Domaine de l'éducation

Malgré le fait que la chaîne de blocs s'accompagne de nombreux défis tels que la sécurité, la confidentialité et l'évolutivité, son adoption dans le secteur de l'éducation est certes à ses balbutiements, mais contribue à l'authentification des certificats académiques et le partage des compétences, des connaissances et des données sécurisées entre les étudiants (Alammary et al., 2019). Ce qui représente de nombreuses réalisations de la chaîne de blocs au niveau académique et sociétal. Par ailleurs, on note qu'en plus de garantir la sécurité et l'immuabilité des certificats que la chaîne de blocs stocke (Grech & Camilleri, 2017) dans ce domaine, les applications de la chaîne de blocs permettent la confidentialité, l'intégrité et la protection des données, facilitent l'authentification de l'identité des étudiants ainsi que leurs certificats numériques, peuvent aider à réduire les coûts inutiles associés aux transactions et au stockage des données, établissent la confiance entre toutes les parties concernées et facilitent la communication entre elles (Alammary et al., 2019). On peut ainsi déduire que la chaîne de blocs peut contribuer à un changement sociétal positif des activités économiques et scientifiques à travers ses fonctionnalités de cryptographie, de sécurité et de son modèle décentralisé (Bdiwi et al., 2017). En effet, il a été soutenu que la chaîne de blocs contribue à la vulgarisation de l'apprentissage diplômante ainsi qu'au renforcement des relations entre les universités et les employeurs (Bandara et al., 2018). C'est dans ce sens que Zheng et al. (2018) affirmeront que : « si nous considérons le processus d'apprentissage et d'enseignement comme la monnaie d'échange, la technologie de la chaîne de blocs peut potentiellement être appliquée au marché de l'éducation en ligne » (Zheng et al., 2018, p. 365, traduction libre).

3.3. Domaine de la gestion de la chaîne d'approvisionnement

Une chaîne d'approvisionnement est « un réseau d'entités dans des secteurs tels que l'agriculture et la fabrication, allant des producteurs, qui produisent un produit ou un service, au consommateur final » (Przytarski et al., 2021). Dans le cas de la gestion de la chaîne

d'approvisionnement, S. S. Kamble et al. (2021) soutiennent que la chaîne de blocs est utilisée dans ce domaine pour offrir le niveau supérieur de traçabilité et de provenance des produits sur la base de l'utilisation d'informations fiables relativement aux autres systèmes. Ce faisant, S. S. Kamble et al. (2021) montrent que l'adoption de la chaîne de blocs dans ce secteur permet à ses utilisateurs d'avoir un avantage concurrentiel. En effet, le fait que toutes les transactions avec chaîne de blocs sont plus sûres, plus transparentes, traçables et efficaces devrait contraindre les gestionnaires de la chaîne d'approvisionnement adopter la chaîne de blocs (Queiroz & Fosso Wamba, 2019). Selon S. S. Kamble et al. (2020), la chaîne de blocs vise par exemple à apporter un changement de paradigme dans la manière dont les transactions sont affectées dans les chaînes d'approvisionnement agricoles. En d'autres termes, son application facilite l'échange transparent d'informations entre les partenaires et les participants dans le contexte de la chaîne d'approvisionnement et permet d'atteindre les objectifs tels que l'intégrité, la confidentialité et la confiance (Upadhyay, 2020). Cependant, compte tenu du fait que l'utilisation de la chaîne de blocs réduit le nombre élevé d'intermédiaires, les retards de paiements et les délais de transaction élevés, elle garantit la traçabilité, l'audibilité, l'immuabilité et la provenance des produits dans ce secteur (Kamble et al., 2020). La chaîne de blocs contribue également à la gestion des droits de propriété intellectuelle, au suivi des pièces imprimées tout au long de son cycle de vie, ainsi qu'à l'amélioration des processus et à la sécurité des données (Kurpjuweit et al., 2021). Par conséquent, l'application de la chaîne de blocs dans ce domaine permet d'améliorer les performances de la chaîne d'approvisionnement (Kamble et al., 2020).

