التوصية

ITU-T X.1411 (03/2023)

السلسلة X شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

مبادئ توجيهية بشأن أمن سلسلة الكتل كخدمة (BaaS)

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
القياس الحيوي عن بُعد	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب (1)	X.1149–X.1140
بروتوكولات الأمن (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1350
أمن أنظمة النقل الذكية (ITS)	X.1399–X.1370
أمن سجل الحسابات الموزع	**X.1429–X.1400**
أمن التطبيقات (2)	X.1459–X.1450
أمن شبكة الويب (2)	X.1489–X.1470
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
الدفاع السيبراني	X.1599–X.1590
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولِّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789–X.1770
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1819–X.1800

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1411

مبادئ توجيهية بشأن أمن سلسلة الكتل كخدمة (BaaS)

ملخص

توفر التوصية ITU-T X.1411 مبادئ توجيهية أمنية عامة لسلسلة الكتل كخدمة (BaaS). ويتم أولاً تحليل التهديدات والثغرات الأمنية في سلسلة الكتل كخدمة ثم تُقدّم التدابير الأمنية لسلسلة الكتل كخدمة. وتتناول التوصية أيضاً المتطلبات الأمنية وتوفر مبادئ توجيهية فيما يتعلق بجميع أنشطة إنشاء سلسلة الكتل كخدمة وتشغيلها واستخدامها.

أصبحت سلسلة الكتل كخدمة (BaaS) سائدة في تطوير سلسلة الكتل نظراً لقدراتها الواعدة والدعم المكثف الذي تتلقاه من الصناعة، وخاصة من كبار موردي الخدمات السحابية. وسلسلة الكتل كخدمة توفر الخدمة والموارد الأساسية لتطبيقات سلسلة الكتل، ومع ذلك، فإنها تواجه تحديات أمنية ناشئة عن كل من تكنولوجيات سلسلة الكتل الأساسية والمنصات السحابية. وبالتالي فإن وضع مبادئ توجيهية بشأن أمن سلسلة الكتل كخدمة يكتسي أهمية كبيرة ويمثل ضرورة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1411	2023-03-03	17	11.1002/1000/15110

مصطلحات أساسية

سلسلة الكتل كخدمة، بيئة الحوسبة السحابية، بروتوكولات الموافقة، العقود الذكية، الأمن

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1411

مبادئ توجيهية بشأن أمن سلسلة الكتل كخدمة (BaaS)

1 مجال التطبيق

تحدد هذه التوصية المبادئ التوجيهية بشأن أمن سلسلة الكتل كخدمة (BaaS). كما تعرض وصفاً للتعاريف الخاصة بسلسلة الكتل كخدمة، وهيكلها والتهديدات الأمنية التي تتعرض لها ومواطن ضعفها والتدابير الخاصة بها. ويقع خارج نطاق هذه التوصية أمن تطبيقات سلسلة الكتل كخدمة التي تقوم على سلسلة الكتل كخدمة.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع للمراجَعة، يُشجع جميع مستعملي هذه التوصية على بحث إمكانية تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1401] التوصية ITU-T X.1401 (2019)، *التهديدات الأمنية التي قد تتعرض لها تكنولوجيا السجلات الموزعة*.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015)، *إطار الأمن للحوسبة السحابية*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 سلسلة الكتل كخدمة (BaaS) [b-ITU-T Y.3530]: فئة خدمة سحابية تكون فيها القدرات المقدمة لعملاء الخدمة السحابية هي القدرة على إعداد منصات لسلسلة الكتل وتطوير تطبيقات لامركزية باستخدام تكنولوجيات سلسلة الكتل.

2.1.3 عميل الخدمة السحابية (cloud service customer) [b-ITU-T Y.3500]: طرف يكون مرتبطاً بعلاقة تجارية لأغراض استخدام الخدمات السحابية.

3.1.3 مقدم الخدمة السحابية (cloud service provider) [b-ITU-T Y.3500]: طرف يوفر الخدمات السحابية.

4.1.3 شريك في الخدمة السحابية (cloud service partner) [b-ITU-T Y.3500]: طرف يشارك في دعم أنشطة مقدم الخدمة السحابية أو عميل الخدمة السحابية أو كليهما، أو يساعد في القيام بتلك الأنشطة.

5.1.3 الموافقة (consensus) [b-ITU-T X.1400]: اتفاق على صلاحية مجموعة من المعاملات.

6.1.3 ما بين النظراء (peer-to-peer) [b-ISO 22739]: يتعلق بشبكة أو استخدامها، أو شبكة من النظراء الذين يتبادلون المعلومات والموارد مباشرة فيما بينهم دون الاعتماد على كيان مركزي.

7.1.3 إثبات العمل (proof of work) [b-ITU-T X.1400]: عملية موافقة لحل مشكلة صعبة (مكلفة ومستنزفة للوقت) تسفر عن نتيجة يسهل على الآخرين التحقق منها.

8.1.3 العقد الذكي (smart contract) [b-ITU-T X.1400]: برنامج مكتوب على نظام سجل الحسابات الموزَّع يشفر القواعد الخاصة بأنواع معينة من معاملات نظام سجل الحسابات الموزَّع بطريقة يمكن التحقق من صحتها، ويستدعى تشغيلها بشروط محددة.

9.1.3 التهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب قد يُلحق ضرراً بنظام أو منظمة.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الهجوم بأغلبية 51% (51% attack): هجوم يتحكم فيه المهاجمون بما يكفي من عُقد سلسلة الكتل أو موارد حاسوبية كافية لإلغاء أو إعادة كتابة سجل نظام السجلات الموزّعة من خلال التحكم في إنشاء الكتل.

2.2.3 تقسيم الشبكة (network partition): سيناريو اتصال الشبكة حيث تنقسم الشبكة إلى أكثر من جزء غير متصل.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

API السطح البيني لبرمجة التطبيقات (*Application Programming Interface*)

BaaS سلسلة الكتل كخدمة (*Blockchain as a Service*)

BSC عميل سلسلة الكتل كخدمة (*Blockchain as a Service Customer*)

BSD مطور سلسلة الكتل كخدمة (*Blockchain as a Service Developer*)

BSP مورد سلسلة الكتل كخدمة (*Blockchain as a Service Provider*)

BSS مطور أمن سلسلة الكتل كخدمة (*Blockchain as a Service Security developer*)

CPU وحدة المعالجة المركزية (*Central Processing Unit*)

CSC عميل الخدمة السحابية (*Cloud Service Customer*)

CSN شريك الخدمة السحابية (*Cloud Service partner*)

CSP مورد الخدمة السحابية (*Cloud Service Provider*)

DDoS رفض الخدمة الموزّع (*Distributed Denial-of-Service*)

GPU وحدة معالجة الرسوم البيانية (*Graphic Processing Unit*)

IAM إدارة الهوية والنفاذ (*Identity and Access Management*)

P2P ما بين النظراء (*Peer-to-Peer*)

PII المعلومات المحدِّدة لهوّية أشخاص (*Personally Identifiable Information*)

PoW إثبات العمل (*Proof of Work*)

SDK مجموعة أدوات تطوير البرمجيات (*Software Development Kit*)

5 اصطلاحات

في هذه التوصية، تشير كلمة "**يُتطلب/يتعيَّن/يلزم/يجب**" إلى متطلَّب يجب التقيد به على نحو صارم ولا يجوز أي حيدان عنه إذا أريد إعلان المطابقة مع مقتضيات هذه التوصية.

