ITUPublications
Recommandations

Union Internationale des Télécommunications
Secteur de la Normalisation

Recommandation

UIT-T X.1411 (03/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

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

Lignes directrices relatives à la sécurité de la chaîne de blocs en tant que service

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.1411

Lignes directrices relatives à la sécurité de la chaîne de blocs en tant que service

Résumé

La Recommandation UIT-T X.1411 contient des lignes directrices génériques sur la sécurité de la chaîne de blocs en tant que service. En premier lieu, les menaces et les failles sur le plan de la sécurité de la chaîne de blocs en tant que service sont analysées, puis les mesures de sécurité de la chaîne de blocs en tant que service sont indiquées. La présente Recommandation porte également sur les exigences en matière de sécurité et fournit des lignes directrices pour toutes les activités liées à la création, au fonctionnement et à l'utilisation de la chaîne de blocs en tant que service.

La chaîne de blocs en tant que service est désormais couramment utilisée dans le développement de la chaîne de blocs, en raison des capacités prometteuses qu'offre cette technologie et de l'appui massif dont elle fait l'objet dans le secteur, en particulier de la part des grands fournisseurs de services d'informatique en nuage. La chaîne de blocs en tant que service fournit le service et les ressources fondamentaux pour les applications de la chaîne de blocs; toutefois, elle est associée à des problèmes sur le plan de la sécurité, liés aux technologies de base de la chaîne de blocs et aux plates-formes d'informatique en nuage. Dans ce contexte, il est essentiel et nécessaire d'avoir des orientations concernant la sécurité de la chaîne de blocs en tant que service.

Historique *

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	**UIT-T X.1411**	**03-03-2023**	**17**	**11.1002/1000/15110**

Mots clés

Chaîne de blocs en tant que service, environnement d'informatique en nuage, protocole de consensus, contrat intelligent, sécurité

* 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/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1411

Lignes directrices relatives à la sécurité de la chaîne de blocs en tant que service

1 Domaine d'application

La présente Recommandation contient des lignes directrices relatives à la sécurité de la chaîne de blocs en tant que service. Elle décrit les définitions, la structure, les menaces et les failles sur le plan de la sécurité, ainsi que les mesures relatives à la chaîne de blocs en tant que service. La sécurité des applications fondées sur la chaîne de blocs en tant que service n'entre pas dans le cadre de la présente Recommandation.

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. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute recommandation ou autre référence étant sujette 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. 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 de Recommandation.

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

[UIT-T X.1601] Recommandation UIT-T X.1601 (2019), *Cadre de sécurité applicable à l'informatique en nuage*.

3 Définitions

3.1 Termes définis par ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 chaîne de blocs en tant que service [b-UIT-T Y.3530]: catégorie de services en nuage dans laquelle les capacités fournies au client des services en nuage sont la création de plates-formes fondées sur la chaîne de blocs et la création d'applications décentralisées au moyen des technologies fondées sur la chaîne de blocs.

3.1.2 client de services en nuage [b-UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de services en nuage.

3.1.3 fournisseur de services en nuage [b-UIT-T Y.3500]: partie qui met à disposition des services en nuage.

3.1.4 partenaire de services en nuage [b-UIT-T Y.3500]: partie fournissant un appui ou une aide pour les activités d'un fournisseur de services en nuage, d'un client de services en nuage, ou des deux.

3.1.5 consensus [b-UIT-T X.1400]: accord selon lequel un ensemble de transactions est valable.

3.1.6 d'homologue à homologue [b-ISO 22739]: réseau d'homologues échangeant directement des informations et des ressources l'un avec l'autre, sans dépendre d'une entité centrale, utilisation d'un tel réseau ou lien avec un tel réseau.

3.1.7 preuve de travail [b-UIT-T X.1400]: processus de consensus visant à résoudre un problème difficile (coûteux ou chronophage) qui produit un résultat facile à vérifier par des tiers.

3.1.8 contrat intelligent [b-UIT-T X.1400]: programme écrit sur le système de registre distribué, qui codifie les règles pour des types particuliers de transactions de système de registre distribué, de telle manière que ces transactions peuvent être validées ou exécutées lorsque des conditions particulières sont réunies.

3.1.9 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

La présente Recommandation définit les termes suivants:

3.2.1 attaque des 51%: attaque dans laquelle les auteurs d'une attaque contrôlent suffisamment de nœuds de la chaîne de blocs ou suffisamment de ressources informatiques pour révoquer ou réécrire le registre du système de registre distribué, en contrôlant la création des blocs.

3.2.2 subdivision du réseau: scénario de connexion de réseau dans lequel le réseau est divisé en plusieurs parties déconnectées.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

BaaS chaîne de blocs en tant que service (*blockchain as a service*)

BSC client de la chaîne de blocs en tant que service (*chaîne de blocs as a service customer*)

BSD développeur de la chaîne de blocs en tant que service (*blockchain as a service developer*)

BSP fournisseur de la chaîne de blocs en tant que service (*blockchain as a service provider*)

BSS développeur de la sécurité de la chaîne de blocs en tant que service (*blockchain as a service security developer*)

CPU unité centrale de traitement (*central processing unit*)

CSC client de services en nuage (*cloud service customer*)

CSN partenaire de services en nuage (*cloud service partner*)

CSP fournisseur de services en nuage (*cloud service provider*)

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

GPU unité de traitement graphique (*graphics processing unit*)

IAM gestion des identités et des accès (*identity and access management*)

P2P d'homologue à homologue (*peer-to-peer*)

PII informations d'identification personnelle (*personally identifiable information*)

PoW preuve de travail (*proof of work*)

SDK kit de développement logiciel (*software development kit*)

5 Conventions

L'expression "**il est nécessaire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

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.

L'expression "**peut, à titre d'option**", indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée 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.

