Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1407

(01/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité de la technologie des registres distribués (DLT)

Exigences de sécurité applicables au service de vérification de l'intégrité numérique basé sur la technologie des registres distribués

Recommandation UIT-T X.1407

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	**X.1400–X.1429**
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1407

Exigences de sécurité applicables au service de vérification de l'intégrité numérique basé sur la technologie des registres distribués

Résumé

La Recommandation UIT-T X.1407 indique les menaces et les exigences de sécurité en ce qui concerne la vérification de l'intégrité numérique basée sur la technologie des registres distribués (DLT).

La preuve originale protégée est stockée en dehors de la chaîne. Les valeurs de données hachées sont stockées dans la chaîne. La Recommandation UIT-T X.1407 permet d'analyser les menaces de sécurité qui pèsent sur les services de vérification de l'intégrité numérique basés sur les technologies DLT, notamment pour ce qui concerne l'enregistrement de la preuve et la provenance de la preuve. Cette Recommandation décrit en outre les exigences de sécurité permettant de contrer les menaces pour la sécurité.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1407	07-01-2022	17	11.1002/1000/14800

Mots clés

Vérification de l'intégrité numérique, technologies des registres distribués, menaces et exigences de sécurité

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1407

Exigences de sécurité applicables au service de vérification de l'intégrité numérique basé sur la technologie des registres distribués

1 Domaine d'application

La présente Recommandation définit les menaces et les exigences de sécurité applicables à la vérification numérique de l'intégrité d'une entité sur la base de la technologie des registres distribués (DLT). La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT fournit des services de distribution, d'interrogation et de suivi d'une preuve numérique de l'intégrité d'une entité en s'appuyant sur les technologies des registres distribués.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

[UIT-T X.1401] Recommandation UIT-T X.1401 (2019), *Menaces de sécurité pour la technologie des registres distribués*.

[UIT-T X.1402] Recommandation UIT-T X.1402 (2020), *Cadre de sécurité pour la technologie des registres distribués*.

[UIT-T X.1404] Recommandation UIT-T X.1404 (2020), *Garantie de sécurité pour la technologie des registres distribués*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants, définis dans le paragraphe 1.4 de la norme [b-ISO 23257] et ailleurs:

3.1.1 registre distribué [b-UIT-T X.1400]: type de registre qui est partagé, dupliqué et synchronisé de manière distribuée et décentralisée.

3.1.2 technologie des registres distribués (DLT) [b-ISO 22739]: technologie permettant d'exploiter et d'utiliser des registres distribués.

3.1.3 plate-forme de technologie des registres distribués [b-ISO 22739]: ensemble d'entités de traitement, de stockage et de communication qui assurent ensemble les fonctions du système DLT sur chaque nœud DLT.

3.1.4 intégrité [b-ISO 13491-2]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.5 registre [b-UIT-T X.1400]: mémoire d'informations contenant des relevés de transactions finals et définitifs (inaltérables).

3.1.6 contrat intelligent [b-ISO 22739]: programme informatique stocké dans un système DLT au sein duquel le résultat d'une exécution du programme est enregistré sur le registre distribué.

3.1.7 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.2 Termes définis dans la présente Recommandation

Néant.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DDoS déni de service réparti (*distributed denial of service*)

DLT technologie des registres distribués (*distributed ledger technology*)

PoS preuve d'enjeu (*proof of stake*)

PoW preuve de travail (*proof of work*)

PBFT tolérance de panne byzantine pratique (*practical byzantine fault tolerance*)

5 Conventions

La présente Recommandation emploie les formes des verbes ci-après lors de la formulation des dispositions:

a) "doit" désigne une obligation;

b) "devrait" désigne une recommandation;

c) "pourra" désigne une permission;

d) "peut" désigne une possibilité et une capacité.

6 Aperçu

Il est difficile de prouver l'intégrité des données lorsque celles-ci sont réparties entre différents systèmes. De plus, le processus de vérification de l'intégrité peut nécessiter des recherches dans un grand nombre de base de données ou de systèmes, ou des recherches manuelles dans des documents papier. Cette situation s'explique par l'absence d'historique complet des transactions, qui pourrait entraîner des retards, des démarches et des frais supplémentaires, et de mauvaises décisions. La technologie DLT se compose de registres inviolables et décentralisés. Sa fiabilité est telle qu'elle ne nécessite pas de recourir à des intermédiaires dans le cadre de l'échange de valeur. Elle repose sur des bases de données décentralisées qui fournissent des relevés authentiques, collaboratifs, transparents, vérifiables et contrôlables pour toutes les transactions. Ainsi, la fonction de traçabilité et l'inviolabilité de la technologie DLT permettent de parvenir à une solution de vérification de l'intégrité numérique qui empêche de falsifier ou de compromettre les données d'origine grâce à un système de détection des modifications.

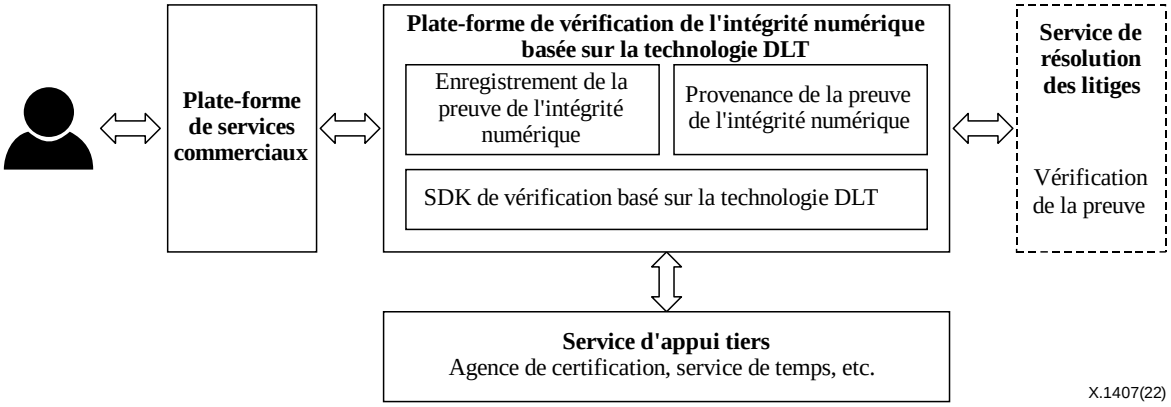

Figure 1 – Illustration de la vérification de l'intégrité numérique basée sur la technologie DLT