وتشير كلمة "**يُوصَى**" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً. وبالتالي لا يستلزم إعلانُ المطابقة تحقُّقَ هذا المتطلَّب.

وتشير عبارة "**يتاح خيار/يكون من المتاح خيار**"، إلى متطلَّب اختياري جائز، ولا تنطوي على أي إيحاء بالتوصية به. ولا يُرمى من هذه العبارة إلى الإيحاء بأن قيام الجهة البائعة بالتنفيذ يجب أن يشتمل على توفير الوظيفة المعنية بمثابة خيار بحيث يتاح لمشغِّل الشبكة/موفِّر الخدمة إعمالها اختيارياً. بل إنها تعني أنه يجوز للجهة البائعة أن تختار توفير هذه الوظيفة أو عدم توفيرها دون أن يؤثر ذلك على إعلانها مطابقة المواصفة المعنية.

وفي متن هذه التوصية وملحقاتها، تظهر في بعض الأحيان كلمات يتعين، ويتعين ألا، وينبغي، ويجوز. وفي هذه الحالة يكون تأويلها، على التوالي، على "**يجب**" و"**يلزم**"، و"**مطلوب**" و"**يجب ألا**" و"**يلزم ألا**" و"**ينبغي**" و"**يجوز**". ويُفسر انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها إعلامية.

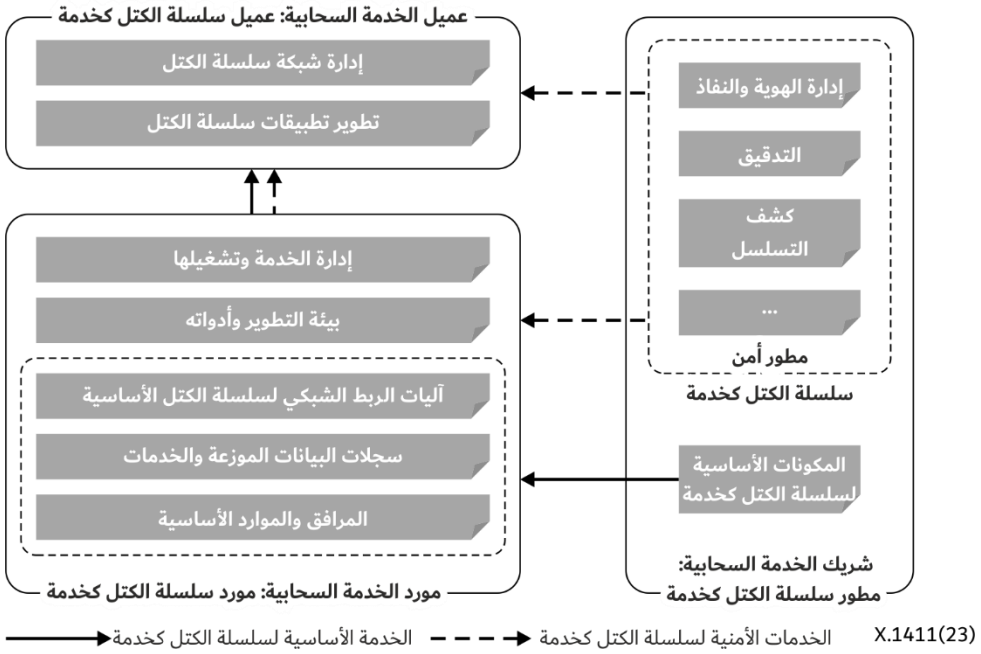
6 نظرة عامة عن أمن سلسلة الكتل كخدمة

توفر سلسلة الكتل كخدمة *بيئة تطوير متكاملة لكل من مطوري وعملاء سلسلة الكتل لإنشاء التطبيقات ذات الصلة بسلسلة الكتل وتطويرها واختبارها واستضافتها ونشرها وتشغيلها*. لذلك، يمكن لعملاء سلسلة الكتل كخدمة استخدام مكونات سلسلة الكتل الأساسية لمنصة سلسلة الكتل كخدمة من أجل الاستخدام الفعّال لشبكات وتطبيقات سلسلة الكتل ونشرها بسهولة.

وبما أن المنصة الأساسية والخدمة الأساسية لسلسلة الكتل كخدمة مبنيتان على الخدمة السحابية، فهناك ثلاثة أدوار رئيسية تشارك في عمل سلسلة الكتل كخدمة، بالتقابل مع الأدوار في الخدمة السحابية.

- **مورد سلسلة الكتل كخدمة (BSP)**: بالتقابل مع مورد الخدمة السحابية (CSP) في بيئة الحوسبة السحابية، يضم مورد سلسلة الكتل كخدمة البنية التحتية لسلسلة الكتل كخدمة وموردي المنصات الذين يقدمون سلسلة الكتل كخدمة. ويبسط مورد سلسلة الكتل كخدمة من تطوير واستخدام سلسلة الكتل وتطبيقاتها بفضل الموارد والوظائف الأساسية ذات الصلة بسلسلة الكتل من حيث التخزين والاتصال والحوسبة ودعم الشبكات. ومورد سلسلة الكتل كخدمة هو المسؤول عن أمن موارد سلسلة الكتل الأساسية وأدوات التطوير المقدمة إلى الأدوار الأخرى لسلسلة الكتل كخدمة.
- **مطور سلسلة الكتل كخدمة (BSD)**: بالتقابل مع شريك الخدمة السحابية (CSN) في بيئة الحوسبة السحابية، يشارك مطور سلسلة الكتل كخدمة في تطوير وتشغيل مكونات سلسلة الكتل كخدمة الأساسية لمساعدة مورد سلسلة الكتل كخدمة في تقديم خدمة سلسلة الكتل. ومطور سلسلة الكتل كخدمة هو المسؤول عن أمن المكونات الأساسية المطورة.
  - **مطور أمن سلسلة الكتل كخدمة (BSS)** هو نوع محدد من مطور سلسلة الكتل كخدمة (BSD). ويساعد مطور أمن سلسلة الكتل كخدمة مورد سلسلة الكتل كخدمة في تعزيز أمن سلسلة الكتل كخدمة (BaaS)، باعتباره طرفاً ثالثاً من موردي الخدمات الأمنية. وتشمل الخدمات الأمنية التي يقدمها مطور أمن سلسلة الكتل كخدمة إدارة الهوية والنفاذ (IAM) والتدقيق وكشف التسلل وغير ذلك.
- **عميل سلسلة الكتل كخدمة (BSC)**: بالتقابل مع عميل الخدمة السحابية (CSC) في بيئة الحوسبة السحابية، يشمل عميل سلسلة الكتل كخدمة عملاء سلسلة الكتل الذين يطلبون خدمات أو موارد لسلسلة الكتل وينفذون إليها ويستخدمونها عبر الوظائف التي يوفرها مورد سلسلة الكتل كخدمة (BSP) مباشرة، أو عبر التطبيقات والخدمات التي يقدمها مطور سلسلة الكتل كخدمة (BSD) بشكل غير مباشر. وعميل سلسلة الكتل كخدمة هو المسؤول عن اتباع القواعد الأمنية التي يوفرها مورد سلسلة الكتل كخدمة عند تشغيل شبكة وتطبيقات سلسلة الكتل الخاصة به. ويُشجع عميل سلسلة الكتل كخدمة على التعاون مع مورد سلسلة الكتل كخدمة في مراقبة أمن شبكات سلسلة الكتل المخصصة والإبلاغ عن الأحداث الأمنية إذا لزم الأمر.