Dans le corps de la présente Recommandation et dans ses annexes, on trouve parfois les expressions **doit**, **ne doit pas**, **devrait et peut**. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est nécessaire, il est interdit, il est recommandé et peut, à titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Aperçu de la sécurité de la chaîne de blocs en tant que service

La chaîne de blocs en tant que service *fournit un environnement de développement intégré dans lequel les développeurs et les clients de la chaîne de blocs peuvent créer, développer, tester, héberger, déployer et exploiter des applications liées à la chaîne de blocs.* Dans ce contexte, les clients de la chaîne de blocs en tant que service (BaaS) peuvent utiliser les composants essentiels de la plate-forme BaaS pour permettre une utilisation efficace et un déploiement facile des réseaux et des applications de la chaîne de blocs.

Dans la mesure où la plate-forme et le service fondamentaux de la chaîne de blocs s'appuient sur le service d'informatique en nuage, trois principaux acteurs jouent un rôle dans le fonctionnement de la chaîne de blocs en tant que service, ce qui correspond aux rôles liés au service d'informatique en nuage.

- **Fournisseur de la chaîne de blocs en tant que service (BSP)**: de la même manière que pour les fournisseurs de services en nuage (CSP) dans l'environnement de l'informatique en nuage, les fournisseurs BSP sont notamment des fournisseurs d'infrastructures et de plates-formes de la chaîne de blocs, qui mettent à disposition la chaîne de blocs en tant que service. Les fournisseurs BSP simplifient le développement et l'utilisation de la chaîne de blocs et des applications, au moyen de ressources et de fonctions fondamentales liées à la chaîne de blocs en ce qui concerne le stockage, la communication, le calcul et l'appui à la mise en réseau. Le fournisseur BSP est responsable de la sécurité des ressources fondamentales de la chaîne de blocs et du développement des outils fournis pour les autres rôles intervenant dans la chaîne de blocs en tant que service.
- **Développeur de la chaîne de blocs en tant que service (BSD)**: de la même manière que pour le partenaire des services en nuage (CSN) dans l'environnement de l'informatique en nuage, le développeur BSD intervient dans le développement et l'exploitation des composants essentiels de la chaîne de blocs en tant que service, afin d'aider le fournisseur BSP à fournir un service fondé sur la chaîne de blocs. Le développeur BSD est chargé de la sécurité la sécurité des composants essentiels développés.
  - **Développeur de la sécurité de la chaîne de blocs en tant que service (BSS)**: il s'agit d'un type particulier de développeur BSD. Le développeur BSS aide le développeur BSP à renforcer la sécurité de la chaîne de blocs en tant que service, en tant que fournisseur de services de sécurité tiers. Les services de sécurité fournis par le développeur BSS comprennent notamment la gestion des identités et des accès (IAM), l'audit, la détection des intrusions et d'autres services.
- **Client de la chaîne de blocs en tant que service (BSC)**: comme dans le cas des clients de services en nuage (CSC) dans l'environnement de l'informatique en nuage, les clients BSC sont des clients de la chaîne de blocs qui demandent et utilisent le service ou la ressource de la chaîne de blocs et qui y accèdent au moyen des fonctions fournies directement par le fournisseur BSP, ou via les applications et des services fournis indirectement par le

développeur BSD indirectement. Le client BSC est responsable du respect des règles de sécurité fournies par le fournisseur BSP pour l'exploitation de son propre réseau et ses propres applications fondés sur la chaîne de blocs. Le client BSC est également encouragé à coopérer avec le fournisseur BSP pour surveiller la sécurité des réseaux de la chaîne de blocs personnalisés et signaler les incidents de sécurité si nécessaire.

Les interactions entre ces rôles sont présentées dans la Figure 1.

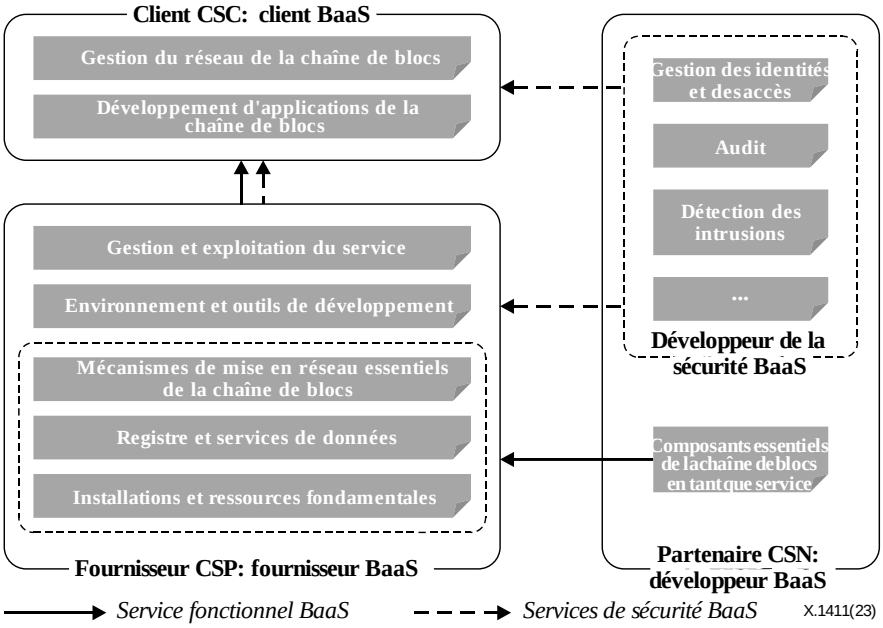

Figure 1 – Fonctions et interactions des rôles dans la chaîne de blocs en tant que service

6.1 Aperçu de la sécurité au niveau des fournisseurs BSP

Le fournisseur BSP fournit les fonctions essentielles de la chaîne de blocs, notamment en ce qui concerne les contrats intelligents, les protocoles de consensus, les connexions d'homologue à homologue (P2P), les algorithmes cryptographiques, les enregistrements des transactions, la gestion du registre, la gestion des nœuds et des ressources, ainsi que la prise en charge d'interfaces de développement et de services de sécurité normalisés. Les fonctions du fournisseur BSP et les problèmes de sécurité connexes sont les suivants:

6.1.1 Installations et ressources fondamentales

Le fournisseur BSP fournit des installations fondamentales pour mettre à disposition des ressources de calcul et de communication et d'autres ressources de base à l'appui de la mise en réseau et du développement d'applications fondés sur la chaîne de blocs. Ces installations peuvent être des dispositifs physiques ou des dispositifs virtualisés, tels que des machines et des conteneurs virtuels.