3.4. Le secteur de la finance

Dans le domaine de la finance, Schuetz & Venkatesh (2020) montrent que la chaîne de blocs a pour but de faciliter l'inclusion financière. En effet, grâce à sa base de données distribuée, la chaîne de blocs accélère les règlements, réduit les coûts de transaction, apporte une solution au problème d'inadéquation des produits à l'aide de sa propriété d'immuabilité et fournit un historique financier (Schuetz & Venkatesh, 2020). Par exemple, plusieurs banques à Singapour ont piloté un projet basé sur la chaîne de blocs pour permettre aux titulaires de comptes d'exporter une attestation unique de leurs entités de bonne foi aux institutions financières (Upadhyay, 2020). Dans le secteur des assurances, il a été montré que la confiance, la transparence et la traçabilité accrue sont autant d'avantages que confèrent l'utilisation de la chaîne de blocs (Bakarich et al., 2020).

3.5. Le vote électronique

Le vote est « un processus inhérent à toutes les sociétés démocratiques » (Hsiao et al., 2017). À cet égard, il y va de l'intérêt des gouvernements ou des organisations de mettre sur pied des

stratégies permettant de garantir des élections représentatives non frauduleuses (Moura & Gomes, 2017). En effet, les élections sont « le pilier fondamental d'un système démocratique permettant au grand public d'exprimer ses opinions sous la forme d'un vote » (Khan et al., 2018). C'est ainsi que pour apporter un véritable changement des procédures démocratique au sein des gouvernements, on assiste à un abandon du système de vote par papier pour des systèmes de votes électroniques dans certains pays (Taş & Tanrıöver, 2020). C'est le cas par exemple de l'Estonie qui dans le secteur de l'économie a lancé l'initiative du système de vote électronique donne à ses citoyens actionnaires d'entreprises cotées à la bourse de Tallinn, d'exercer leur droit de vote en ligne en toute sécurité lors des assemblées d'actionnaires (Ojo & Adebayo, 2017).

Certes les systèmes de vote électronique comblent certains défis des votes par papiers, comme la vulnérabilité aux erreurs et à l'exploitation (Hsiao et al., 2017), mais offrent aussi plusieurs avantages parmi lesquels : l'accessibilité des personnes âgées et des personnes handicapées aux élections ainsi que l'utilisation rapide des résultats (Taş & Tanrıöver, 2020). Cependant, la satisfaction de la transparence, le secret du scrutin, l'intégrité et la fiabilité des données sont autant de défis que ces systèmes ne satisfont pas et qui par conséquent impactent la confiance des électeurs (Moura & Gomes, 2017). En effet, propriétaire dès leur conception, ces systèmes de vote électroniques traditionnels sont centralisés. Autrement dit, leur base de code, leur base de données et leur sortie sont contrôlées par un fournisseur qui délivre lui aussi les outils de surveillance (Noizat, 2015). Fort de ce constat, la technologie chaîne de blocs à travers ses propriétés d'immuabilité, de haute disponibilité, de fiabilité, d'audibilité, de confiance des électeurs ainsi que de sa structure décentralisée semble motiver son adoption au niveau des gouvernements tout en comblant la plupart des défis auxquels sont soumis les systèmes de vote électronique non basés sur la chaîne de blocs (Moura & Gomes, 2017).

Tout compte fait, de nombreux avantages sous-tendent l'adoption de la chaîne de blocs par les gouvernements pour la gestion du processus démocratique à travers les élections en effet, le vote électronique basé sur la chaîne de blocs accorde à la fois la transparence et la confidentialité (Taş & Tanrıöver, 2020). Dans ce contexte, les électeurs ne peuvent pas par exemple être identifiés à cause de l'usage des clés privées cryptographiques, les votes individuels étant par ailleurs accessibles au public. Ce qui confère autant de privilège et de sécurité à ce mode de vote électronique contrairement au modèle basé sur les urnes traditionnelles (Kshetri & Voas, 2018). Relativement aux propriétés de la chaîne de blocs, il s'avère que pendant que la transparence et l'immuabilité renforcent l'intégrité des votes,

l'anonymat et la sécurité peuvent être atteints et entretenus par des codages induits par les crypto systèmes à clés publiques (Hsiao et al., 2017).