وتُعرض التفاعلات بين هذه الأدوار في الشكل 1.



الشكل 1 – الوظائف والتفاعلات بين الأدوار في سلسلة الكتل كخدمة

1.6 نظرة عامة عن أمن مورد سلسلة الكتل كخدمة

يوفر مورد سلسلة الكتل كخدمة (BSP) وظائف سلسلة الكتل الأساسية بما في ذلك العقود الذكية، وبروتوكولات الموافقة والتوصيلات بين النظراء (P2P)، وخوارزميات التجفير، وسجلات المعاملات، وإدارة السجلات، وإدارة العُقد والموارد، بالإضافة إلى دعم سطوح التطوير البينية الموحدة والخدمات الأمنية. وفيما يلي وظائف مورد سلسلة الكتل كخدمة (BSP) والتحديات الأمنية ذات الصلة بها.

1.1.6 المرافق والموارد الأساسية

يوفر مورد سلسلة الكتل كخدمة (BSP) المرافق الأساسية لتوفير موارد الحوسبة والاتصالات الأساسية، والموارد الأخرى لدعم تطوير الربط الشبكي لسلسلة الكتل وتطبيقاتها. ويمكن أن تكون تلك المرافق أجهزة مادية أو أجهزة افتراضية مثل الآلات والحاويات الافتراضية.

وتواجه المرافق الأساسية تحديات من قبيل المخاطر البيئية للمرافق المادية، وهجمات الأبواب الخلفية، والموارد المشتركة بين الشاغلين، وما إلى ذلك.

2.1.6 سجلات البيانات وخدماتها

يوفر مورد سلسلة الكتل كخدمة (BSP) خدمات البيانات داخل السلسلة وخارجها، مثل تخزين بيانات العملاء والنظام وإدارتها والاستعلام عنها من أجل عميل سلسلة الكتل كخدمة (BSC). وفي هذه الحالة، يضمن سجل البيانات داخل السلسلة مقاومة العبث بينما تدعم قاعدة البيانات خارج السلسلة خدمات البيانات التي تتسم بالكفاءة.

وفيما يتعلق بأمن البيانات، يواجه مورد سلسلة الكتل كخدمة (BSP) التحديات الأمنية التالية:

- خدمات البيانات غير المتاحة، بما في ذلك التخزين غير المتسق للبيانات داخل السلسلة وخارج السلسلة الناتج عن أقسام الشبكة، وفقدان البيانات الناجم عن فشل قاعدة البيانات ومرافق التخزين، والمراجعات غير المصرح بها لسجل البيانات، وما إلى ذلك.

– انتهاك الخصوصية، بما في ذلك النفاذ غير المصرح به إلى بيانات الأفراد، واشتقاق المعلومات الحساسة من البيانات، والتدمير غير الناجح للبيانات الخاصة، وما إلى ذلك.

3.1.6 آليات الربط الشبكي الأساسية لسلسلة الكتل

يوفر مورد سلسلة الكتل كخدمة (BSP) مجموعة من الخيارات في آليات الربط الشبكي الأساسية لسلسلة الكتل لتبسيط إعداد شبكات سلسلة الكتل المخصصة. وتتكون آليات الربط الشبكي الأساسية لسلسلة الكتل من بروتوكولات الموافقة وبروتوكولات التوصيل بين النظراء وخوارزميات التجفير. ويمكن لعميل سلسلة الكتل كخدمة (BSC) اختيار مجموعة محددة من مكونات الربط الشبكي من جميع الخيارات وتعيين المعلمات المقابلة لإعداد شبكة سلسلة كتل مخصصة على نحو سريع.

ومورد سلسلة الكتل كخدمة (BSP) هو المسؤول عن معالجة التحديات الأمنية لآليات الربط الشبكي الأساسية لسلسلة الكتل. وتؤثر هذه التحديات على أمن شبكات سلسلة الكتل المخصصة وحتى تطبيقات سلسلة الكتل المدمجة في منصة سلسلة الكتل كخدمة (BaaS)، حيث يستخدم عميل سلسلة الكتل كخدمة (BSC) بشكل مباشر آليات الربط الشبكي الأساسية لسلسلة الكتل لتطوير شبكات سلسلة الكتل وتطبيقاتها. وهنا، تشمل التحديات الأمنية النفاذ غير المصرح به إلى موارد سلسلة الكتل وأقسام الشبكة والعُقد الضارة وما إلى ذلك. وعلى سبيل المثال، قد تؤدي أقسام الشبكة الناتجة عن خدمات سلسلة الكتل غير المتاحة إلى تأخير غير مقبول في التوصل إلى توافق داخل شبكة سلسلة الكتل الموزعة.

4.1.6 بيئة التطوير وأدواته

يقوم مورد سلسلة الكتل كخدمة (BSP) بتهيئة بيئة تطوير متكاملة مزودة بسطح بيني لبرمجة التطبيقات (API) ومجموعة أدوات للتطوير وأدوات التطوير الأخرى لتبسيط تطوير تطبيقات سلسلة الكتل. ونظراً لأن العقد الذكي هو آلية بديهية في تطوير تطبيقات سلسلة الكتل، فإن مورد سلسلة الكتل كخدمة يبسط أيضاً نشر العقود الذكية ويوفر مجموعة من العقود الذكية للوظائف المشتركة، مثل إدارة الهوية والنفاذ.