Les installations fondamentales sont exposées à des problèmes, tels que des risques environnementaux liés aux installations physiques, l'injection de portes dérobées, les ressources partagées entre les locataires, etc.

6.1.2 Registre et services de données

Le fournisseur BSP fournit des services de données à la fois sur la chaîne et en dehors de la chaîne, par exemple pour le stockage, la gestion, l'interrogation des données client et des données système pour le client BSC. Dans ce contexte, le registre de données sur la chaîne de blocs garantit la résistance face aux tentatives d'altération, tandis que la base de données en dehors de la chaîne assure des services de données efficaces.

Sur le plan de la sécurité des données, le fournisseur BSP est confronté aux difficultés suivantes:

– l'indisponibilité des services de données, notamment l'incohérence du stockage des données sur la chaîne et en dehors de la chaîne due aux partitions du réseau, la perte de données causée par une défaillance de la base de données et des installations de stockage, la modification non autorisée du registre de données, etc.;
– les fuites de données confidentielles, notamment l'accès non autorisé à des données personnelles, l'obtention d'informations sensibles à partir des données, l'échec de la destruction des données confidentielles, etc.

6.1.3 Mécanismes de mise en réseau essentiels de la chaîne de blocs

Le fournisseur BSP fournit un ensemble d'options au niveau des mécanismes de mise en réseau essentiels de la chaîne de blocs, afin de simplifier la mise en place de réseaux personnalisés sur la chaîne de blocs. Les mécanismes de mise en réseau essentiels de la chaîne de blocs comprennent des protocoles de consensus, des protocoles de connexion P2P et des algorithmes cryptographiques. Le client BSC peut choisir un ensemble particulier de composants de mise en réseau parmi toutes les options et définir les paramètres correspondants pour mettre rapidement en place un réseau personnalisé sur la chaîne de blocs.

Le fournisseur BSP est chargé de résoudre les problèmes de sécurité liés aux mécanismes de mise en réseau essentiels de la chaîne de blocs. Ces problèmes portent atteinte à la sécurité des réseaux personnalisés sur la chaîne de blocs et même aux applications de la chaîne de blocs qui sont fondées sur la plate-forme de la chaîne de blocs en tant que service (BaaS), car le client BSC utilise directement les mécanismes de mise en réseau essentiels de la chaîne de blocs pour concevoir des réseaux et des applications fondés sur la chaîne de blocs. Parmi les problèmes de sécurité, on peut citer l'accès non autorisé aux ressources de la chaîne de blocs, les partitions du réseau, les nœuds malveillants, etc. À titre d'exemple, les partitions de réseau causées par l'indisponibilité des services de chaîne de blocs peuvent entraîner un retard inacceptable dans l'obtention d'un consensus au sein du réseau de la chaîne de blocs distribué.

6.1.4 Environnement et outils de développement

Le fournisseur BSP fournit un environnement de développement intégré doté d'une interface de programmation d'applications (API), d'une boîte à outils de développement et d'autres outils de développement, pour simplifier le développement d'applications fondées sur la chaîne de blocs. Dans la mesure où le contrat intelligent constitue un mécanisme instinctif pour le développement d'applications fondées sur la chaîne de blocs, le fournisseur BSP simplifie également le déploiement des contrats intelligents et fournit un ensemble de contrats intelligents pour les fonctions communes, telles que la gestion des identités et des accès.

Parmi les difficultés connexes, on peut citer le contrôle inapproprié de l'accès aux interfaces API, l'incompatibilité des interfaces, l'exécution imprévue des contrats intelligents, etc.

6.1.5 Gestion et fonctionnement des services

Le fournisseur BSP est chargé de surveiller l'état du service chaîne de blocs et de créer des alertes à ce sujet, en ce qui concerne les installations physiques, les nœuds de la chaîne de blocs, les connexions réseau et les ressources allouées, ainsi que la gestion des identités et des accès et d'autres fonctions de gestion de la sécurité. Le fournisseur BSP appuie et gère également les fonctions liées à la chaîne de blocs fournies par développeur BSD.

Les problèmes de sécurité connexes comprennent notamment l'indisponibilité des fonctions de gestion, la gestion inappropriée des accès, l'accès non autorisé aux fonctions d'administration, une explosion des ressources consommées et les risques liés aux composants de la chaîne de blocs fournis par le développeur BSD.

6.2 Aperçu de la sécurité au niveau des développeurs BSD

Le développeur BSD met au point les composants de base de la chaîne de blocs en tant que service pour le fournisseur BSP ou fournit des services de sécurité pour tous les rôles.

6.2.1 Conception des composants de base de la chaîne de blocs en tant que service

Le développeur BSD fournit les composants de base de la chaîne de blocs en tant que service, tels que les contrats intelligents, les algorithmes cryptographiques, les protocoles de consensus et les algorithmes cryptographiques, en tant que fournisseur tiers.

Les défis et les menaces connexes en matière de sécurité comprennent l'incompatibilité des interfaces, des conceptions de protocoles non sécurisées, des portes dérobées au niveau de la mise en œuvre des protocoles, etc.

6.2.2 Services de sécurité

Le développeur BSS fait fonction de fournisseur de services de sécurité tiers pour tous les rôles de l'écosystème BaaS. Par exemple, le développeur BSS peut assurer la détection des intrusions pour le compte des fournisseurs BSP, l'audit du code pour les développeurs BSD et la gestion des identités et des accès pour les clients BSC.

Parmi les problèmes de sécurité, on peut citer l'obsolescence des règles de sécurité ou l'inadéquation des opérations effectuées par les employés du développeur BSS, notamment.

