ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

**UIT-T F.751.8 (07/2023)**

SÉRIE F: Services de télécommunication non téléphoniques

Services multimédias

# Cadre technique pour l'adaptation de la technologie des registres distribués (DLT) à la réglementation

RECOMMANDATIONS UIT-T DE LA SÉRIE F

**Services de télécommunication non téléphoniques**

| | |
|---|---|
| SERVICE TÉLÉGRAPHIQUE | F.1-F.109 |
| Méthodes d'exploitation pour le service télégraphique public international | F.1-F.19 |
| Le réseau gentex | F.20-F.29 |
| Commutation de messages | F.30-F.39 |
| Le service international de télémessagerie | F.40-F.58 |
| Le service télex international | F.59-F.89 |
| Statistiques et publications des services télégraphiques internationaux | F.90-F.99 |
| Services de télécommunication à location et à heures prédéterminées | F.100-F.104 |
| Services phototélégraphiques | F.105-F.109 |
| SERVICE MOBILE | F.110-F.159 |
| Service mobile et services multidestination par satellite | F.110-F.159 |
| SERVICES TÉLÉMATIQUES | F.160-F.399 |
| Service public de télécopie | F.160-F.199 |
| Service télétex | F.200-F.299 |
| Service vidéotex | F.300-F.349 |
| Dispositions générales relatives aux services télématiques | F.350-F.399 |
| SERVICES DE MESSAGERIE | F.400-F.499 |
| SERVICES D'ANNUAIRE | F.500-F.549 |
| COMMUNICATION DE DOCUMENTS | F.550-F.599 |
| Communication de documents | F.550-F.579 |
| Interfaces de communication de programmation | F.580-F.599 |
| SERVICES DE TRANSMISSION DE DONNÉES | F.600-F.699 |
| **SERVICES MULTIMÉDIAS** | **F.700-F.799** |
| SERVICES DU RNIS | F.800-F.849 |
| TÉLÉCOMMUNICATIONS PERSONNELLES UNIVERSELLES | F.850-F.899 |
| ACCESSIBILITÉ ET FACTEURS HUMAINS | F.900-F.999 |

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

# Recommandation UIT-T F.751.8

## Cadre technique pour l'adaptation de la technologie des registres distribués (DLT) à la réglementation


**Résumé**

La Recommandation UIT-T F.751.8 définit le cadre technique pour l'adaptation de la technologie des registres distribués (DLT) à la réglementation, y compris les difficultés réglementaires et les capacités techniques. La conception du cadre technique de la technologie DLT dans la présente Recommandation est étroitement liée aux caractéristiques de cette technologie, notamment la décentralisation, l'inaltérabilité et l'ouverture. La présente Recommandation peut servir d'orientations à l'intention des fournisseurs de services DLT et des développeurs de systèmes DLT lorsque les systèmes DLT doivent être adaptés à la réglementation.



**Historique**[*]

| Édition | Recommandation | Approbation | Commission d'études | ID unique |
|---|---|---|---|---|
| 1.0 | UIT-T F.751.8 | 10-07-2023 | 16 | 11.1002/1000/15174 |

**Mots clés**

Chaîne de blocs; technologie des registres distribués; réglementation


[*] Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

## 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 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.

A 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/.

© UIT 2023

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

## TABLE DES MATIÈRES


| | | Page |
|---|---|---|
| 1 | Domaine d'application | 1 |
| 2 | Références | 1 |
| 3 | Définitions | 1 |
| | 3.1 Termes définis ailleurs | 1 |
| | 3.2 Termes définis dans la présente Recommandation | 1 |
| 4 | Abréviations et acronymes | 2 |
| 5 | Conventions | 2 |
| 6 | Aperçu | 2 |
| 7 | Difficultés réglementaires | 3 |
| | 7.1 Fuite d'informations confidentielles | 3 |
| | 7.2 Inaltérabilité des dossiers et absence de fonctionnalité permettant d'effacer les transactions/contenus | 3 |
| | 7.3 Menaces de sécurité | 3 |
| | 7.4 Perte de jetons, de monnaie numérique et d'autres actifs | 3 |
| | 7.5 Délits financiers et autres délits | 3 |
| 8 | Capacités techniques pour l'adaptation à la réglementation | 3 |
| | 8.1 Cadre technique | 3 |
| | 8.2 Capacités au niveau des applications | 4 |
| | 8.3 Capacités en matière de protection de la vie privée/confidentialité | 4 |
| | 8.4 Capacités d'effacement des données | 5 |
| | 8.5 Capacités relatives à la sécurité des données | 5 |
| | 8.6 Capacité concernant le niveau de base | 6 |
| Bibliographie | | 7 |