Les scénarios de base sur des plates-formes de vérification de l'intégrité numérique fondée sur la technologie DLT incluent l'enregistrement de la preuve et la provenance de la preuve. L'utilisateur sur la plate-forme de services commerciaux demande à vérifier une preuve numérique, enregistre la preuve sur le registre DLT et stocke la hachure de la signature numérique extraite au sein du contrat d'enregistrement de la preuve de l'intégrité numérique. Le processus de vérification de l'intégrité de la preuve repose sur la vérification de la valeur de hachage de la preuve et sur la comparaison entre cette valeur de hachage et les hachures stockées sur le registre DLT. De plus, afin de garantir l'utilisation légale d'une preuve numérique et de protéger les droits des utilisateurs, un service d'interrogation et de vérification de preuve numérique est fourni dans le domaine de la criminalistique pour les litiges en ligne.

Bien que la fonction de traçabilité et l'inviolabilité des registres DLT permettent de mieux contrôler et exploiter l'intégrité des relevés, des menaces pèsent sur l'utilisation de la technologie DLT. Certaines visent les utilisateurs, d'autres les preuves numériques ou encore les processus d'enregistrement et de provenance des preuves. Par conséquent, il est nécessaire et utile de récapituler les menaces de sécurité dans différentes catégories sur la base des analyses des activités menées dans le cadre de la vérification de l'intégrité numérique basée sur la technologie DLT. L'analyse de ces menaces aboutit à la définition d'un ensemble d'exigences de sécurité.

7 Parties prenantes et processus associés à la vérification de l'intégrité numérique basée sur la technologie DLT

7.1 Parties prenantes

7.1.1 Parties prenantes internes

Les parties prenantes internes devraient regrouper:

a) L'utilisateur.

b) La plate-forme de services commerciaux.

c) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT.

7.1.2 Parties prenantes externes

Les parties prenantes externes regroupent:

a) Les services d'appui fournis par des tiers, notamment les organisations qui délivrent des certificats des autorités de certification, qui proposent des services de temps, ainsi que d'autres services;

b) Les organismes de réglementation, notamment les organes judiciaires nationaux et d'autres organisations chargées de résoudre les litiges.

7.2 Les processus de vérification de l'intégrité numérique basée sur la technologie DLT

7.2.1 Enregistrement de la preuve de l'intégrité numérique

Le processus d'enregistrement de la preuve de l'intégrité numérique sur les registres DLT comporte les étapes clés suivantes:

a) L'utilisateur interagit avec une plate-forme de services commerciaux et pourra rendre nécessaire la protection de l'authenticité des informations à caractère commercial. La plate-forme commerciale envoie les caractéristiques extraites des informations d'origine à la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT.

b) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT génère une preuve électronique contenant les caractéristiques extraites, la date et l'heure, et d'autres informations nécessaires.

c) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT génère une valeur de hachage unique pour la preuve électronique à l'aide de fonctions de hachage cryptographique (SHA256, par exemple).

d) La plate-forme de services commerciaux crée une signature numérique pour la valeur de hachage avec la clé privée du propriétaire.

e) La plate-forme de services commerciaux soumet le relevé de preuve à l'adresse du contrat intelligent sur les registres distribués.

f) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT vérifie que la signature numérique et les informations sont complètes, exécute le contrat intelligent et crée un relevé dans le registre.

g) La preuve enregistrée est placée dans un nouveau bloc, lequel est transmis au réseau.

7.2.2 Provenance de la preuve de l'intégrité numérique

Le processus clé de provenance de la preuve de l'intégrité numérique se déroule comme suit:

a) L'utilisateur interroge la preuve de l'intégrité numérique sur les registres distribués.

b) En cas de litige en ligne, la plate-forme de résolution des litiges lance une enquête judiciaire concernant la preuve numérique sur la base des relevés sur les registres distribués.

8 Menaces de sécurité concernant la vérification de l'intégrité numérique basée sur la technologie DLT

Ce paragraphe contient une analyse des menaces de sécurité pour les parties prenantes, c'est-à-dire l'utilisateur, la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT et les processus inhérents à la vérification de l'intégrité numérique basée sur la technologie DLT, à savoir l'enregistrement de la preuve de l'intégrité numérique et la provenance de la preuve de l'intégrité numérique. Les menaces qui pèsent sur les composantes du protocole, du réseau et des données dans les applications basées sur la technologie DLT sont décrites en détail dans la Recommandation [UIT-T X.1401].

8.1 Menaces de sécurité concernant l'utilisateur

8.1.1 Fraude à l'identité de l'utilisateur

Les utilisateurs enregistrés présentent des demandes illégales sous de fausses identités pour obtenir des autorisations dont ils ne disposent pas sous leur véritable identité.

8.1.2 Fuite de clé privée

Les menaces de fuite de clé privée dans un registre comprennent principalement les attaques perpétrées contre le logiciel d'un client et les attaques physiques (par exemple la divulgation de clés imprimées à des tiers). La fuite d'une clé privée permet à d'autres utilisateurs d'accéder à la plate-forme de vérification basée sur la technologie DLT, ce qui porte atteinte à la sécurité de cette plate-forme. La menace de fuite de clé privée est décrite en détail dans le paragraphe 6.3.2 de la Recommandation [UIT-T X.1401].