6.3 Aperçu de la sécurité au niveau des clients BSC

Le client BSC utilise les services fournis par le fournisseur BSP et le développeur BSD pour mettre en place un réseau personnalisé et des applications fondés sur la chaîne de blocs. Il existe deux types de clients BSC: d'une part, les administrateurs, qui construisent et gèrent des réseaux personnalisés fondés sur la chaîne de blocs, et d'autre part, les membres, qui rejoignent un réseau personnalisé fondé sur la chaîne de blocs. Un client BSC donné peut être à la fois l'administrateur d'un réseau personnalisé fondé sur la chaîne de blocs et le membre d'un autre réseau personnalisé fondé sur la chaîne de blocs.

Tous les types de clients BSC sont confrontés à des problèmes de sécurité au niveau de la gestion et de l'utilisation des clés. L'administrateur est aussi confronté à des problèmes de sécurité lors de la mise en place et de la gestion de réseaux personnalisés fondés sur la chaîne de blocs, tels que le paramétrage inapproprié des nœuds, des connexions et d'autres ressources de la chaîne de blocs.

7 Menaces sur le plan de la sécurité de la chaîne de blocs en tant que service

Les menaces auxquelles sont exposés les fournisseurs BSP, les développeurs BSD et les clients BSC relèvent de trois catégories:

– conceptions techniques non sécurisées, défauts au niveau de la mise en œuvre et gestion inappropriée des ressources fondamentales, des fonctions centrales de la chaîne de blocs et des systèmes de services de la chaîne de blocs;

– interactions non sécurisées entre le client BSC, le développeur BSD et le fournisseur BSP, notamment des interfaces incompatibles, et chaîne d'approvisionnement non sécurisée;

– opérations inappropriées des employés, y compris l'utilisation et le stockage inappropriés des mots de passe.

Les menaces relatives à la sécurité pour chaque rôle sont présentées aux paragraphes 7.1 à 7.3.

7.1 Menaces liées à la sécurité des fournisseurs BSP

7.1.1 Menaces pour les services d'informatique en nuage

Dans la mesure où le fournisseur BSP fournit des ressources fondamentales de la chaîne de blocs, en s'appuyant sur des services d'informatique en nuage, le fournisseur BSP est confronté à des problèmes et des menaces propres au service d'informatique en nuage, comme indiqué dans les paragraphes 7 et 8 de la Recommandation [UIT-T X.1601]. À titre d'exemple, l'accès non autorisé à une partition de la ressource d'un autre locataire, dans l'environnement partagé des services en nuage, peut entraîner des embranchements de la chaîne de blocs au niveau du système de chaîne de blocs de ce locataire, en réécrivant ou en révisant ses registres de données.

7.1.2 Menaces liées aux mécanismes de mise en réseau essentiels de la chaîne de blocs

Les menaces auxquels sont exposés les protocoles de consensus, les protocoles de connexion P2P et les moteurs de chiffrement peuvent trouver leur source dans des vulnérabilités au niveau de la conception des protocoles, des failles dans la mise en œuvre des mécanismes et une gestion inappropriée. On trouvera des informations détaillées au paragraphe 6 de la Recommandation [UIT-T X.1401].

7.1.3 Défaut de fiabilité du service de données

Les menaces liées au registre de données distribués concernent notamment l'insuffisance des ressources de la chaîne de blocs, les failles au niveau du système de stockage et une gestion non sécurisée du stockage, qui peuvent entraîner un enregistrement incohérent des données, la perte de données, l'altération des données et la fuite de données. Par exemple, les données système et les données relatives à la chaîne de blocs d'un réseau personnalisé fondé sur la chaîne de blocs s'étendent lorsque le réseau est en fonctionnement. Lorsque le fournisseur BSP ne fournit pas suffisamment de ressources de stockage au réseau personnalisé fondé sur la chaîne de blocs pour faire face à l'expansion des données, le réseau personnalisé écrase les anciennes données avec les nouvelles données ou abandonne directement les nouvelles données, entraînant la perte de données dans le réseau. On peut aussi citer un autre exemple, dans lequel les défaillances au niveau des installations de communication ou de stockage peuvent entraîner un stockage incohérent des données au niveau des registres de données distribués. En cas de défaillance prolongée, les partitions de réseau ainsi créées entraînent des retards inattendus dans la génération des blocs, la consultation des données et d'autres services de données.

7.1.4 Menaces liées à l'environnement de développement

L'environnement de développement intégré, l'environnement de compilation, les contrats intelligents, les interfaces API, le kit de développement logiciel (SDK) et d'autres fonctions liées à l'accessibilité de développement fournies par le fournisseur BSP sont exposés à des menaces au niveau du processus de conception, de mise en œuvre, de configuration et d'exploitation de ces fonctions de développement. Par exemple, les défauts d'authentification de l'interface API peuvent entraîner un accès non autorisé à la ressource fondamentale de la chaîne de blocs et une utilisation non autorisée de cette ressource. Par ailleurs, les contrats intelligents présentent des vulnérabilités en matière de sécurité au niveau de la conception logique, de la mise en œuvre des contrats et de la gestion du code, telles que le dépassement d'entiers positifs ou négatifs dans un contrat intelligent, qui peut entraîner des résultats d'exécution inattendus.

7.1.5 Fonctions tierces non sécurisées

Le fournisseur BSP prend en charge les fonctions tierces fournies par le développeur BSD et les intègre dans la plate-forme BaaS au moyen d'interfaces API. Dans ce contexte, l'existence de failles et de logiciels malveillants dans les fonctions tierces, l'incompatibilité des interfaces API et l'inadéquation du contrôle d'accès aux interfaces API peuvent entraîner des dysfonctionnements dans le système BaaS.

7.1.6 Accès non sécurisé au système

L'accès non sécurisé au système comprend le défaut de contrôle d'accès ou le caractère inapproprié du contrôle d'accès aux installations, au registre de données, au réseau et aux applications de la chaîne de blocs. Il peut donner lieu à l'altération des données de la chaîne de blocs, à des intrusions dans des réseaux personnalisés fondés sur la chaîne de blocs et à la fuite d'informations privées.