# Recommandation UIT-T F.751.8

## Cadre technique pour l'adaptation de la technologie des registres distribués (DLT) à la réglementation

### 1 Domaine d'application

La présente Recommandation définit un cadre technique pour adapter la technologie des registres distribués (DLT) à la réglementation. Elle porte sur les domaines suivants:

– défis réglementaires liés à la technologie DLT;

– capacités techniques nécessaires pour que la technologie DLT s'adapte à la réglementation.

La présente Recommandation s'adresse aux fournisseurs de services DLT et aux développeurs de systèmes DLT. Elle ne s'adresse pas aux régulateurs de ces technologies. Son objectif n'est pas de fournir des solutions réglementaires à l'intention des régulateurs, mais plutôt de proposer des solutions techniques aux difficultés liées à la réglementation de cette technologie.

### 2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T F.751.0] Recommandation UIT-T F.751.0 (2020), *Exigences pour les systèmes de registres distribués*.

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

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 consensus** [b-UIT-T X.1400]: accord selon lequel un ensemble de transactions est valide.

**3.1.2 mécanisme de consensus** [b-UIT-T X.1400]: règles et procédures permettant de parvenir à un consensus.

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

**3.1.4 secret** [b-UIT-T J.160]: moyen de s'assurer que des informations ne sont pas divulguées à des personnes autres que celles à qui elles sont destinées. La confidentialité est assurée par le chiffrement des informations. Terme parfois utilisé pour désigner la confidentialité.

**3.1.5 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

Aucun.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AML lutte contre le blanchiment de capitaux (*anti-money-laundering*)

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

GAFI Groupe d'action financière sur le blanchiment de capitaux

IoT Internet des objets (*Internet of things*)

KYC connaissance des clients (*know your customer*)

PKI infrastructure de clé publique (*public key infrastructure*)

TEE environnement d'exécution fiable (*trusted execution environment*)

## 5 Conventions

Dans la présente Recommandation:

– L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

– L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

– Les expressions "**peut, à titre d'option**" et "**peut**" indiquent une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elles ne doivent pas être interprétées comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

## 6 Aperçu

La technologie des registres distribués (DLT) permet à un grand groupe de nœuds du réseau DLT de parvenir à des accords et d'enregistrer des informations sans autorité centrale. Le développement rapide de cette technologie pose des difficultés sur le plan de la réglementation concernant, entre autres, la protection de la vie privée/confidentialité, la réglementation applicable à la protection des données, la gestion des attaques visant les réseaux et la réglementation applicable aux cryptomonnaies. La technologie DLT est appliquée à différents domaines, comme les cryptomonnaies, la gestion de la chaîne d'approvisionnement et l'Internet des objets. En conséquence, il est nécessaire de récapituler les exigences réglementaires en se fondant sur l'analyse des fonctions et caractéristiques de la technologie DLT et de définir le cadre technique qui permettra de combler les vides entre ouverture et réglementation. Les premiers travaux effectués ont permis d'élaborer [b-DLT 4.1] et se sont poursuivis pour aboutir aux spécifications techniques présentées ci-après.

## 7 Difficultés réglementaires

### 7.1 Fuite d'informations confidentielles

Des informations confidentielles peuvent être révélées directement dans la chaîne, avec la combinaison de données extérieures avec des données dans la chaîne ou en dehors de la chaîne. Les transactions et les clés publiques pourraient être disponibles directement dans la chaîne, en particulier dans le cas des systèmes DLT sans permission. Des données extérieures pourraient permettre l'identification de clés publiques associées à des personnes ou des entreprises et, partant, l'identification de transactions.