وتشمل التحديات ذات الصلة التحكم في النفاذ غير المناسب للسطح البيني لبرمجة التطبيقات، والسطوح البينية غير المتوافقة، والتشغيل غير المتوقع للعقود الذكية، وما إلى ذلك.

5.1.6 إدارة الخدمة والتشغيل

مورد سلسلة الكتل كخدمة (BSP) هو المسؤول عن مراقبة حالة خدمة سلسلة الكتل والتنبيه بشأنها، من حيث المرافق المادية وعُقد سلسلة الكتل وتوصيلات الشبكة والموارد المخصصة، بالإضافة إلى إدارة الهوية والنفاذ ووظائف إدارة الأمن الأخرى. كما يدعم مورد سلسلة الكتل كخدمة (BSP) ويدير الوظائف المتعلقة بسلسلة الكتل التي يوفرها مطور سلسلة الكتل كخدمة (BSD).

وتشمل التحديات الأمنية ذات الصلة وظائف الإدارة غير المتاحة، وإدارة النفاذ غير المناسب، والنفاذ غير المصرح به للإدارة، والكمية الهائلة للموارد المستهلكة، والمخاطر في المكونات المتعلقة بسلسلة الكتل المقدمة من مطور سلسلة الكتل كخدمة (BSD).

2.6 نظرة عامة عن أمن مطور سلسلة الكتل كخدمة

يقوم مطور سلسلة الكتل كخدمة (BSD) بتطوير المكونات الأساسية لسلسلة الكتل كخدمة (BaaS) من أجل مورد سلسلة الكتل كخدمة (BSP)، أو يقوم بتوفير خدمات أمنية لجميع الأدوار.

1.2.6 تطوير المكونات الأساسية لسلسلة الكتل كخدمة

يوفر مطور سلسلة الكتل كخدمة (BSD)، باعتباره مورد طرف ثالث، المكونات الأساسية لسلسلة الكتل كخدمة (BaaS) مثل العقود الذكية وخوارزميات التجفير وبروتوكولات الموافقة وخوارزميات التشفير.

وتشمل التحديات والتهديدات الأمنية ذات الصلة السطوح البينية غير المتوافقة، وتصميمات البروتوكولات غير الآمنة، والنفاذ عبر الأبواب الخلفية في تنفيذ البروتوكولات، وغيرها.

2.2.6 الخدمات الأمنية

يعمل مطور أمن سلسلة الكتل كخدمة (BSS) كمورد خدمات أمن تابع لجهة خارجية لجميع الأدوار في النظام الإيكولوجي لسلسلة الكتل كخدمة. فعلى سبيل المثال، يمكن أن يوفر مطور أمن سلسلة الكتل كخدمة وظائف كشف التسلل لمورد سلسلة الكتل كخدمة (BSP)، وتدقيق الشفرات لمطوري سلسلة الكتل كخدمة (BSD)، وإدارة الهوية والنفاذ (IAM) لعميل سلسلة الكتل كخدمة (BSC).

وتشمل التحديات الأمنية قواعد الأمن المتقادمة والعمليات غير السليمة لموظفي مطور أمن سلسلة الكتل كخدمة (BSS) وغيرها.

3.6 نظرة عامة عن أمن عميل سلسلة الكتل كخدمة

يستخدم عميل سلسلة الكتل كخدمة (BSC) الخدمات التي يقدمها مورد سلسلة الكتل كخدمة (BSP) ومطور سلسلة الكتل كخدمة (BSD) لبناء شبكة مخصصة لسلسلة الكتل وتطبيقات سلسلة الكتل. وهناك نوعان من عملاء سلسلة الكتل كخدمة (BSC): أحدهما هو المسؤول الذي يبني ويدير شبكات سلسلة الكتل المخصصة، والآخر هو العضو الذي ينضم إلى شبكة سلسلة الكتل المخصصة. وبالنسبة إلى عميل محدد لسلسلة الكتل كخدمة (BSC)، يمكن أن يكون المسؤول في إحدى شبكات سلسلة الكتل المخصصة والعضو في إحدى شبكات سلسلة الكتل المخصصة الأخرى.

ويواجه جميع أنواع عملاء سلسلة الكتل كخدمة (BSC) تحديات أمنية في إدارة المفاتيح واستخدامها. ويواجه المسؤول أيضاً تحديات أمنية في إعداد وإدارة شبكات سلسلة الكتل المخصصة، مثل الإعداد غير المناسب لعقد سلسلة الكتل والتوصيلات والموارد الأخرى.

7 التهديدات الأمنية التي تعترض سلسلة الكتل كخدمة

يمكن تصنيف التهديدات التي تعترض مورد سلسلة الكتل كخدمة (BSP) ومطور سلسلة الكتل كخدمة (BSD) وعميل سلسلة الكتل كخدمة (BSC) إلى ثلاثة أنواع:

- التصميمات التقنية غير الآمنة، وتدفقات التنفيذ، والإدارة غير السليمة للموارد الأساسية، والوظائف الأساسية لسلسلة الكتل وأنظمة خدمة سلسلة الكتل.
- التفاعلات غير الآمنة بين مورد ومطور وعميل سلسلة الكتل كخدمة، بما في ذلك السطوح البينية غير المتوافقة وسلسلة التوريد غير الآمنة.
- عمليات الموظفين غير السليمة، بما في ذلك الاستخدام غير المناسب لكلمات السر وتخزينها.

وتعرض التهديدات الأمنية لكل دور في الفقرات من 1.7 إلى 3.7.

1.7 التهديدات الأمنية التي تعترض مورد سلسلة الكتل كخدمة

1.1.7 التهديدات التي تعترض الخدمة السحابية

نظراً لأن مورد سلسلة الكتل كخدمة (BSP) يوفر موارد سلسلة الكتل الأساسية استناداً إلى الخدمات السحابية، فإنه يواجه تحديات وتهديدات موروثة من الخدمة السحابية، كما هو موضح في الفقرتين 7 و8 من التوصية [ITU-T X.1601]. فعلى سبيل المثال، قد يؤدي النفاذ غير المصرح به إلى قسم من مورد شاغل آخر في البيئة المشتركة للخدمات السحابية إلى تفرع سلسلة الكتل لنظام سلسلة الكتل الخاص بهذا الشاغل عن طريق إعادة كتابة أو مراجعة سجلات البيانات الخاصة به.

2.1.7 التهديدات التي تعترض الآليات الأساسية للربط الشبكي لسلسلة الكتل

يمكن أن تحدث التهديدات لبروتوكولات الموافقة وبروتوكولات التوصيل بين النظراء ومحركات التشفير بسبب ثغرات في تصميمات البروتوكولات والعيوب في تنفيذ الآليات والإدارة غير المناسبة. ولمزيد من التفاصيل، انظر الفقرة 6 في التوصية [ITU-T X.1401].