3.6. Le secteur de la santé

Un dossier de santé électronique est « une technologie de l'information (TI) conçue pour l'automatisation des patients en matière d'autogestion de la santé » (Marsan et al., 2017). L'intégration des dossiers de santé électronique dans le système de santé a fait des soins de santé un domaine très essentiel des technologies de l'information (Hussien et al., 2019). Bien qu'il soit nécessaire, le dossier de santé électronique est un type de TI dont l'adoption par les potentiels utilisateurs en termes de confidentialité des données a connu un manque de confiance envers ses fournisseurs (Marsan et al., 2017). Par ailleurs, le fait que les différentes structures sanitaires ne disposent pas les mêmes données ou informations de santé relatives aux patients transforme l'accès complet à une base de données partagée des patients en une équation quasi impossible à résoudre (Radanović & Likić, 2018). De plus, il s'avère que dans presque tous les domaines de la santé, de nombreux problèmes tels que le manque d'interopérabilité qui résulte des différences structurelles et des acteurs de la santé occasionne des coûts à la fois en termes d'argent et de vies humaines (Dhagarra et al., 2019). En effet, les institutions sont non seulement réticentes en ce qui concerne le partage des données relatives à la vie privée des patients et de plus, en dépit de la complexité des données elles-mêmes, le transfert d'une information au-delà des frontières institutionnelles requière une compréhension commune des structures impliquées (Peterson et al., 2016). En plus de ce problème d'interopérabilité qu'il convient absolument de résoudre, on note également celui du manque d'infrastructure et la confidentialité des données (Dhagarra et al., 2019) dérive de l'absence d'une prise en compte de la nature intime et hautement personnelle de l'information sur la santé (Engelhardt, 2017). Sous cette réserve, il est soutenu que les problèmes de confidentialité des données, d'authentification, d'accessibilité des données, du stockage des données aussi bien des patients que des fournisseurs dans divers domaines du secteur des soins de santé sont résolus par la chaîne de blocs (Hussien et al., 2019). Par exemple, dans le but de sécuriser l'accès et l'intégrité des dossiers de santé publique, le gouvernement estonien en synergie avec les autorités estoniennes de la santé, les citoyens et d'autres entreprises privées a lancé l'initiative de migrer les données gouvernements vers la chaîne de blocs (Ojo & Adebayo, 2017).

Références

Acquah, M. A., Chen, N., Pan, J.-S., Yang, H.-M. & Yan, B. (2020) Securing fingerprint template using blockchain and distributed storage system. Symmetry, 12 (6), 1-15.

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education : A systematic review. Applied Sciences, 9(12), 2400.

Angelis, J. & Ribeiro da Silva, E. (2019) Blockchain adoption: A value driver perspective. Business Horizons, 62 (3), 307-314.

Bakarich, K. M., Castonguay, J. "Jack", & O'Brien, P. E. (2020). The Use of Blockchains to Enhance Sustainability Reporting and Assurance. Accounting Perspectives, 19(4), 389-412.

Bandara, I. B., Ioras, F., & Arraiza, M. P. (2018). The emerging trend of blockchain for validating degree apprenticeship certification in cybersecurity education.

Bdiwi, R., De Runz, C., Faiz, S., & Cherif, A. A. (2017). Towards a new ubiquitous learning environment based on blockchain technology. 101-102.

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains unchaîned : Blockchain technology and its use in the public sector.

Bhatia, S., & Wright de Hernandez, A. (2019). Blockchain is already here. What does that mean for records management and archives? Journal of Archival Organization, 16(1), 75-84.

Blockchain France. (2018) Comprendre la tokenisation. Available https://blockchainfrance.net/2018/05/22/comprendre-la-tokenisation/. (accessed 08/05/2022.

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

Carter, L., & Ubacht, J. (2018). Blockchain applications in government. 1-2.