Dans les registres distribués sans permission, il n'y a pas de contrôle d'accès et toutes les données stockées directement dans la chaîne sont accessibles à tous. Le stockage d'informations confidentielles (sans chiffrement) dans un registre distribué sans permission est considéré comme une fuite de données confidentielles.

### 7.2 Inaltérabilité des dossiers et absence de fonctionnalité permettant d'effacer les transactions/contenus

Selon l'application DLT et le type de données, la réglementation prévoit l'obligation d'effacer les données personnelles. Cette obligation figure dans la loi et la réglementation, ce qui peut être en contradiction avec l'inaltérabilité des systèmes DLT.

NOTE – Le "droit à l'oubli" inscrit dans l'Article 17 du Règlement général sur la protection des données [b-GDPR] adopté par l'UE est un exemple de cette obligation d'effacement des données.

La réglementation applicable à la protection des données et d'autres textes de loi pourraient également exiger de pouvoir corriger les transactions, ce qui n'est possible que grâce à des bifurcations qui mettent en danger la fiabilité des systèmes DLT.

### 7.3 Menaces de sécurité

Les menaces visant la sécurité des composants DLT sont décrites dans les § 5.1 (menaces visant les protocoles), 5.2 (menaces visant les réseaux) et 5.3 (menaces visant les données) de [UIT-T X.1401].

### 7.4 Perte de jetons, de monnaie numérique et d'autres actifs

La perte de jetons, de monnaie numérique et d'autres actifs découle souvent de menaces visant les données. Toutefois, ces pertes pourraient également être dues à des escroqueries intentionnelles faisant intervenir des pièces frauduleuses, des systèmes DLT frauduleux ou l'entité derrière les adresses des comptes. Des attaques par hameçonnage pourraient également amener des personnes à faire des transactions qu'elles n'auraient pas effectuées autrement.

### 7.5 Délits financiers et autres délits

Les systèmes de registres distribués peuvent être utilisés pour commettre des délits financiers, tels que le blanchiment de capitaux, ou pour faciliter la commission d'autres délits comme les attaques par rançongiciel, entre autres. Les transactions pourraient contenir des contenus illégaux qui respectent les règles du protocole mais sont incompatibles avec la réglementation et d'autres textes de loi.

## 8 Capacités techniques pour l'adaptation à la réglementation

### 8.1 Cadre technique

La conception du cadre technique permettant l'adaptation de la technologie DLT à la réglementation est étroitement liée aux caractéristiques de cette technologie comprenant la décentralisation, l'autonomie, l'inaltérabilité, l'ouverture, la transparence et l'anonymat. Les capacités techniques pour

l'adaptation de la technologie DLT à la réglementation sont définis des points de vue suivants: niveau d'application, respect de la vie privée/confidentialité, effacement des données, sécurité des données et niveau de base. Dans les systèmes DLT avec permission, les responsabilités sont essentielles et il est recommandé aux fournisseurs de services DLT de définir une entité juridique d'orchestration sous-jacente pour réduire l'incertitude des mesures réglementaires.

### 8.2 Capacités au niveau des applications

– Il est recommandé que les systèmes DLT qui sont utilisés pour transférer des actifs numériques comprennent un module qui prend en charge les règles définies par le GAFI et/ou les réglementations nationales particulières.

– Il est recommandé que les systèmes DLT avec permission prennent en charge des fonctionnalités de connaissance des clients (KYC) et de lutte contre le blanchiment de capitaux (AML) grâce à l'utilisation de technique telles que les signatures fondées sur l'infrastructure de clé publique (PKI).

– Les fournisseurs de services DLT et les développeurs de systèmes DLT peuvent, à titre d'option, utiliser des techniques telles que la limitation des droits des transactions et le blocage de comptes pour intervenir dans les transactions créées par des nœuds malveillants ou ayant un comportement anormal.