3.1.7 خدمة غير موثوقة للبيانات

تشمل التهديدات التي يتعرض لها سجل البيانات الموزع عدم وجود موارد كافية لسلسلة الكتل، ووجود عيوب في نظام التخزين وإدارة تخزين غير آمنة، مما قد يؤدي إلى عدم تناسق سجل البيانات، وفقدان البيانات، والتلاعب بالبيانات، وتسرب البيانات. فعلى سبيل المثال، تتوسع بيانات النظام وسلسلة الكتل لشبكة سلسلة الكتل المخصصة عندما تعمل شبكة سلسلة الكتل. وفي حالة عدم توفير مورد سلسلة الكتل كخدمة (BSP) لموارد تخزين كافية لشبكة سلسلة الكتل المخصصة لتلبية توسع البيانات، فإن شبكة سلسلة الكتل المخصصة ستستبدل البيانات القديمة بالبيانات الجديدة أو ستسقط البيانات الجديدة مباشرة، مما يؤدي إلى فقدان البيانات في شبكة سلسلة الكتل المخصصة. ومثال آخر هو المكان الذي يمكن أن يؤدي فيه الفشل في مرافق الاتصالات أو التخزين إلى تخزين غير متسق للبيانات في سجلات البيانات الموزعة. وإذا استمرت حالات الفشل لفترة طويلة، فإن أقسام الشبكة الناتجة تتسبب في حدوث تأخيرات غير متوقعة في إنشاء الكتل والاستعلام عن البيانات وخدمات البيانات الأخرى.

4.1.7 التهديدات على بيئة التطوير

تعترض بيئة التطوير المتكاملة، وبيئة التجميع، والعقود الذكية، والسطوح البينية لبرمجة التطبيقات، ومجموعة أدوات تطوير البرمجيات (SDK)، وغيرها من وظائف تطوير إمكانية النفاذ التي يوفرها مورد سلسلة الكتل كخدمة (BSP)، تهديدات في عملية تصميم وظائف التطوير تلك وتنفيذها وتشكيلها وتشغيلها. فعلى سبيل المثال، قد تؤدي عيوب استيقان السطوح البينية لبرمجة التطبيقات إلى النفاذ غير المصرح به واستخدام مورد سلسلة الكتل الأساسي. وإلى جانب ذلك، تواجه العقود الذكية ثغرات أمنية في التصميم المنطقي، وتنفيذ العقود وإدارة الشفرات، مثل الزيادة والنقصان للأعداد الصحيحة في العقود الذكية، مما يؤدي إلى نتائج غير متوقعة عند التشغيل.

5.1.7 وظائف الأطراف الثالثة غير الآمنة

يدعم مورد سلسلة الكتل كخدمة (BSP) وظائف الأطراف الثالثة التي يوفرها مطور سلسلة الكتل كخدمة (BSD) ويقوم بدمجها في منصة سلسلة الكتل كخدمة (BaaS) عبر السطوح البينية لبرمجة التطبيقات. وهنا، قد تؤدي الأخطاء والبرمجيات الضارة في وظائف الأطراف الثالثة، بالإضافة إلى السطوح البينية لبرمجة التطبيقات غير المتوافقة والتحكم غير المناسب في النفاذ إلى هذه السطوح، إلى اضطراب نظام سلسلة الكتل كخدمة (BaaS).

6.1.7 النفاذ غير الآمن إلى النظام

يشمل النفاذ غير الآمن إلى النظام الافتقار إلى التحكم في النفاذ أو التحكم غير المناسب في النفاذ إلى مرافق سلسلة الكتل وسجلات البيانات والشبكة والتطبيقات. ويمكن أن يتسبب ذلك في التلاعب ببيانات سلسلة الكتل، واقتحام شبكات سلسلة الكتل المخصصة، وتسريب المعلومات الخاصة.

7.1.7 التهديدات الداخلية

قد يقوم موظفو مورد سلسلة الكتل كخدمة (BSP) بطريق الخطأ أو عن عمد بسلوكيات ضارة، مثل مشاركة كلمات السر مع أشخاص غير مصرح لهم، وترك كلمات السر في أماكن غير آمنة، وكشف المعلومات الشخصية، وما إلى ذلك. وقد تؤدي التهديدات الداخلية إلى تسرب المعلومات الخاصة، والنفاذ غير المصرح به إلى شبكات سلسلة الكتل المخصصة وعدم تيسر خدمات سلسلة الكتل.

8.1.7 سلسلة التوريد غير الموثوقة

تستخدم منصة خدمة سلسلة الكتل مكونات البرمجيات والأجهزة التي يوفرها العديد من الموردين. وسيؤدي عدم الاستمرار في الإمداد بالبرمجيات والأجهزة إلى تقويض قدرات الحوسبة والتوصيلات والموارد الأخرى لخدمات سلسلة الكتل. وفي هذه الحالة، فإن تيسر خدمات سلسلة الكتل سيكون في خطر. فعلى سبيل المثال، يعتمد إثبات عمل (PoW) بروتوكول الموافقة على التنافس على

قدرات الحوسبة بين عقد سلسلة الكتل عبر الإنترنت، وبالتالي فإن الإمداد المتوقف لقدرات الحوسبة والتوصيلات يمكن أن يؤثر على نتائج الموافقة لشبكات سلسلة الكتل القائمة على إثبات العمل.

وبالإضافة إلى ذلك، يمكن أن تؤدي البرمجيات الضارة والثغرات الأمنية القابلة للاستغلال في البرمجيات والأجهزة، وكذلك في معماريات سلسلة الكتل مفتوحة المصدر، إلى عمليات لتوليد كتل غير متوقعة، ورفض الخدمة، وتسرب البيانات وإساءة استخدامها، وما إلى ذلك.

9.1.7 التهديدات التي تعترض البيئة المادية

قد تتسبب الحرائق والفيضانات والصواعق والكوارث البيئية الأخرى التي تؤثر على المرافق الأساسية، في عدم تيسر المرافق المادية التي توفر الاتصالات والحوسبة والموارد الأساسية الأخرى. فعلى سبيل المثال، يمكن أن يتسبب انقطاع التيار الكهربائي المتعمد أو العرضي إلى عدم توصيل جزء من عُقد سلسلة الكتل. وفي هذه الحالة، تخضع عملية الموافقة لسيطرة عدد أقل من عقد سلسلة الكتل، مما يؤدي إلى نتائج موافقة غير صحيحة وتأخير إضافي في إنشاء الكتل.