Casino, F., Dasaklis, T. K. & Patsakis, C. (2019) A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36 (2019), 55-81.

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. Ieee access, 8, 90225-90265.

Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., Erickson, L. C., & Li, J. D. (2020). Blockchains for Government : Use Cases and Challenges. Digit. Gov.: Res. Pract., 1(3). https://doi.org/10.1145/3427097

Cong, L. W., He, Z. & Li, J. (2021) Decentralized mining in centralized pools. The Review of Financial Studies, 34 (3), 1191-1235.

Contexte Numérique. (2018). Les pistes du Parlement pour transformer la France en une « blockchain nation ». https://www.contexte.com/numerique/actualite/95224.html

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

Demestichas, K., Peppes, N., Alexakis, T. & Adamopoulou, E. (2020) Blockchain in Agriculture Traceability Systems: A Review. Applied Sciences-Basel, 10 (12), 1-22.

Dhagarra, D., Goswami, M., Sarma, P., & Choudhury, A. (2019). Big Data and blockchain supported conceptual model for enhanced healthcare coverage : The Indian context. Business Process Management Journal.

Dubovitskaya, A., Novotny, P., Xu, Z. & Wang, F. (2020) Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review. Oncology, 98 (6), 403-411.

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2018). A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Networks, 1-11.

Ellervee, A., Matulevicius, R. & Mayer, N. (2017) A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology. ER Forum/Demos.

Engelhardt, M. A. (2017). Hitching healthcare to the chain : An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10).

Esmaeilzadeh, P. & Mirzaei, T. (2019) The Potential of Blockchain Technology for Health Information Exchange: Experimental Study From Patients' Perspectives. Journal of Medical Internet Research, 21 (6), 1-24.

Evangelatos, N., Özdemir, V. & Brand, A. (2020) Blockchain for Digital Health: Prospects and Challenges. OMICS: A Journal of Integrative Biology, 24 (5), 237-240.

Fan, L., Gil-Garcia, J. R., Song, Y., Cronemberger, F., Hua, G., Werthmuller, D., Burke, G. B., Costello, J., Meyers, B. R., & Hong, X. (2019). Sharing big data using blockchain technologies in local governments : Some technical, organizational and policy considerations. Information Polity, 24(4), 419-435.

Gosselin, F. (2019). Administrations publiques : La chaîne de blocs, une avenue à explorer. Gestion, 44(2), 72-75.

Grech, A., & Camilleri, A. F. (2017). Blockchain in education. Luxembourg: Publications Office of the European Union.

Gürsoy, G., Bjornson, R., Green, M. E. & Gerstein, M. (2020) Using blockchain to log genome dataset access: efficient storage and query. BMC medical genomics, 13 (7), 1-9.

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C. & Veneziani, M. (2020) Permissionless and permissioned blockchain diffusion. International Journal of Information Management, 54 (2020), 1-15.

Holbl, M., Kompara, M., Kamisalic, A. & Zlatolas, L. N. (2018) A Systematic Review of the Use of Blockchain in Healthcare. Symmetry-Basel, 10 (10), 470.

Hou, H. (2017). The application of blockchain technology in E-government in China. 1-4.

Hsiao, J.-H., Tso, R., Chen, C.-M., & Wu, M.-E. (2017). Decentralized E-voting systems based on the blockchain technology. In Advances in Computer Science and Ubiquitous Computing (p. 305-309). Springer.

Hughes, L., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V. & Akella, V. (2019) Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International Journal of Information Management, 49 (2019), 114-129.

Hussien, H. M., Yasin, S. M., Udzir, S., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application : Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of medical systems, 43(10), 1-35.

Hylock, R. H. & Zeng, X. M. (2019) A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. Journal of Medical Internet Research, 21 (8), 1-30.

Jimoh, F. O., Abdullahi, U. G., & Ibrahim, I. A. (2019). An Overview of Blockchain Technology Adoption. Journal of Computer Science, 7(2), 26-36.

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. International Journal of Information Management, 52, 101967.