– Les fournisseurs de services DLT et les développeurs de systèmes DLT peuvent, à titre d'option, fournir un lien vers une infrastructure PKI officiellement reconnue. Cette solution peut, à titre d'option, être utilisée pour identifier les transactions avec une entité juridique.

### 8.3 Capacités en matière de protection de la vie privée/confidentialité

– Il est recommandé qu'un système DLT ne publie pas d'informations confidentielles ou de données personnelles, y compris les informations d'identité bancaire, les données personnelles/informations d'identification personnelle, les données relatives aux transactions, les informations relatives aux actifs numériques et les autres informations confidentielles, à moins que leur publication soit justifiée.

– Il n'est pas recommandé de stocker des données contenant ce type d'information dans un système DLT sans permission. S'il est nécessaire qu'un système DLT vérifie ce type de données, il est recommandé de ne stocker qu'un engagement ou un autre justificatif de données dans le système DLT.

– S'il n'est pas possible de ne pas stocker ces données dans un système DLT, il est recommandé d'utiliser des méthodes de chiffrement telles que les justificatifs à apport nul de connaissance, la confusion de comptes ou des méthodes reposant sur l'isolement matériel (environnement TEE) pour protéger les données confidentielles (données commerciales ou données personnelles) contre la divulgation.

– Il est recommandé de sécuriser correctement les données confidentielles stockées en dehors de la chaîne grâce à des méthodes de chiffrement appropriées.

– Il est recommandé que les systèmes DLT dans lesquels des informations confidentielles sont stockées offrent des contrôles d'accès adaptés afin de garantir que seul un accès autorisé est possible. Il est recommandé de limiter l'accès aux utilisateurs qui sont autorisés et/ou aux situations dans lesquelles l'accès est autorisé.

– Il est recommandé d'utiliser des méthodes de contrôle d'accès appropriées pour le stockage en dehors de la chaîne.

– Il est possible, à titre d'option, d'utiliser le chiffrement, des justificatifs à apport nul de connaissance et des fonctions de hachage cryptographique pour sécuriser les informations dans la chaîne. Toutefois, le caractère inaltérable du stockage dans la chaîne pose le problème de l'impossibilité de bloquer les méthodes d'accès compromis. Il est recommandé d'effectuer une analyse des risques et/ou une analyse des incidences sur la protection des données pour ce qui est du stockage de données confidentielles/personnelles dans la chaîne.

### 8.4 Capacités d'effacement des données

L'une des caractéristiques essentielles des systèmes de registres distribués est un niveau élevé d'inaltérabilité. La suppression pure et simple de l'inaltérabilité reviendrait à supprimer la raison ayant motivé le choix initial d'utiliser un système de registres distribués.

Lorsqu'il n'est pas souhaitable que tous les attributs d'une transaction soient inaltérables, il est recommandé de stocker les données en dehors de la chaîne et de seulement les valider, par exemple, en stockant un justificatif de validation des données en dehors de la chaîne. À cet effet, des technologies telles que les justificatifs à apport nul de connaissance, un engagement des données ou une valeur de hachage peuvent, à titre d'option, être stockées dans la chaîne. Il est obligatoire de veiller avec soin à ce qu'aucune information ne devant pas être divulguée ne puisse être déduite des données stockées dans la chaîne.

Dans certains cas d'utilisation, la vérification des données en dehors de la chaîne pourrait ne pas suffire et la conservation des données est nécessaire. Toutefois, cette conservation pourrait être requise pour une période donnée ou lorsque certaines conditions sont réunies. Ces cas d'utilisation sont, par exemple, les données de transaction qui doivent être préservées uniquement tant qu'il n'y a pas de transaction suivante et les dossiers qui doivent être préservés pendant une période donnée (par exemple, 10 ans). Dans ces cas, on peut, à titre d'option, établir un registre distribué qui supprime automatiquement ces données lorsque la transaction suivante a été menée à bien ou à la fin de la période prévue. Des techniques telles que l'élagage [b-Nakamoto] ou le hachage caméléon [b-Camenisch] peuvent, à titre d'option, être utilisées.