8.1.3 Perte de clé privée

Les menaces de perte de clé privée comprennent principalement les attaques par logiciels malveillants, les attaques physiques (par exemple la perte de clés privées imprimées sur papier), etc. Ces actions peuvent entraîner la divulgation des renseignements personnels de l'utilisateur, ce qui permet aux utilisateurs malveillants d'accéder à la plate-forme de vérification basée sur la technologie DLT et d'annihiler la sécurité de cette plate-forme. La menace de perte de clé privée est décrite en détail dans le paragraphe 6.3.3 de la Recommandation [UIT-T X.1401].

8.1.4 Divulgation de renseignements personnels

Les informations de preuve du propriétaire peuvent contenir des informations personnelles sensibles comme son nom ou des informations sur son identité, et les renseignements personnels de l'utilisateur peuvent fuiter au cours du processus d'enregistrement de la preuve. La menace de divulgation de renseignements personnels est décrite en détail dans le paragraphe 6.3.1 de la Recommandation [UIT-T X.1401].

8.2 Menaces de sécurité concernant l'enregistrement des informations

8.2.1 Preuves frauduleuses

Sur la base de l'algorithme d'extraction des caractéristiques de la preuve numérique, les attaquants pourraient construire différentes valeurs de caractéristiques dont le contenu est semblable à celui du document original. Ainsi, les attaquants pourraient écrire du contenu illégal dans les registres distribués.

8.2.2 Altération des preuves

L'utilisateur malveillant peut falsifier les preuves du document original, détruire l'authenticité d'une preuve ou la faire disparaître, et écrire ainsi une preuve altérée dans les registres distribués. Les attaques par l'algorithme de chiffrement asymétrique peuvent nuire à la sécurité des transmissions et du stockage. L'attaque par l'algorithme de chiffrement asymétrique est décrite en détail dans le paragraphe 6.1.5 de la Recommandation [UIT-T X.1401].

8.2.3 Attaque basée sur la dépendance vis-à-vis de l'horodatage

Les attaques peuvent consister à manipuler le service d'horodatage de la plate-forme de vérification basée sur la technologie DLT: la plate-forme n'est donc plus en mesure de suivre avec précision la séquence des événements d'enregistrement des preuves, et n'est donc plus capable de fournir une base criminalistique efficace en ce qui concerne la provenance des preuves.

8.2.4 Attaque des 51%

Lorsque les attaquants possèdent plus de 51% de la puissance de calcul, ils peuvent construire une nouvelle chaîne, laquelle peut invalider les preuves de la chaîne principale. De plus, une attaque des 51% peut permettre aux contrevenants de s'enregistrer avec succès. L'attaque des 51% est décrite en détail dans le paragraphe 6.1.1 de la Recommandation [UIT-T X.1401].

8.2.5 Attaque par corruption

Lorsque des attaquants disposant des ressources suffisantes corrompent les nœuds avec des autorisations de vote, ils peuvent nuire aux droits et aux intérêts d'un réseau DLT contenant des preuves. De cette manière, les attaquants écrivent des informations de preuve illégales dans le réseau DLT contenant des preuves. L'attaque par corruption est décrite dans le paragraphe 6.1.1 de la Recommandation [UIT-T X.1401].

8.2.6 Attaque par retenue de bloc

Sur une plate-forme de vérification basée sur la technologie DLT reposant sur l'algorithme de consensus de la preuve de travail, un attaquant peut conserver un bloc qu'il a miné et miner le bloc suivant secrètement s'il dispose d'une puissance suffisante. En générant plusieurs blocs quand d'autres mineurs n'en génèrent qu'un seul, l'attaquant peut faire perdre de la puissance aux autres mineurs. La cible de l'attaque est un opérateur de plate-forme qui accepte les validations zéro. Les preuves de la chaîne principale peuvent alors être invalidées, et le contrevenant pourrait également s'enregistrer avec succès. L'attaque par retenue de bloc est décrite en détail dans le paragraphe 6.1.1 de la Recommandation [UIT-T X.1401].

8.2.7 Attaque par saut de chaîne

Un attaquant peut passer d'une chaîne de blocs à une autre en tirant parti de la difficulté des algorithmes d'ajustement de la chaîne. L'attaquant peut ainsi obtenir une récompense illégitime et occasionner des pertes aux autres utilisateurs. En outre, cela pourrait entraîner une augmentation significative de la puissance de calcul effective au sein du pool de minage et le contrevenant pourrait également s'enregistrer avec succès. L'attaque par saut de chaine est décrite en détail dans le paragraphe 6.1.1 de la Recommandation [UIT-T X.1401].

8.2.8 Attaque par déni de service réparti

Sur une plate-forme de vérification basée sur la technologie DLT, un attaquant peut bloquer le réseau en lançant des attaques par déni de service réparti. Les plus répandues sont les attaques Sybil et Eclipse. Elles peuvent conduire à un enregistrement réussi de preuves frauduleuses. L'attaque Sybil est décrite en détail dans le paragraphe 6.2.3 et l'attaque Éclipse dans le paragraphe 6.2.1 de la Recommandation [UIT-T X.1401].

8.2.9 Attaque par détournement du protocole de passerelle frontière

Un attaquant peut tirer parti du détournement du protocole de passerelle frontière et de la division en deux parties ou plus des nœuds de réseau des registres distribués. Par conséquent, le registre DLT est subdivisé en deux chaînes parallèles ou plus. À ce moment-là, l'enregistrement des preuves et l'enregistrement des preuves frauduleuses peuvent être effectués sur des branches parallèles. Une fois l'attaque terminée, le registre distribué contenant les preuves est réunifié avec la chaîne principale la plus longue, les autres branches sont éliminées et tous les relevés de preuves sur ces chaînes deviennent invalides. Ainsi, des preuves frauduleuses peuvent être enregistrées avec succès.