7.1.7 Menaces internes

Les employés du fournisseur BSP peuvent, de manière accidentelle ou délibérée, avoir des comportements malveillants, par exemple en partageant des mots de passe avec des personnes non autorisées, en laissant apparaître des mots de passe à des endroits qui ne sont pas sécurisés, en exposant des informations personnelles, etc. Les menaces internes peuvent entraîner la fuite d'informations privées, l'accès non autorisé à des réseaux personnalisés fondés sur la chaîne de blocs et l'indisponibilité des services de la chaîne de blocs.

7.1.8 Défaut de fiabilité de la chaîne d'approvisionnement

La plate-forme de services de la chaîne de blocs utilise des composants logiciels et matériels fournis par différents fournisseurs. Un arrêt de l'approvisionnement en éléments logiciels et matériels compromet les capacités de calcul, les connexions et les autres ressources des services de chaîne de blocs. Dans ce cas, la disponibilité des services des chaîne de blocs est menacée. Par exemple, le protocole de consensus de la preuve de travail repose sur la concurrence des capacités de calcul entre les nœuds de chaîne de blocs en ligne. Par conséquent, la rupture au niveau des capacités de calcul et de connexion peut avoir des incidences sur les résultats de consensus des réseaux de la chaîne de blocs fondés sur la preuve de travail.

En outre, les logiciels malveillants et les vulnérabilités exploitables dans les éléments logiciels et matériels, ainsi que dans les architectures de la chaîne de blocs à code source ouvert, pourraient entraîner la création imprévue de blocs, des dénis de service, des fuites de données, des utilisations abusives, etc.

7.1.9 Menaces liées à l'environnement physique

Les incendies, les inondations, les orages et d'autres catastrophes environnementales touchant les installations fondamentales peuvent entraîner l'indisponibilité des installations physiques fournissant les communications, les calculs et d'autres ressources fondamentales. Par exemple, une panne d'alimentation délibérée ou accidentelle peut entraîner la mise hors ligne d'une partition de nœuds de la chaîne de blocs. Dans ce cas, le processus de consensus est contrôlé par un plus petit nombre de nœuds de la chaîne de blocs, ce qui entraîne des résultats de consensus incorrects et un retard supplémentaire dans la génération des blocs.

7.2 Les menaces liées à la sécurité des développeurs BSD

7.2.1 Menaces visant les fonctions tierces

Le développeur BSD fournit des composants de base de la chaîne de blocs, des mécanismes de sécurité de la chaîne de blocs et des fonctions de développement d'applications de la chaîne de blocs, en tant que fournisseur tiers. Les menaces connexes comprennent les vulnérabilités de sécurité inhérentes aux composants essentiels de la chaîne de blocs, les défauts de mise en œuvre de ces fonctions tierces, les interfaces incompatibles et le contrôle d'accès non sécurisé des interfaces.

En outre, le comportement malveillant éventuel des employés du développeur BSD peut aussi donner lieu à la fuite d'informations privées, à des portes dérobées dans des fonctions tierces et à des opérations inattendues des fonctions de sécurité.

7.3 Menaces de sécurité auxquelles est exposé le client de la chaîne de blocs en tant que service (client BSC)

7.3.1 Fuite et perte de clés

La gestion des clés est assurée par le client BSC lui-même ou par un service tiers. Le mauvais stockage des clés, la corruption d'un fichier de clés ou le manque de fiabilité d'un service de clés tiers peuvent être à l'origine d'une perte ou d'une fuite de clés, qui se traduit par une perte d'actifs pour le client BSC, la divulgation de données privées et la perturbation des réseaux de chaînes de blocs personnalisées.

7.3.2 Mauvaise gestion des réseaux de chaînes de blocs personnalisées

Le client BSC crée ses propres réseaux de chaînes de blocs personnalisées et déploie des mécanismes de sécurité reposant sur les fonctions de la chaîne de blocs assurées par le fournisseur BSP et le développeur BSD. C'est pourquoi une mauvaise configuration des réseaux de chaînes de blocs et des mécanismes de sécurité menacera les réseaux de chaînes de blocs. Par exemple, si le client BSC n'alloue pas suffisamment de ressources de stockage pour l'exploitation du réseau de chaînes de blocs personnalisées, il se peut que ledit réseau échoue à mettre à jour les données de la chaîne de blocs, ce qui entraînera *in fine* une incohérence entre les registres de données des chaînes de blocs.

8 Exigences de sécurité de la chaîne de blocs en tant que service

8.1 Configuration de la sécurité d'un réseau de chaînes de blocs personnalisées

Il est recommandé que le fournisseur BSP donne des recommandations sur les configurations propres au réseau de chaînes de blocs personnalisées afin de répondre aux exigences de sécurité du client BSC. Il est également recommandé que le fournisseur BSP formule des recommandations sur le déploiement des mécanismes de sécurité nécessaires aux réseaux de chaînes de blocs personnalisées.

a) Il est nécessaire que le fournisseur BSP spécifie la fourchette recommandée pour le nombre total de nœuds.

b) Il est nécessaire que le fournisseur BSP spécifie le nombre minimum de nœuds à avoir en ligne pour éviter les attaques à 51%, ainsi que les autres menaces connues auxquelles est exposé le réseau de chaînes de blocs.

c) Il est nécessaire que le fournisseur BSP spécifie le nombre minimum de voisins pour chaque nœud afin d'éviter la partition du réseau de chaînes de blocs.

d) Il est recommandé que le fournisseur BSP spécifie les types de nœuds recommandés ainsi que le nombre préconisé pour chaque type spécifié et les droits qui y sont associés.

e) Il est recommandé que le fournisseur BSP spécifie la ressource de stockage minimum, l'unité centrale de traitement (CPU) et l'unité de traitement graphique (GPU) nécessaires pour chaque type de nœud.

f) Il est recommandé que le fournisseur BSP spécifie les protocoles de consensus et les protocoles d'homologue à homologue en fonction des configurations des nœuds.

g) Il est recommandé que le fournisseur BSP assure les fonctions de sécurité de base, y compris l'IAM et la gestion des clés, du réseau de chaînes de blocs personnalisées.

h) Le fournisseur BSP peut, à titre d'option, assurer l'évaluation de la sécurité des configurations du réseau de chaînes de blocs. À cet égard, il doit apporter au client BSC des suggestions et des solutions en matière de sécurité.