Kamble, S. S., Gunasekaran, A., Kumar, V., Belhadi, A., & Foropon, C. (2021). A machine learning based approach for predicting blockchain adoption in supply Chain. Technological Forecasting and Social Change, 163(2021), 120465. https://doi.org/10.1016/j.techfore.2020.120465

Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53-62.
Khezr, S., Moniruzzaman, M., Yassine, A. & Benlamri, R. (2019) Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9 (9), 1-28.
Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. Ieee Software, 35(4), 95-99.
Kurpjuweit, S., Schmidt, C. G., Klöckner, M., & Wagner, S. M. (2021). Blockchain in additive manufacturing and its impact on supply chains. Journal of Business Logistics, 42(1), 46-70.
Lakhani, K. R. & Iansiti, M. (2017) The truth about blockchain. Harvard Business Review, 95 (1), 119-127.
Leeming, G., Cunningham, J. & Ainsworth, J. (2019) A Ledger of Me: Personalizing Healthcare Using Blockchain Technology. Frontiers in medicine, 6 (171), 1-10.
Lemieux, V. L. (2016) Trusting records: is Blockchain technology the answer? Records Management Journal, 26 (2), 110-139.
Leporcher, Y.-M., Goujon, F., Chouli, B., Bellanger, M. & Panciatici, O. (2019) Les Blockchains : De la théorie à la pratique, de l'idée à l'implémentation. Editions ENI, Saint-Herblain.
Marsan, J., Audebrand, L. K., Croteau, A.-M., & Magnin, G. (2017). Healthcare service innovation based on information technology : The role of social values alignment. Systemes d'information management, 22(1), 97-127.
Mayuranathan, M., Murugan, M. & Dhanakoti, V. (2021) Enhanced security in cloud applications using emerging blockchain security algorithm. Journal of Ambient Intelligence and Humanized Computing, 12 (7), 6933-6945.
McPhee, C., & Ljutic, A. (2017). Blockchain. Technology Innovation Management Review, 7(10), 3-5.
Monde. (2020). Des comptes de services gouvernementaux canadiens piratés. https://www.24heures.ch/des-comptes-de-services-gouvernementaux-canadiens-pirates-100109328247
Moura, T., & Gomes, A. (2017). Blockchain voting and its effects on election transparency and voter confidence. 574-575.
Murray, M. C. (2019) Tutorial: A Descriptive Introduction to the Blockchain. Communications of the Association for Information Systems, 45 (1), 464-487.
Nofer, M., Gomber, P., Hinz, O. & Schiereck, D. (2017) Blockchain. Business & Information Systems Engineering, 59 (3), 183-187.
Noizat, P. (2015). Blockchain electronic vote. In Handbook of digital currency (p. 453-461). Elsevier.
Ojo, A., & Adebayo, S. (2017). Blockchain as a next generation government information infrastructure : A review of initiatives in D5 countries. Government 3.0–Next Generation Government Technology Infrastructure and Services, 283-298.
Ølnes, S., Ubacht, J., & Janssen, M. (2017a). Blockchain in government : Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly, 34, 355-364.
Pandey, P. & Litoriya, R. (2020) Securing and authenticating healthcare records through blockchain technology. Cryptologia, 44 (4), 341-356.
Peterson, K. J., Deeduvanu, R., Kanjamala, P., & Mayo, K. B. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.
Przytarski, D., Stach, C., Gritti, C., & Mitschang, B. (2021). Query Processing in Blockchain Systems : Current State and Future Challenges. Future Internet, 14(1), 1.

Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain : An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46(2019), 70-82. https://doi.org/10.1016/j.ijinfomgt.2018.11.021

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

Rashideh, W. (2020) Blockchain technology framework: Current and future perspectives for the tourism industry. Tourism Management, 80 (2020), 1-13.

Roman-Belmonte, J. M., De la Corte-Rodriguez, H. & Rodriguez-Merchan, E. C. (2018) How blockchain technology can change medicine. Postgraduate medicine, 130 (4), 420-427.

Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology : Adoptions, applications, challenges and future research. Computer Communications, 169, 179-202.