8.3 Menaces de sécurité concernant la provenance des preuves

8.3.1 Attaque par écriture d'informations frauduleuses

Aucune donnée de transaction dans un registre DLT ne peut être retirée. Dès lors que l'information est écrite dans le registre DLT, elle ne peut être supprimée. Les attaquants peuvent écrire des informations frauduleuses dans les registres distribués en lançant des attaques contre les contrats intelligents, par exemple des attaques par exceptions compromises, comme décrit en détail dans le paragraphe 6.1.2 de la Recommandation [UIT-T X.1401]. La plate-forme génère de nouveaux blocs, ce qui entraîne des attaques par bloc spam et perturbe de fait le fonctionnement de la plate-forme de vérification basée sur la technologie DLT.

8.3.2 Divulgation des informations de preuve

En ce qui concerne la provenance des preuves, un algorithme devrait être utilisé pour chiffrer et stocker les informations de preuve. Il est important d'assurer la sécurité de l'algorithme de chiffrement. Les attaques par algorithme de chiffrement asymétrique peuvent nuire à la sécurité de la plate-forme de vérification basée sur la technologie DLT. L'attaque par l'algorithme de chiffrement asymétrique est décrite en détail dans le paragraphe 6.1.5 de la Recommandation [UIT-T X.1401].

9 Exigences de sécurité applicables à la vérification de l'intégrité numérique basée sur la technologie DLT

Le présent paragraphe décrit les exigences de sécurité applicables à la vérification de l'intégrité numérique basée sur la technologie DLT, compte tenu des analyses relatives aux menaces de sécurité présentées dans le paragraphe 7. En outre, le présent paragraphe contient des exigences de sécurité applicables aux parties prenantes, à savoir l'utilisateur, la plate-forme de vérification de l'intégrité numérique et les processus inhérents aux services de vérification de l'intégrité numérique basée sur la technologie DLT (l'enregistrement des preuves numériques et la provenance des preuves numériques). Les exigences applicables à la sécurité des données, du réseau, du consensus et des applications sont décrites en détail dans les paragraphes 8.1 à 8.4 de la Recommandation [UIT-T X.1402].

9.1 Exigences de sécurité applicables à l'utilisateur

9.1.1 Protection de l'identité de l'utilisateur

Les exigences de sécurité suivantes destinées à lutter contre la fraude à l'identité s'appliquent à la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT.

a) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait préciser l'autorisation d'exploitation de chaque utilisateur. La plate-forme devrait permettre à l'utilisateur de se servir d'une clé privée pour signer les informations et les envoyer au registre DLT. Ce dernier devrait récupérer la clé publique basée sur la signature, identifier les utilisateurs sur la base de la clé publique et authentifier les opérations des utilisateurs.

b) Lorsqu'un utilisateur s'enregistre sur la plate-forme, celle-ci doit d'abord vérifier les informations d'identité de l'utilisateur, et pourra ensuite attribuer une étiquette à chaque utilisateur.

c) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait écrire toutes les opérations de chaque utilisateur dans les registres distribués.

d) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait exiger que l'identité de l'utilisateur soit authentifiée pour chaque enregistrement de preuve, notamment au moyen d'un contrôle d'accès, d'un mot de passe, d'une signature numérique et d'une reconnaissance biométrique.

9.1.2 Protection des clés privées

Les exigences de sécurité suivantes relatives à la protection des clés privées sont applicables à la plate-forme de vérification basée sur la technologie DLT.

a) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait lutter contre la fuite de clés privées; un opérateur de plate-forme de vérification basée sur la technologie DLT devrait empêcher qu'un code frauduleux porte atteinte à ses clients.

b) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait prévenir la perte de clés privées; les utilisateurs d'une plate-forme de vérification basée sur la technologie DLT devraient conserver leurs clés privées dans un endroit sûr et éviter de les laisser sur des supports physiques ou dématérialisés facilement accessibles (comme du papier

d'impression) sans aucun mécanisme de protection; il est possible de renforcer la protection des clés privées en demandant notamment des numéros d'identification personnels, des mots de passe, les empreintes digitales et d'autres données biométriques.

9.1.3 Protection de la confidentialité

La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait adopter des mesures pertinentes de protection de la sécurité dans les liaisons de traitement de l'information (collecte, stockage, utilisation, partage, transfert ou encore divulgation publique), afin de lutter contre la collecte illégale, l'utilisation abusive et la fuite des informations du propriétaire, et de renforcer le plus possible la protection des droits et des intérêts légitimes du propriétaire.

9.2 Exigences de sécurité applicables à l'enregistrement des preuves

9.2.1 Lutte contre les preuves frauduleuses

Les exigences de sécurité suivantes relatives à la lutte contre les preuves numériques frauduleuses s'appliquent à la plate-forme de vérification basée sur la technologie DLT.

a) La plate-forme de vérification basée sur la technologie DLT devrait présenter des algorithmes de consensus avec un niveau de garantie de sécurité (LoSA) et une résistance du mécanisme de consensus (CMS) [UIT-T X.1404], tels que la tolérance de panne byzantine pratique (PBFT), afin de lutter contre la falsification des preuves numériques.

b) La plate-forme de vérification basée sur la technologie DLT devrait surveiller la puissance de calcul effective du réseau, afin de détecter les modifications et d'empêcher les attaques par saut de chaîne.

c) La plate-forme de vérification basée sur la technologie DLT devrait renforcer la difficulté des algorithmes de construction de valeurs propres, tout en veillant à ce que le système fonctionne de manière raisonnablement efficace.