8.2 Gestion des identités et des accès

Il est recommandé que le fournisseur BSP assure les fonctions de gestion des identités et des accès pour le système BaaS et le réseau de chaînes de blocs personnalisées. Les fonctions de gestion des identités et des accès sont déployées non seulement pour protéger les identités, mais aussi pour faciliter les processus de gestion des accès, d'authentification et d'autorisation.

a) Il est nécessaire que le fournisseur BSP assure les fonctions d'enregistrement et de désenregistrement des identités pour le système BaaS.

b) Il est recommandé que le fournisseur BSP assure les fonctions d'enregistrement et de désenregistrement des identités pour le réseau de chaînes de blocs personnalisées.

c) Il est nécessaire que le fournisseur BSP assure la gestion du compte d'accès pour le système BaaS, de manière à différencier le fournisseur BSP, le client BSC, et le développeur BSD.

d) Il est recommandé que le fournisseur BSP assure la gestion des comptes d'accès dans le réseau de chaînes de blocs personnalisées. Tout réseau de chaînes de blocs personnalisées doit avoir un ou plusieurs rôles de client assortis de différents droits d'accès.

e) Il est nécessaire que le fournisseur BSP assure l'authentification de l'accès pour le système BaaS. Chaque identité peut accéder uniquement à la ressource correspondant à son droit d'accès.

f) Il est recommandé que le fournisseur BSP assure l'authentification de l'accès pour le réseau de chaînes de blocs personnalisées.

g) Le fournisseur BSP peut, à titre d'option, assurer des fonctions de gestion de l'accès à granularité fine, notamment les fonctions de contrôle de l'accès fondé sur le rôle.

h) Le fournisseur BSP peut, à titre d'option, surveiller la fréquence d'activité des adresses IP d'accès, des comptes d'accès, des dispositifs d'accès, et autres. Les activités d'accès comprennent notamment l'enregistrement, le désenregistrement et les mises à jour des clés.

8.3 Gestion des clés

Il est recommandé que le fournisseur BSP assure les fonctions de gestion des clés pour protéger la sécurité de la génération, du stockage, de la distribution, de l'utilisation, de la sauvegarde, de la récupération et de la révocation des clés.

a) Il est nécessaire que le fournisseur BSP prévoie des systèmes de gestion de clés complets qui précisent les informations de clés et la procédure de gestion.

b) Il est nécessaire que le fournisseur BSP évalue la sécurité des algorithmes de nombres aléatoires et des autres paramètres qui sont utilisés pour générer des clés. Les algorithmes de nombres aléatoires doivent avoir un caractère aléatoire et imprévisible.

c) Il est recommandé que le fournisseur BSP facilite les fonctions de gestion des clés par une tierce partie. La sécurité des fonctions de gestion des clés par une tierce partie doit être évaluée et garantie avant d'être proposée au client BSC.

d) Il est recommandé que le fournisseur BSP assure les fonctions de révocation des clés pour le désenregistrement des comptes suspects.

e) Il est recommandé que le fournisseur BSP assure les fonctions de récupération de clés en cas de perte de clés. Seuls les comptes authentifiés peuvent accéder aux fonctions de récupération des clés.

f) Il est recommandé que le fournisseur BSP demande au client BSC de procéder régulièrement à une mise à jour des clés. La fréquence de mise à jour doit varier en fonction du niveau de sécurité.

g) Il est recommandé que le client BSC déploie la fonction de gestion de clés dans le réseau de chaînes de blocs personnalisées.

h) Il est nécessaire que le client BSC maîtrise et respecte les procédures de sécurité relatives à l'utilisation, au stockage, à la récupération et à la révocation des clés, conformément à la fonction de gestion des clés déployée dans le réseau de chaîne de blocs personnalisées.

i) Il est recommandé que le client BSC signale toute utilisation suspecte des clés au fournisseur BSP selon la procédure prédéfinie dans la fonction de gestion des clés.

j) Le fournisseur BSP peut, à titre d'option, utiliser un système de stockage de clés bipartite ou multipartite pour les clés principales et les clés secrètes.

8.4 Protection de la vie privée

Il est recommandé que le fournisseur BSP assure la protection de la collecte des informations d'identification personnelle (PII), de l'accès à ces informations et d'autres opérations en lien avec ces informations.

a) Il est nécessaire que le fournisseur BSP respecte la réglementation, les politiques et la législation en vigueur aux niveaux national et local en matière de protection de la vie privée, notamment en ce qui concerne la collecte et le stockage des informations PII.

b) Il est nécessaire que le fournisseur BSP garantisse la désidentification des informations PII affichées.

c) Il est nécessaire que le fournisseur BSP mette en place des mesures de sécurité visant à garantir la possibilité de supprimer totalement des informations PII qui se trouvent sur la chaîne lorsque le client BSC en fait la demande, par exemple en utilisant un algorithme de la fonction de hachage caméléon fondé sur la technologie de la chaîne de blocs, ou qu'il stocke les informations PII en dehors de la chaîne.

d) Il est recommandé que le fournisseur BSP invite les organisations professionnelles à effectuer des audits sur les opérations sensibles liées aux informations PII.

8.5 Sécurité des moteurs cryptographiques

Il est recommandé que le fournisseur BSP garantisse la sécurité des moteurs cryptographiques qui sont déployés dans les réseaux de chaîne de blocs personnalisées.

a) Il est nécessaire que le fournisseur BSP prenne en charge les algorithmes cryptographiques courants dont la sécurité a été vérifiée publiquement.

b) Il est nécessaire que le fournisseur BSP invite des organisations professionnelles à auditer la sécurité des moteurs cryptographiques.

c) Il est recommandé que le fournisseur BSP prenne en charge les moteurs cryptographiques fournis par le développeur BSD. Il est recommandé que le développeur BSD fournisse les résultats de l'évaluation de la sécurité de ses moteurs cryptographiques.