2.7 التهديدات الأمنية التي تعترض مطور سلسلة الكتل كخدمة

1.2.7 التهديدات التي تعترض وظائف الأطراف الثالثة

يوفر مطور سلسلة الكتل كخدمة (BSD) مكونات سلسلة الكتل الأساسية، والآليات الأمنية لسلسلة الكتل، ووظائف تطوير تطبيقات سلسلة الكتل، كمورد خدمات خارجي. وتشمل التهديدات ذات الصلة الثغرات الأمنية الكامنة في المكونات الأساسية لسلسلة الكتل، وعيوب تنفيذ وظائف الأطراف الثالثة، والسطوح البينية غير المتوافقة، والتحكم في النفاذ غير الآمن إلى هذه السطوح.

وإلى جانب ذلك، يمكن أن يؤدي السلوك الضار لموظفي مطور سلسلة الكتل كخدمة (BSD) أيضاً إلى تسرب المعلومات الخاصة، والنفاذ من الأبواب الخلفية في وظائف الأطراف الثالثة، والعمليات غير المتوقعة للوظائف الأمنية.

3.7 التهديدات الأمنية التي تعترض عميل سلسلة الكتل كخدمة

1.3.7 حالات تسرب المفاتيح وفقدانها

يدير عميل سلسلة الكتل كخدمة (BSC) المفاتيح بنفسه أو عبر خدمة يقدمها طرف ثالث. وقد يؤدي التخزين غير السليم للمفاتيح، أو تلف ملف المفاتيح، أو خدمات مفاتيح غير موثوقة تقدمها أطراف ثالثة، إلى فقدان المفاتيح أو تسربها، مما يؤدي إلى فقدان أصول عميل سلسلة الكتل كخدمة، والكشف عن المعلومات الخاصة، واضطراب شبكات سلسلة الكتل المخصصة.

2.3.7 الإدارة غير السليمة لشبكات سلسلة الكتل المخصصة

يقوم عميل سلسلة الكتل كخدمة (BSC) بإعداد شبكات سلسلة الكتل المخصصة الخاصة به ونشر آليات الأمن بناءً على وظائف سلسلة الكتل التي يوفرها مورد سلسلة الكتل كخدمة (BSP) ومطور سلسلة الكتل كخدمة (BSD). وبناءً على ذلك، ستمثل التشكيلات غير السليمة لشبكات سلسلة الكتل المخصصة وآليات الأمن تهديداً على شبكات سلسلة الكتل المخصصة. فعلى سبيل المثال، إذا خصص عميل سلسلة الكتل كخدمة (BSC) موارد تخزين غير كافية لعمليات شبكة سلسلة الكتل المخصصة، فقد تفشل شبكة سلسلة الكتل المخصصة في تحديث بيانات سلسلة الكتل، مما يؤدي في نهاية المطاف إلى عدم اتساق سجلات بيانات سلسلة الكتل.

8 المتطلبات الأمنية لسلسلة الكتل كخدمة

1.8 تشكيلة أمن شبكة سلسلة الكتل المخصصة

يوصى بأن يقدم مورد سلسلة الكتل كخدمة (BSP) توصيات بشأن تشكيلات شبكة سلسلة الكتل المخصصة لتلبية المتطلبات الأمنية الخاصة بعميل سلسلة الكتل كخدمة (BSC). وإلى جانب ذلك، يوصى بأن يقدم مورد سلسلة الكتل كخدمة توصيات حول نشر آليات الأمن اللازمة فيما يتعلق بشبكات سلسلة الكتل المخصصة.

أ) يجب أن يحدد مورد سلسلة الكتل كخدمة النطاق الموصى به لإجمالي عدد العقد.

ب) يجب أن يحدد مورد سلسلة الكتل كخدمة الحد الأدنى لعدد العقد عبر الإنترنت لتجنب التهديدات بنسبة 51% والتهديدات الأخرى المعروفة لشبكة سلسلة الكتل.

ج) يجب أن يحدد مورد سلسلة الكتل كخدمة الحد الأدنى لعدد العقد المجاورة لكل عقدة لتجنب تقسيم شبكة سلسلة الكتل.

د) يوصى بأن يحدد مورد سلسلة الكتل كخدمة أنواع العقد الموصى بها، مع تحديد عدد كل نوع وحقوقه.

هـ) يوصى بأن يحدد مورد سلسلة الكتل كخدمة الحد الأدنى من موارد التخزين ووحدة المعالجة المركزية (CPU) ووحدة معالجة الرسوم البيانية (GPU) لكل نوع من أنواع العقد.

و) يوصى بأن يحدد مورد سلسلة الكتل كخدمة بروتوكولات الموافقة الموصى بها وبروتوكولات ما بين النظراء وفقاً لتشكيلات العقد.

ز) يوصى بأن يوفر مورد سلسلة الكتل كخدمة وظائف الأمن الأساسية، بما في ذلك إدارة الهوية والنفاذ وإدارة المفاتيح، لشبكة سلسلة الكتل المخصصة.

ح) يمكن لمورد سلسلة الكتل كخدمة أن يوفر بصورة اختيارية تقييماً أمنياً لتشكيلات شبكة سلسلة الكتل المخصصة. ويتعين أن يقدم مورد سلسلة الكتل كخدمة الاقتراحات والحلول الأمنية ذات الصلة إلى عميل سلسلة الكتل كخدمة (BSC).

2.8 إدارة الهوية والنفاذ

يوصى بأن يوفر مورد سلسلة الكتل كخدمة (BSP) وظائف إدارة الهوية والنفاذ في نظام سلسلة الكتل كخدمة وشبكة سلسلة الكتل المخصصة. وتُنشر وظائف إدارة الهوية والنفاذ ليس لحماية الهويات فحسب، بل لتسهيل إدارة النفاذ والاستيقان والتخويل أيضاً.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة وظائف تسجيل الهوية وإلغاء التسجيل في نظام سلسلة الكتل كخدمة.

ب) يوصى بأن يوفر مورد سلسلة الكتل كخدمة وظائف تسجيل وإلغاء تسجيل الهوية لشبكة سلسلة الكتل المخصصة.

ج) يجب أن يوفر مورد سلسلة الكتل كخدمة إدارة النفاذ إلى الحساب لنظام سلسلة الكتل كخدمة للتمييز بين مورد سلسلة الكتل كخدمة (BSP) وعميل سلسلة الكتل كخدمة (BSC) ومطور سلسلة الكتل كخدمة (BSD).

د) يوصى بأن يوفر مورد سلسلة الكتل كخدمةإدارة النفاذ إلى الحساب في شبكة سلسلة الكتل المخصصة. ويتعين أن يكون لأي شبكة من شبكات سلسلة الكتل المخصصة دور واحد أو أكثر للعملاء مع حقوق نفاذ مختلفة.

هـ) يجب أن يوفر مورد سلسلة الكتل كخدمة استيقان النفاذ إلى نظام سلسلة الكتل كخدمة. ويمكن لكل هوية أن تنفذ إلى الموارد وفقاً لحقوق النفاذ الخاصة بها فقط.