9.2.2 Lutte contre la falsification des preuves

Les exigences de sécurité suivantes relatives à la lutte contre la falsification des preuves numériques s'appliquent à la plate-forme de vérification basée sur la technologie DLT.

a) La plate-forme de vérification basée sur la technologie DLT devrait utiliser du matériel chiffré.

b) La plate-forme de vérification basée sur la technologie DLT devrait utiliser des algorithmes de chiffrement pour garantir une transmission sûre des informations de preuve. Les services tiers associés devraient utiliser des algorithmes de chiffrement pour garantir que les informations de preuve sont stockées en toute sécurité. La plate-forme et les services tiers associés devraient choisir des algorithmes de chiffrement adéquats, pour lesquels un compromis devrait être trouvé entre la sécurité, le coût des calculs et la longueur de clé – il est possible de choisir d'augmenter la longueur des clés pour compenser les risques provoqués par l'accroissement de la puissance de calcul.

9.2.3 Protection de l'enregistrement des preuves

Les exigences de sécurité suivantes relatives au contrôle de la sécurité de l'enregistrement s'appliquent à la plate-forme de vérification basée sur la technologie DLT.

a) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT doit être synchronisée avec un service de temps tiers fiable.

b) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait envoyer des avertissements concernant des attaques contre la sécurité, des failles, des codes frauduleux, des analyses de menaces et des fuites de données, et transmettre d'autres renseignements sur les menaces; elle devrait aussi identifier les problèmes rencontrés sur la

plate-forme par l'intermédiaire de recherches de vulnérabilités et de tests de sécurité automatisés.

c) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait proposer des fonctionnalités d'authentification de l'identité et de contrôle d'accès pour atténuer les risques d'attaque contre la sécurité, comme des modifications malveillantes et des attaques à distance.

d) En ce qui concerne les applications mobiles, la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait fournir des méthodes de protection de la sécurité, comme le renforcement et l'obfuscation du code source pour lutter contre la rétro-ingénierie, la décompilation et l'intégration d'un code frauduleux.

e) La plate-forme peut utiliser la technologie des points de contrôle pour écrire au client en codant matériellement afin que ce dernier accepte toutes les transactions effectives avant le point de contrôle, empêchant ainsi une attaque des 51%. Le point de contrôle devrait: introduire un mécanisme de consensus de preuve d'enjeu amélioré avec une marge et des sanctions; horodater chaque transaction; établir une authentification de nœud tierce fiable pour authentifier l'identité; et ne pas accepter les confirmations zéro.

f) La plate-forme peut recourir au filtrage des ports pour nettoyer le trafic anormal, assurer la sécurité de l'informatique en nuage et offrir un niveau de protection élevé pour la résolution du système de noms de domaine (DNS) dans le système afin de garantir une mise en œuvre sûre. Elle devrait aussi réguler la taille des blocs de données pour éviter les attaques de spam.

g) La plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait proposer des fonctions de collecte de preuves et de traçage des incidents de sécurité, analyser les causes de ces incidents et proposer des solutions pour repousser les attaques.

9.3 Exigences de sécurité applicables à la provenance des preuves

9.3.1 Prévention contre l'écriture d'informations malveillantes

Pour assurer la sécurité de la provenance des preuves, la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait:

a) réguler la taille des blocs de données pour empêcher les nœuds de générer des blocs spam;

b) veiller à ce que les entités non autorisées et anonymes ne puissent pas rechercher des données de compte et des données de transaction dans les nœuds d'un système de registre distribué, ni accéder à ces données;

c) utiliser des bibliothèques qui garantissent la sécurité des calculs, par exemple SafeMath;

d) examiner le code afin d'éviter les flux de nombres entiers et les exceptions compromises et ainsi d'empêcher les attaques contre les contrats intelligents;

e) utiliser des générateurs aléatoires de nombres imprévisibles afin d'empêcher les utilisateurs malveillants de contrôler les résultats des contrats intelligents;

f) faire en sorte que les contrôles d'accès définis lors du développement de programmes soient aussi stricts que possible, pour empêcher que des attaquants procèdent à un changement de propriété des fonctions de contrats intelligents en vue d'obtenir le plus haut niveau d'autorisation d'exploitation.

9.3.2 Protection des informations de preuve

Pour assurer la sécurité des informations de preuve, la plate-forme de vérification de l'intégrité numérique basée sur la technologie DLT devrait:

a) utiliser du matériel chiffré pour stocker les informations de preuve en dehors de la chaîne;

b) choisir les algorithmes de chiffrement adéquats, pour lesquels un compromis devrait être trouvé entre la sécurité, le coût des calculs et la longueur de clé – il est possible de choisir

d'augmenter la longueur des clés pour compenser les risques provoqués par l'accroissement de la puissance de calcul;

c) utiliser un mécanisme de contrôle d'accès efficace pour pouvoir contrôler l'accès aux informations de preuve.

Appendice I

Cas d'utilisation d'une facture électronique basée sur la technologie des registres distribués

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Dans le cadre du mécanisme de consensus, seules les factures établies par les autorités fiscales peuvent être vérifiées et approuvées, tandis que les factures établies par tout autre nœud ne peuvent être confirmées, ce qui garantit l'authenticité des factures. Dans le cas des contrats intelligents, les transactions et la facturation se déroulent simultanément, et les paiements des consommateurs et la facturation ont lieu de manière fluide. La Figure I.1 présente une vue d'ensemble. Pour obtenir plus de détails, veuillez consulter la norme [b-IEEE 2142.1-2021] *Recommended Practice for E-Invoice Business Using Blockchain Technology* (Bonnes pratiques relatives à la facturation électronique à l'aide de la technologie de la blockchain).