8.6 Sécurité de la connexion entre entités homologues

Il est recommandé que le fournisseur BSP garantisse que les connexions entre entités homologues résistent aux nœuds non fiables et malveillants.

a) Il est nécessaire que le fournisseur BSP prévoie des mécanismes d'authentification pour gérer l'accès aux réseaux entre homologues.

b) Il est nécessaire que le fournisseur BSP utilise la technologie cryptographique pour établir des canaux de transmission sécurisés entre les nœuds distribués.

c) Il est nécessaire que le fournisseur BSP prenne en charge les protocoles échangés entre entités homologues avec fiabilité et modularité. Fiabilité signifie que les nœuds déconnectés conservent leur cohérence avec les autres nœuds après reconnexion. Modularité signifie que les protocoles prennent en charge l'ajout ou la suppression dynamique ou statique de nœuds pendant le fonctionnement normal des réseaux de chaînes de blocs.

d) Il est nécessaire que le fournisseur BSP prenne en charge les protocoles d'homologue à homologue dans tout nœud ayant plus d'un voisin.

e) Il est recommandé que le fournisseur BSP prenne en charge les protocoles d'homologue à homologue de sorte qu'un nœud déconnecté n'entraîne pas de partition du réseau.

f) Il est recommandé que le fournisseur BSP fournisse la topologie en temps réel du réseau entre homologues.

g) Il est recommandé que le fournisseur BSP prévoie une alerte si le réseau entre homologues rencontre des partitions ou des nœuds malveillants.

8.7 Sécurité des mécanismes de consensus

Il est recommandé que le fournisseur BSP garantisse la sécurité de la conception et de l'exploitation du mécanisme de consensus.

a) Il est nécessaire que le fournisseur BSP fournisse les algorithmes de consensus dont la sécurité a été vérifiée ou évaluée publiquement.

b) Il est nécessaire que le fournisseur BSP aide le client BSC à déployer les algorithmes de consensus fournis par le développeur BSD.

c) Il est nécessaire que le fournisseur BSP fournisse au client BSC une évaluation de la sécurité des algorithmes de consensus. L'évaluation de la sécurité doit notamment inclure le nombre seuil de nœuds de consensus et la fréquence de consensus recommandée.

d) Il est nécessaire que le fournisseur BSP garantisse que les nœuds de consensus sont authentifiés avant de rejoindre le consensus.

e) Il est nécessaire que le fournisseur BSP surveille le processus de consensus et évalue la période de consensus, le nœud de consensus et le résultat du consensus.

f) Il est recommandé que le fournisseur BSP envoie des alertes et propose des solutions lorsqu'une anomalie est détectée dans le processus de consensus surveillé.

8.8 Sécurité des contrats intelligents

Il est recommandé que le fournisseur BSP assure de bout en bout la gestion du cycle de vie des contrats intelligents – création, déploiement, mise à niveau, déclenchement, exécution et suppression.

a) Il est nécessaire que le fournisseur BSP fournisse les spécifications de code, les exigences de logique et d'autres directives normatives pour les contrats intelligents.

b) Il est recommandé que le fournisseur BSP assure un environnement sécurisé et fiable, de type "bac à sable", pour l'exécution des contrats intelligents.

c) Il est nécessaire que le fournisseur BSP assure la gestion des accès de manière appropriée pour les contrats intelligents en vue de limiter les opérations malveillantes ou d'éviter que de contrats intelligents erronés infectent d'autres contrats.

d) Il est nécessaire que le fournisseur BSP prenne en charge les mécanismes de sécurité et d'intervention d'urgence pour les contrats intelligents.

e) Il est nécessaire que le fournisseur BSP limite la complexité des contrats intelligents en termes de consommation de ressources et de durée d'exécution.

f) Il est recommandé que le fournisseur BSP surveille et contrôle la consommation excessive de ressources de la chaîne de blocs par les contrats intelligents.

g) Il est recommandé que le fournisseur BSP prenne en charge la résiliation des contrats intelligents lorsque ceux-ci dépassent la limite fixée en termes de consommation de ressources.

h) Il est recommandé que le fournisseur BSP propose des solutions techniques pour prévenir les attaques par déni de service réparti (DDoS) liées au contrat intelligent.

i) Il est recommandé que le fournisseur BSP mette à la disposition du développeur BSD des fonctions permettant de détecter automatiquement les vulnérabilités en matière de sécurité inhérentes au code source et au code d'octet du contrat intelligent.

j) Il est recommandé que le fournisseur BSP s'assure que le développeur BSD surveille les activités relatives aux contrats intelligents afin d'y détecter les comportements anormaux.

8.9 Surveillance des ressources

Il est recommandé que le fournisseur BSP surveille la consommation de ressources dans la chaîne de blocs en tant que service et envoie une alerte lorsque l'état des ressources est anormal.

a) Il est recommandé que le client BSC permette au fournisseur BSP de surveiller la consommation de ressources des nœuds dans les réseaux de chaînes de blocs personnalisées sur les points suivants: stockage, calcul, unité centrale de traitement, connexions du réseau, état en ligne, durée en ligne, etc.

b) Il est recommandé que le fournisseur BSP envoie au client BSC une alerte signalant une pénurie de ressources lorsque les nœuds du réseau de chaînes de blocs personnalisées sont confrontés à une pénurie de ressources. Le fournisseur BSP doit fournir des solutions au client BSC pour remédier à la pénurie de ressources.

c) Il est recommandé que le client BSC permette au fournisseur BSP de surveiller l'état du réseau concernant les réseaux de chaînes de blocs personnalisées, et notamment la fréquence de génération de blocs, les générateurs de blocs et la taille des blocs.

d) Il est recommandé que le BSP envoie au client BSC une alerte d'intrusion lorsqu'une anomalie est détectée dans l'état du réseau surveillé. Le fournisseur BSP doit fournir au client BSC l'analyse des anomalies correspondante, les informations relatives au nœud anormal et les solutions recommandées.