Lorsque ces technologies sont utilisées,

– il faut définir de manière claire les parties du registre qui doivent rester inaltérables;
– il faut définir de manière claire les conditions dans lesquelles les autres parties peuvent être modifiées;
– le protocole utilisé par le registre distribué doit définir les modalités à utiliser pour effacer ces données;
– le protocole utilisé par le registre distribué doit garantir que les données qu'il est obligatoire de ne pas effacer ou de ne pas modifier sont toujours protégées contre les modifications;
– il faut garantir que les copies d'archive du registre ne seront conservées que conformément à la réglementation applicable.

L'objectif de l'effacement des données est de se conformer aux prescriptions réglementaires prévues dans les textes de loi, aux recommandations ou aux autres exigences existant au niveau local. Il est recommandé que la fonctionnalité d'effacement soit limitée à une partie des données afin que la confiance dans l'inaltérabilité du reste des données soit maintenue.

### 8.5 Capacités relatives à la sécurité des données

– Il est recommandé que les fournisseurs de services DLT et les développeurs de systèmes DLT garantissent que la conception des systèmes DLT utilisant le chiffrement ou d'autres technologies respectent les exigences en matière de sécurité et de qualité de fonctionnement des services DLT, notamment la fiabilité, le caractère complet et l'inaltérabilité, en particulier en utilisant des algorithmes de chiffrement et des mécanismes de consensus appropriés.

– Il est recommandé que les fournisseurs de services DLT et les développeurs de systèmes DLT garantissent la cohérence des données dans la chaîne.

### 8.6 Capacité concernant le niveau de base

– Il est recommandé que les fournisseurs de services DLT et les développeurs de systèmes DLT veillent comme il se doit à garantir l'intégrité, la confidentialité, l'exécution, la disponibilité et l'utilisation des réseaux DLT.

– Il est recommandé que les développeurs de systèmes DLT parent aux menaces visant les réseaux grâce à un cadre de sécurité approprié.

– Les fournisseurs de services DLT et les développeurs de systèmes DLT peuvent, à titre d'option, utiliser des méthodes telles que l'augmentation de la puissance de calcul ou l'empilement de ressources pour empêcher les attaques visant les consensus.

– Il est recommandé que les fournisseurs de services DLT et les développeurs de systèmes DLT prennent en charge la sécurité des contrats intelligents exécutés sur les systèmes DLT grâce à la vérification formelle ou à d'autres méthodes de détection des vulnérabilités.

– Les développeurs de systèmes DLT peuvent, à titre d'option, concevoir une tolérance aux pannes dans les systèmes DLT contre les nœuds malveillants. Il est recommandé que le système DLT se rétablisse lorsqu'un ensemble de nœuds normaux dysfonctionnent ou deviennent des nœuds malveillants.

# Bibliographie


[b-UIT-T J.160] Recommandation UIT-T J.160 (2005), *Cadre architectural pour l'acheminement de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

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

[b-Camenisch] Camenisch J., Derler D., Kernn S., Pöhls H.C., Samelin K., and Slamanig D. (2017), *Chameleon-hashes with ephemeral trapdoors and Applications to Invisible Sanitizable Signatures*, Public-Key Cryptography, Berlin, Springer, pp. 152–182. https://doi.org/10.1007/978-3-662-54388-7_6.

[b-DIN SPEC 4997] DIN SPEC 4997 (2020), *Privacy by blockchain design: A standardised model for processing personal data using blockchain technology*.

[b-DLT 4.1] UIT-T HSTP.DLT-RF (2019), *Technologie des registres distribués: cadre réglementaire*.

[b-GDPR] Règlement général sur la protection des données de l'Union européenne, Article 17, *Droit à l'effacement ("droit à l'oubli")*, https://gdpr.eu/article-17-right-to-be-forgotten/.

[b-ISO/IEC 27000] ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-Nakamoto] Nakamoto S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

# 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 | Équipements 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 |

Published in Switzerland
Geneva, 2023