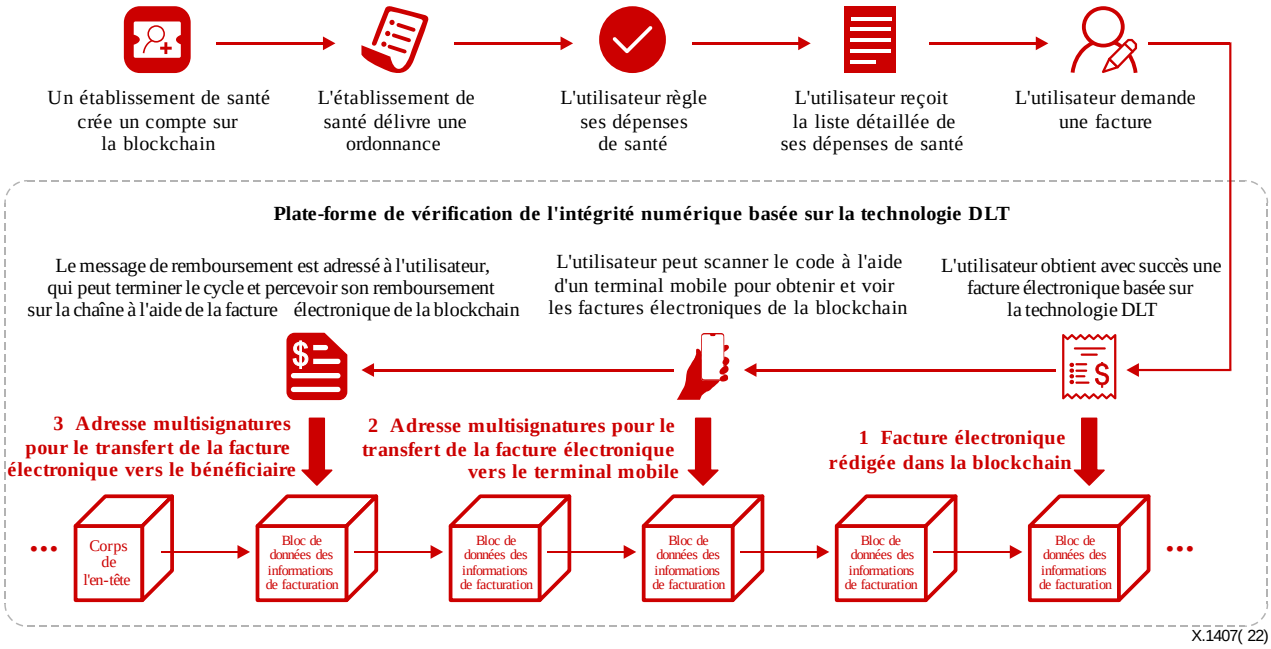

Figure I.1 – Vue d'ensemble de cas d'utilisation de la facture électronique basée sur la technologie DLT

Le cas d'utilisation par un établissement de santé des factures électroniques basées sur la technologie des registres distribués est décrit comme suit:

a) L'établissement de santé enregistre un compte sur la blockchain, se connecte au système de facturation basé sur la technologie DLT et définit les conditions de facturation sur la chaîne.

b) L'établissement de santé délivre une ordonnance.

c) L'utilisateur règle ses dépenses de santé en possession de son ordonnance.

d) L'utilisateur reçoit une liste détaillée des dépenses de santé une fois que le paiement a été effectué.

e) L'utilisateur demande une facture.

f) L'utilisateur obtient avec succès une facture électronique de la blockchain.

g) L'utilisateur peut scanner le code sur son terminal mobile pour recevoir et consulter la facture électronique de la blockchain.

h) Le terminal mobile peut envoyer le message de remboursement, et l'utilisateur peut se servir de la facture électronique de la blockchain pour terminer le cycle et percevoir son remboursement sur la chaîne.

Le processus de facturation basé sur le paiement peut comporter les phases suivantes:

– Phase A: transaction
– Phase B: émission de la facture
– Phase C: remboursement
– Phase D: acquittement de l'impôt

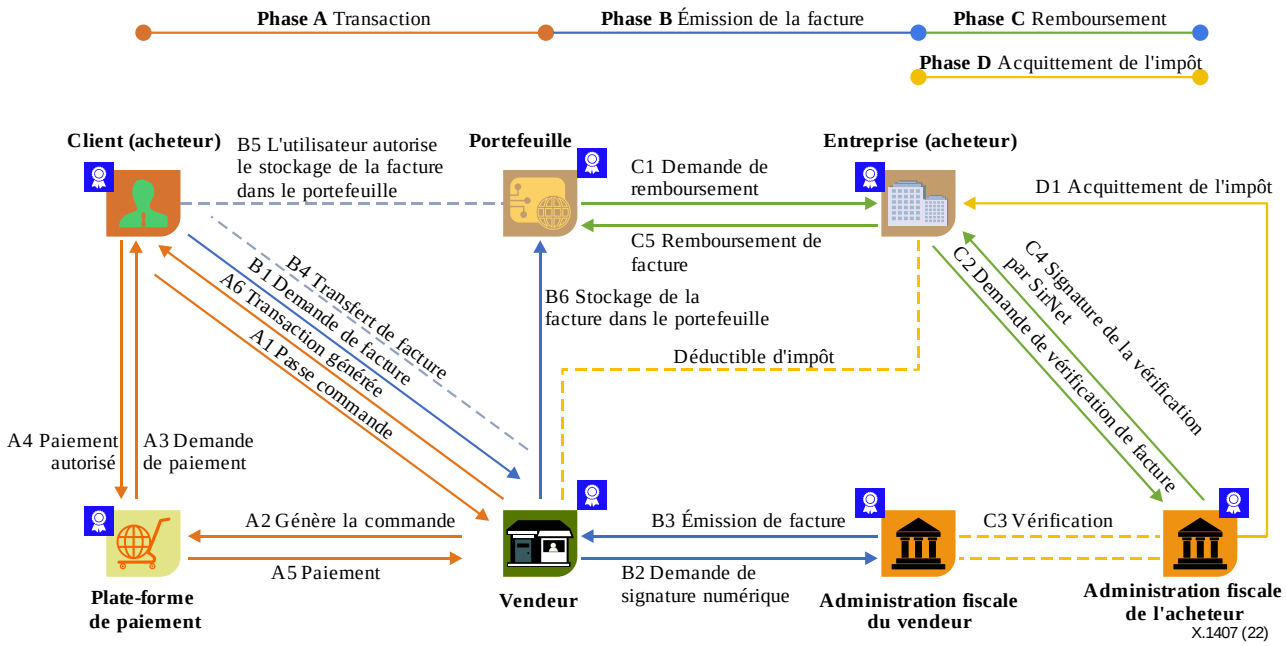

Figure I.2 – Diagramme de flux du cas d'utilisation d'une facture électronique basée sur la technologie DLT