و) يوصى بأن يوفر مورد سلسلة الكتل كخدمة استيقان النفاذ إلى شبكة سلسلة الكتل المخصصة.

ز) يمكن أن يوفر مورد سلسلة الكتل كخدمة بصورة اختيارية وظائف إدارة النفاذ الدقيقة، مثل وظائف التحكم في النفاذ القائم على الأدوار.

ح) يمكن أن يراقب مورد سلسلة الكتل كخدمة بصورة اختيارية وتيرة نشاط النفاذ إلى بروتوكول الإنترنت، والنفاذ إلى الحساب، وأجهزة النفاذ وغيرها. وتشمل أنشطة النفاذ التسجيل وإلغاء التسجيل وتحديث المفاتيح وغير ذلك.

3.8 إدارة المفاتيح

يوصى بأن يوفر مورد سلسلة الكتل كخدمة (BSP) وظائف الإدارة الرئيسية لحماية أمن إنشاء المفاتيح وتخزينها وتوزيعها واستخدامها وإنشاء نسخ احتياطية منها واستردادها وإبطالها.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة مخططات شاملة لإدارة المفاتيح، مع توضيح المعلومات الخاصة بالمفاتيح والإجراءات الإدارية.

ب) يجب أن يقيم مورد سلسلة الكتل كخدمة أمن خوارزميات الأرقام العشوائية والمعلمات الأخرى المستخدمة لإنشاء المفاتيح. ويتعين أن تحقق خوارزميات الأرقام العشوائية مستوى العشوائية المطلوب وعدم القدرة على التنبؤ بها.

ج) يوصى بأن يدعم مورد سلسلة الكتل كخدمة وظائف إدارة المفاتيح للأطراف الثالثة. ويتعين تقييم أمن وظائف إدارة المفاتيح للأطراف الثالثة وضمانه قبل تقديمها إلى عميل سلسلة الكتل كخدمة (BSC).

د) يوصى بأن يوفر مورد سلسلة الكتل كخدمة وظائف الإلغاء الرئيسية للحسابات المشبوهة والتي أُلغي تسجيلها.

هـ) يوصى بأن يوفر مورد سلسلة الكتل كخدمة وظائف استرجاع المفاتيح المفقودة. ويمكن فقط للحسابات المستيقن منها النفاذ إلى وظائف استرجاع المفاتيح.

و) يوصى بأن يلزم مورد سلسلة الكتل كخدمة عميل سلسلة الكتل كخدمة بتحديث المفاتيح بشكل دوري. ويتعين أن تختلف فترة التحديث حسب مستويات الأمن.

ز) يوصى بأن ينشر عميل سلسلة الكتل كخدمة وظيفة إدارة المفاتيح في شبكة سلسلة الكتل المخصصة.

ح) يجب أن يقوم عميل سلسلة الكتل كخدمة بإتقان واتباع الإجراءات الآمنة لاستخدام المفاتيح وتخزينها واستعادتها وإلغاءها، وفقاً لوظيفة إدارة المفاتيح المستخدمة في شبكة سلسلة الكتل المخصصة.

ط) يوصى بأن يقوم عميل سلسلة الكتل كخدمة بالإبلاغ عن الاستخدام المشبوه للمفاتيح لمورد سلسلة الكتل كخدمة على النحو المحدد مسبقاً في وظيفة إدارة المفاتيح.

ي) يمكن أن يستخدم مورد سلسلة الكتل كخدمة اختيارياً نظام تخزين مفاتيح مكون من طرفين أو متعدد الأطراف للمفاتيح الرئيسية والمفاتيح السرية.

4.8 حماية الخصوصية

يوصى بأن يوفر مورد سلسلة الكتل كخدمة الحماية عند جمع المعلومات المحددة لهوية أشخاص (PII) والنفاذ إليها والعمليات الأخرى ذات الصلة بها.

أ) يجب التزام مورد سلسلة الكتل كخدمة باللوائح والسياسات والتشريعات الوطنية والمحلية المتعلقة بحماية الخصوصية مثل جمع المعلومات المحددة لهوية أشخاص (PII) وتخزينها.

ب) يجب أن يتيح مورد سلسلة الكتل كخدمة منع التعرف على المعلومات المحددة لهوية أشخاص المعروضة.

ج) يجب أن ينشر مورد سلسلة الكتل كخدمة تدابير أمنية لضمان إمكانية حذف المعلومات المحددة لهوية أشخاص الموجودة على السلسلة حذفاً تاماً عندما يستوجب قيام عميل سلسلة الكتل كخدمة القيام بذلك، مثل استخدام تكنولوجيا سلسلة الكتل القائمة على خوارزمية الاختزال Chameleon، أو لتخزين المعلومات المحددة لهوية أشخاص خارج السلسلة.

د) يوصى بأن يدعو مورد سلسلة الكتل كخدمة المنظمات المهنية لإجراء عمليات تدقيق على العمليات الحساسة الخاصة بالمعلومات المحددة لهوية أشخاص.

5.8 أمن محركات التشفير

يوصى بأن يضمن مورد سلسلة الكتل كخدمة أمن محركات التشفير التي يتم نشرها في شبكات سلسلة الكتل المخصصة.

أ) يجب أن يدعم مورد سلسلة الكتل كخدمة خوارزميات التشفير السائدة، التي تم التحقق من أمنها بشكل عام.

ب) يجب أن يدعو مورد سلسلة الكتل كخدمة المنظمات المهنية لتدقيق أمن محركات التشفير.

ج) يوصى بأن يدعم مورد سلسلة الكتل كخدمة محركات التشفير التي يوفرها مطور سلسلة الكتل كخدمة (BSD). ويوصى بأن يوفر مطور سلسلة الكتل كخدمة نتائج التقييم الأمني لمحركات التشفير.

6.8 أمن التوصيل فيما بين النظراء

يوصى بأن يضمن مورد سلسلة الكتل كخدمة مقاومة التوصيلات فيما بين النظراء العقد الضارة وغير الموثوقة.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة مخططات الاستيقان لإدارة النفاذ إلى شبكات ما بين النظراء.

ب) يجب أن يستخدم مورد سلسلة الكتل كخدمة تكنولوجيا للتجفير بهدف إنشاء قنوات إرسال آمنة بين العقد الموزعة.

ج) يجب أن يدعم مورد سلسلة الكتل كخدمة بروتوكولات ما بين النظراء على نحو موثوق وقابل للتوسع. وتشير الموثوقية إلى أن العقد غير الموصولة تحافظ على الاتساق مع العقد الأخرى بعد إعادة التوصيل. وتشير قابلية التوسع إلى أن البروتوكولات تدعم إضافة عقد أو إزالتها بشكل ديناميكي أو ثابت مع شبكات سلسلة الكتل التي تعمل بشكل طبيعي.