Schuetz, S., & Venkatesh, V. (2020). Blockchain, adoption, and financial inclusion in India : Research opportunities. International Journal of Information Management, 52, 101936.

Seebacher, S. & Schüritz, R. (2017) Blockchain technology as an enabler of service systems: A structured literature review. International conference on exploring services science. Springer.

Shang, Q., & Price, A. (2019). A blockchain-based land titling project in the Republic of Georgia : Rebuilding public trust and lessons for future pilot projects. Innovations: Technology, Governance, Globalization, 12(3-4), 72-78.

Shermin, V. (2017) Disrupting governance with blockchains and smart contracts. Strategic Change, 26 (5), 499-509.

Sicilia, M.-Á., & Visvizi, A. (2018). Blockchain and OECD data repositories : Opportunities and policymaking implications. Library hi tech.

Solaiman, E., Wike, T. & Sfyrakis, I. (2020) Implementation and evaluation of smart contracts using a hybrid on- and off-blockchain architecture. Concurrency and Computation: Practice and Experience, 33 (2020), 1-17

Son, K. T., Thang, N. T., Do, L. P. & Dong, T. M. (2018) Application of blockchain technology to guarantee the integrity and transparency of documents. International Journal of Computer Science and Network Security, 18 (12), 7-15.

Stoica, M., Ghilic-Micu, B., Mircea, M., & Sinioros, P. (2020). E-Government in a New Technological Ecosystem. Informatica Economica, 24(3), 5-15.

Subramanian, H. C., Cousins, K. C., Bouayad, L., Sheth, A., Conway, D., Salcedo, E. & Pineda, J. (2020) Blockchain Regulations and Decentralized Applications: Panel Report from AMCIS 2018. Communications of the Association for Information Systems, 47 (9), 189-206.

Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management, 34(5), 1481-1505. https://doi.org/10.1108/JEIM-12-2020-0532

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328.

Thakur, V., Doja, M., Dwivedi, Y. K., Ahmad, T., & Khadanga, G. (2020). Land records on blockchain for implementation of land titling in India. International Journal of Information Management, 52, 101940.

Tönnissen, S., Beinke Jan, H. & Teuteberg, F. (2020) Understanding token-based ecosystems – a taxonomy of blockchain-based business models of start-ups. Electronic Markets, 30 (2), 307-323.

Upadhyay, N. (2020) Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, 54 (2020), 1-26.

Wang, L., Luo, X. R., & Xue, B. (2018). Too good to be true ? Understanding how blockchain revolutionizes loyalty programs. Twenty-fourth Americas Conference on Information Systems, New Orleans, 16-18.

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52(2020), 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Wei, J., Wulan, B., Yan, J., Sun, M. & Jing, H. (2019) The Adoption of Blockchain Technologies in Data Sharing: A State of the Art Survey. Univ Calgary Press, Calgary.

Xu, J., Xue, K. P., Li, S. H., Tian, H. Y., Hong, J. A., Hong, P. L. & Yu, N. H. (2019) Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data. IEEE Internet of Things Journal, 6 (5), 8770-8781.

Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H. & Vasilakos, A. V. (2019b) Designing blockchain-based applications a case study for imported product traceability. Future Generation Computer Systems, 92 (2019), 399-406

Zahed Benisi, N., Aminian, M. & Javadi, B. (2020) Blockchain-based decentralized storage networks: A survey. Journal of Network and Computer Applications, 162 (2020), 1-10.

ZDNet. (2022) NFT : Tokens non fongible, la nouvelle lubie de la blockchain. Available https://www.zdnet.fr/pratique/nft-tokens-non-fongible-la-nouvelle-lubie-de-la-blockchain-39919709.htm#:~:text=L'une%20des%20sp%C3%A9cificit%C3%A9s%20de,ne%20les%20distingue%20entre%20eux. (accessed 19/03/2022.

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

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

Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M. & Karuppayah, S. (2019) A Review on the Role of Blockchain Technology in the Healthcare Domain. Electronics, 8 (6), 1-29.