Pendant la phase de transaction, lorsque le client (autrement dit l'acheteur) passe commande, le fournisseur de service (autrement dit le vendeur) génère la commande sur la plate-forme de paiement, qui confirme alors la commande après avoir reçu l'accord du client, et le reçu est généré une fois le paiement effectué. Le reçu peut se présenter sous la forme d'un bloc de paiement sur une chaîne ou un registre de paiement dans une base de données centralisée.

Pendant la phase d'émission de la facture, la facture est délivrée par l'administration fiscale d'origine du marchand à la demande du client présentée par exemple depuis le portefeuille du client, et le reçu du paiement est utilisé en tant que sortie transactionnelle non dépensée (UTXO) aux fins d'émission de la facture. Les nœuds participants regroupent les nœuds de consensus centraux ancrés dans la couche principale du registre et les nœuds de vérification de paiement simplifiée (SPV), tels que le nœud du marchand et le nœud du portefeuille personnel, etc.

Pendant la phase de remboursement, l'entreprise en relation avec le client (CAE), en tant que nœud SPV, vérifie la facture lorsque le client débute le processus de remboursement, et la facture stockée dans le portefeuille personnel est remboursée en tant qu'UTXO.

Pendant la phase d'acquittement de l'impôt, les nœuds de destination de l'administration fiscale et le nœud SPV de l'entreprise en relation avec le client s'intègrent au processus, et la facture est utilisée en tant qu'UTXO pour le remboursement de la TVA.

L'utilisation de la technologie DLT dans le cadre du système de facturation électronique comporte plusieurs avantages:

1) L'authenticité de la facture est garantie, et l'intégralité du processus d'obtention de la facture, d'émission de la facture, de diffusion, d'entrée et de remboursement est traçable.

2) Les données de la facture sont inviolables, et l'autorité fiscale, la partie chargée de la facturation, la partie chargée de la diffusion et la partie chargée du remboursement prennent part conjointement au processus de comptabilité.

3) La facturation électronique basée sur la technologie DLT ne nécessite aucune vignette fiscale ni aucun type de matériel particulier. En revanche, la facturation classique nécessite plusieurs vignettes pour chaque magasin dans le cas des chaînes de magasins. Une facture électronique basée sur la technologie DLT est remboursée automatiquement grâce au système ERP et l'augmentation du nombre de magasins n'engendre aucun frais supplémentaire.

4) Dans le cas des factures classiques, si l'administration fiscale n'est pas en mesure d'approuver autant de factures que le souhaite une entreprise en raison d'un développement temporaire de son activité, le contribuable peut demander à l'administration fiscale d'approuver plus de factures. Toutefois, les factures basées sur la technologie DLT sont fournies sur demande et il n'est pas nécessaire de passer par un autre processus pour les obtenir.

5) L'obtention et l'achat de papier auprès des Offices d'administration fiscale pour établir des factures classiques demandent du temps et des efforts, alors qu'il n'est pas nécessaire d'utiliser du papier pour établir des factures électroniques basées sur la technologie DLT.

Appendice II

Cas d'utilisation de la vérification des diplômes universitaires basée sur la technologie des registres distribués

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

La vérification des diplômes est un processus chronophage, car il peut durer des jours, voire des semaines. Les employeurs se posent des questions quant à l'authenticité des qualifications et passent beaucoup de temps à échanger avec les universités pour vérifier l'intégrité des diplômes et s'assurer que les candidats possèdent d'excellentes compétences. La blockchain permettra d'assurer la transparence et de simplifier le partage de diplômes vérifiés avec divers employeurs ou toute autre partie.

Les employeurs peuvent vérifier l'intégrité d'un diplôme universitaire grâce à la technologie DLT. Les registres distribués constituent une source fiable et reconnue pour stocker les diplômes des étudiants, lesquels sont accessibles à un ensemble divers d'institutions et d'universités. Il s'agit de registres publics accessibles en permanence, protégés contre les changements dont les institutions font l'objet ou la perte de dossiers privés.

Ce modèle se compose des éléments suivants:

Utilisateurs

– Émetteur (université)
– Bénéficiaire (étudiants)
– Vérificateur (employeurs)

Systèmes

– Nœuds des universités
– Plate-forme de blockchain

Données

– Hachures des diplômes
– Diplômes au format électronique

La Figure II.1 représente le processus de vérification de l'intégrité d'un diplôme, qui repose sur la vérification de la valeur de hachage du diplôme et la comparaison de la hachure avec celles stockées dans la blockchain. Le processus comporte les étapes suivantes:

– L'université délivre un nouveau diplôme au format électronique à un étudiant et importe le fichier sur un registre DLT.
– Le registre DLT hache et stocke le fichier correspondant au diplôme.
– À des fins de vérification de l'intégrité, l'étudiant ou l'employeur importe le document correspondant au diplôme sur la plate-forme basée sur la technologie DLT.
– Le registre DLT génère la hachure pour le document, puis la compare avec les hachures stockées sur la blockchain.
– Si la hachure générée correspond à l'une des hachures stockées dans la blockchain, alors le diplôme est authentique.