8.10 Système de détection des intrusions

Il est recommandé que le fournisseur BSP fournisse des mécanismes pour prévenir les codes malveillants et d'autres intrusions, et en assure la mise à jour.

a) Il est nécessaire que le fournisseur BSP communique les règles de sécurité des contrats intelligents ainsi qu'un inventaire des vulnérabilités. Le fournisseur BSP doit prévoir des interfaces d'accès sous une forme courante pour la détection des vulnérabilités.

b) Il est nécessaire que le fournisseur BSP installe un logiciel de protection contre les logiciels malveillants ou configure un logiciel doté de fonctions permettant de détecter et de supprimer les logiciels malveillants.

c) Il est recommandé que le fournisseur BSP garantisse la prévention des codes malveillants dans chaque nœud de la chaîne de blocs et élimine tout code malveillant avant que celui-ci n'accède au réseau de chaînes de blocs.

d) Il est recommandé que le fournisseur BSP prévoie des règles concernant les mécanismes de prévention des codes malveillants, y compris la mise à jour périodique de l'inventaire des codes malveillants, ainsi que la vérification et la suppression régulière des codes malveillants.

e) Il est recommandé que le fournisseur BSP s'assure que le développeur BSD évalue à intervalles réguliers l'efficacité des mesures techniques visant à lutter contre les attaques par code malveillant.

8.11 Audit de sécurité

Il est recommandé que le fournisseur BSP charge un ou plusieurs développeurs BSD d'effectuer un audit de sécurité de l'infrastructure de la chaîne de blocs, du code source et d'autres fonctions de base.

a) Il est recommandé que le fournisseur BSP choisisse un ou plusieurs développeurs BSD pour effectuer une évaluation et un audit de la sécurité du logiciel de base de la chaîne de blocs, du réseau et d'autres environnements d'exploitation situés avant le service de chaîne de blocs en ligne, afin de garantir que les risques de sécurité au niveau de l'infrastructure soient contrôlables.

b) Il est recommandé que le fournisseur BSP charge au moins un développeur BSD d'effectuer un audit de sécurité du code source, axé principalement sur les risques et les problèmes de qualité au niveau du code source.

c) Il est recommandé que le développeur BSD transmette au fournisseur BSP le rapport d'audit du code source contenant les points de conformité/non-conformité ainsi qu'une liste des suggestions de révision pour le code source concerné.

d) Il est recommandé que le fournisseur BSP charge un développeur BSD d'évaluer les fonctions IAM afin de garantir qu'il n'y a pas de risques de fuite de clé privée ni de fuite d'informations des utilisateurs.

8.12 Gestion des fonctions assurées par des tiers

Il est recommandé que le fournisseur BSP garantisse un fonctionnement sécurisé des fonctions assurées par des tiers selon des conditions prédéfinies.

a) Il est nécessaire que le fournisseur BSP précise les spécifications fonctionnelles et les exigences de sécurité des fournisseurs tiers.

b) Il est nécessaire que le fournisseur BSP signe des accords de coopération relatifs aux composantes de service avec les fournisseurs de services tiers et précise les obligations et les responsabilités de ces derniers.

c) Il est recommandé que le fournisseur BSP contrôle ou audite les services assurés par des tiers et évalue si ses services sont conformes aux accords signés.

8.13 Sécurité de la chaîne d'approvisionnement

Il est recommandé que le fournisseur BSP apporte la garantie que sa chaîne d'approvisionnement résiste aux changements de fournisseurs et aux fournisseurs malveillants.

a) Il est nécessaire que le fournisseur BSP élabore des politiques et des procédures de gestion de la sécurité de la chaîne d'approvisionnement, y compris les critères de gestion de la sécurité des participants à la chaîne d'approvisionnement;

b) Il est nécessaire que le fournisseur BSP évalue de manière systématique la vulnérabilité de sa chaîne d'approvisionnement dans l'infrastructure, ainsi que l'utilisation du code source ouvert dans le système.

c) Il est recommandé que le fournisseur BSP informe le client BSC des risques liés à la chaîne d'approvisionnement dans le système de chaîne de blocs en tant que service.

d) Il est nécessaire que le fournisseur BSP confirme à ses divers fournisseurs les logiciels et les matériels qui lui sont indispensables.

Tableau 1 – Exigences de sécurité de la chaîne de blocs en tant que service (BaaS)

Menace de sécurité		Exigences de sécurité												
		Configuration de sécurité	IAM	Gestion des clés	Protection de la vie privée	Sécurité des moteurs cryptogra-phiques	Sécurité des connexions entre homologues (P2P)	Sécurité du mécanisme de consensus	Sécurité des contrats intelligents	Surveillance des ressources	Système de détection des intrusion	Audit de sécurité	Gestion des fonctions assurées par des tiers	Sécurité de la chaîne d'approvi-sionnement
BSP	7.1.1	✓	✓	✓	✓				✓			✓	✓	✓
	7.1.2					✓	✓	✓	✓		✓	✓	✓	✓
	7.1.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7.1.4							✓	✓	✓	✓			
	7.1.5										✓	✓	✓	✓
	7.1.6		✓	✓										
	7.1.7		✓										✓	
	7.1.8											✓	✓	✓
	7.1.9												✓	
BSD	7.2.1			✓	✓	✓	✓	✓		✓	✓		✓	
BSC	7.3.1		✓	✓										
	7.3.2	✓								✓			✓	

Bibliographie

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

[b-UIT-T Y.3500] Recommandation UIT-T Y.3500 (2014) | ISO/CEI 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-UIT-T Y.3530] Recommandation UIT-T Y.3530 (2020), *Informatique en nuage – Exigences fonctionnelles pour la chaîne de blocs en tant que service*.

[b-ISO 22739] ISO 22739:2020, *Technologies de chaîne de blocs et de registre distribué – Vocabulaire*.
<https://www.iso.org/standard/73771.html>

[b-ISO/IEC 27000] ISO/IEC 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>

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

Published in Switzerland
Geneva, 2023