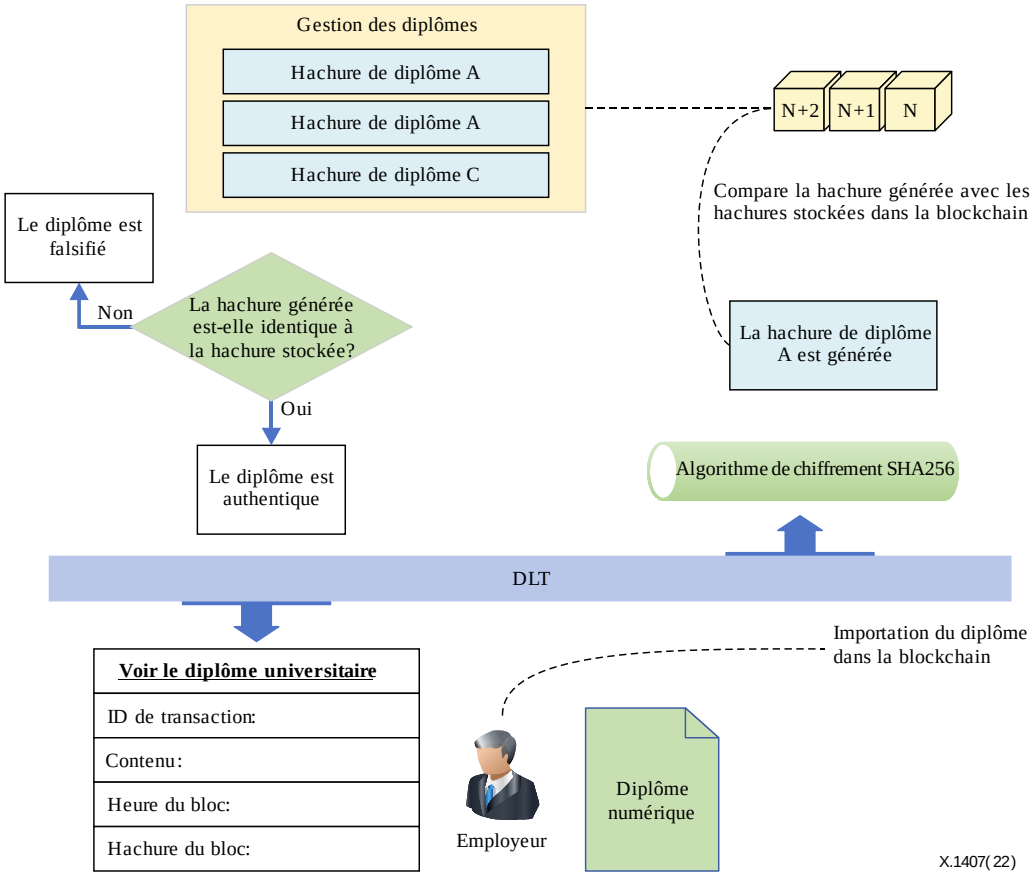

Figure II.1 – Vue d'ensemble de la vérification de diplôme universitaire basée sur la technologie DLT

Il est avantageux d'utiliser la technologie DLT à des fins de vérification de l'authenticité des diplômes universitaires pour les raisons suivantes:

– La technologie DLT résout les difficultés actuelles rencontrées dans le processus de validation et d'authentification.

– La technologie DLT peut regrouper toutes les universités sur une seule plate-forme.

– La technologie DLT encourage les employeurs à travailler systématiquement avec les universités.

– La technologie DLT permet d'enregistrer et de partager des informations authentiques et complètes sur une source unique digne de confiance.

– La technologie DLT permet de consacrer moins de temps, d'argent et d'efforts.

Bibliographie

[b-ITU-T X.1400] Recommandation UIT-T X.1400 (2020), *Termes et définitions concernant la technologie des registres distribués*.

[b-ISO 13491-2] ISO 13491-2:2017(en anglais), *Services financiers – Dispositifs cryptographiques de sécurité (services aux particuliers) – Partie 2: Listes de contrôle de conformité de sécurité pour les dispositifs utilisés dans les transactions financières.*
<https://www.iso.org/obp/ui/#iso:std:iso:13491:-2:ed-4:v1:en>

[b-ISO 23257] ISO 23257:2022, *Technologies des chaînes de blocs et technologies de registre distribué – Architecture de référence*.

[b-ISO/CEI 27000] ISO/CEI 27000:2018 (en anglais), *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

[b-ISO 22739] ISO 22739:2020, *Chaîne de blocs et technologies de registres distribués – Vocabulaire.*
<https://www.iso.org/standard/73771.html>

[b-IEEE 2142.1-2021] IEEE 2142.1-2021, *IEEE Recommended practice for e-invoice business using blockchain technology (Bonnes pratiques relatives à la facturation électronique à l'aide de la technologie de la blockchain).*
<https://standards.ieee.org/ieee/2142.1/7590/>

[b-ISO 56000] ISO 56000:2020, *Management de l'innovation – Principes essentiels et vocabulaire.*
<https://www.iso.org/fr/standard/69315.html

[b-ISO 5807] ISO 5807:1985, *Traitement de l'information – Symboles de documentation et conventions applicables aux données, aux organigrammes de programmation et d'analyse, aux schémas des réseaux de programmes et des ressources de système.*
<https://www.iso.org/standard/11955.html>

[b-Kaur] Kaur, S., Chaturvedi, S., Sharma, A. Kar, J. (2021), *A Research Survey on Applications of Consensus Protocols in Blockchain (Enquête sur les applications des protocoles de consensus dans la blockchain)*, Security and Communication Networks, Vol. 2021, identificateur de l'article: 6693731, janvier, pp. 1-22.
<https://www.iso.org/fr/standard/11955.html>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2022