د) يجب أن يدعم مورد سلسلة الكتل كخدمة بروتوكولات ما بين النظراء في كل عقدة لديها أكثر من عقدة مجاورة.

هـ) يوصى بأن يدعم مورد سلسلة الكتل كخدمة بروتوكولات ما بين النظراء بحيث لا تؤدي أي عقدة غير موصولة إلى تقسيم الشبكة.

و) يوصى بأن يوفر مورد سلسلة الكتل كخدمة طوبولوجيا في الوقت الفعلي لشبكات ما بين النظراء.

ز) يوصى بأن يوفر مورد سلسلة الكتل كخدمة إنذاراً إذا كانت شبكة ما بين النظراء تواجه تقسيماً أو عقداً ضارة.

7.8 أمن آلية الموافقة

يوصى بأن يعمل مورد سلسلة الكتل كخدمة على ضمان أن يكون تصميم آلية الموافقة وعملياتها آمنة.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة خوارزميات موافقة تم إثبات أمنها أو تقييمه علناً.

ب) يجب أن يدعم مورد سلسلة الكتل كخدمة عميل سلسلة الكتل كخدمة في نشر خوارزميات الموافقة التي يوفرها مطور سلسلة الكتل كخدمة (BSD).

ج) يجب أن يوفر مورد سلسلة الكتل كخدمة التقييم الأمني لخوارزميات الموافقة الخاصة بعميل سلسلة الكتل كخدمة. ويجب أن يتضمن التقييم الأمني عتبة لعدد عقد الموافقة ووتيرة الموافقة الموصى بها وغير ذلك.

د) يجب أن يضمن مورد سلسلة الكتل كخدمة استيقان عُقد الموافقة قبل الانضمام إلى الموافقة.

هـ) يجب أن يراقب مورد سلسلة الكتل كخدمة عملية المراقبة وأن يقيّم فترة المراقبة وعقدها ونتائجها.

و) يوصى بأن يوفر مورد سلسلة الكتل كخدمة إنذارات وحلول عندما تُقيّم عملية الموافقة المراقبة على أنها غير طبيعية.

8.8 أمن العقد الذكي

يوصى بأن يوفر مورد سلسلة الكتل كخدمة إدارة شاملة لدورة حياة العقود الذكية، بما في ذلك إنشاء العقود الذكية ونشرها وتحديثها وتشغيلها وتنفيذها وإلغائها.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة مواصفات الشفرات والمتطلبات المنطقية والتوجيهات المعيارية الأخرى بشأن العقود الذكية.

ب) يوصى بأن يوفر مورد سلسلة الكتل كخدمة بيئة معزولة موثوق بها، مثل البيئات التجريبية، من أجل تشغيل العقود الذكية.

ج) يجب أن يوفر مورد سلسلة الكتل كخدمة إدارة نفاذ مناسبة فيما يتعلق بالعقود الذكية لتقييد العمليات الضارة أو منع العقود الذكية الخاطئة من إلحاق الضرر بالعقود الأخرى.

د) يجب أن يدعم مورد سلسلة الكتل كخدمة آليات الاستجابة للطوارئ الأمنية ذات الصلة بالعقود الذكية.

هـ) يجب أن يحد مورد سلسلة الكتل كخدمة من تعقيد العقود الذكية من حيث استهلاك الموارد ووقت التنفيذ.

و) يوصى بأن يراقب مورد سلسلة الكتل كخدمة الاستهلاك المفرط لموارد سلسلة الكتل من قبل العقود الذكية والتحكم فيه.

ز) يوصى بأن يدعم مورد سلسلة الكتل كخدمة إنهاء العقود الذكية عندما تتجاوز القيود التي توضع فيما يتعلق بالموارد.

ح) يوصى بأن يوفر مورد سلسلة الكتل كخدمة الحلول التقنية لمنع هجمات رفض الخدمة الموزع (DDoS) المتعلقة بالعقد الذكي.

ط) يوصى بأن يلزم مورد سلسلة الكتل كخدمة مطور سلسلة الكتل كخدمة بتوفير وظائف للكشف التلقائي عن الثغرات الأمنية في شفرة مصدر العقد الذكي وشفرة البايتات الخاصة بالعقد الذكي.

ي) يوصى بأن يلزم مورد سلسلة الكتل كخدمة مطور سلسلة الكتل كخدمة بمراقبة أنشطة العقود الذكية للكشف المبكر عن السلوكيات غير الطبيعية لهذه العقود.

9.8 مراقبة الموارد

يوصى بأن يراقب مورد سلسلة الكتل كخدمة استهلاك الموارد في سلسلة الكتل كخدمة وتوفير إنذار عندما تكون حالة الموارد غير طبيعية.

أ) يوصى بأن يسمح عميل سلسلة الكتل كخدمة لمورد سلسلة الكتل كخدمة بمراقبة استهلاك موارد العقد في شبكات سلسلة الكتل المخصصة، من حيث التخزين والحوسبة ووحدة المعالجة المركزية وتوصيلات الشبكة والحالة على الإنترنت ومدة الاتصال بالإنترنت وغير ذلك.

ب) يوصى بأن يقدم مورد سلسلة الكتل كخدمة تنبيه بشأن نقص الموارد إلى عميل سلسلة الكتل كخدمة عندما تواجه عقد شبكة سلسلة الكتل المخصصة نقصاً في الموارد. ويتيعّن أن يوفر مورد سلسلة الكتل كخدمة حلولاً لعميل سلسلة الكتل كخدمة من أجل تخفيف حدة النقص في الموارد.

ج) يوصى بأن يسمح عميل سلسلة الكتل كخدمة لمورد سلسلة الكتل كخدمة بمراقبة حالة شبكات سلسلة الكتل المخصصة من حيث معدل إنشاء الكتل ومولدات الكتل وحجم الكتل وغيرها.

د) بأن يوفر مورد سلسلة الكتل كخدمة إنذاراً بالتسلل إلى عميل سلسلة الكتل كخدمة للعملاء عندما تُرصد حالة الشبكة على أنها غير طبيعية. ويتعين أن يزود مورد سلسلة الكتل كخدمة عميل سلسلة الكتل كخدمة بالتحليل غير الطبيعي الناجم ومعلومات عن العقد غير الطبيعية ذات الصلة والحلول الموصى بها.

10.8 نظام كشف الاقتحام

يوصى بأن يوفر مورد سلسلة الكتل كخدمة ويحدث الآليات الخاصة بمنع الشفرات الضارة وحالات الاقتحام الأخرى.

أ) يجب أن يوفر مورد سلسلة الكتل كخدمة القواعد الأمنية للعقد الذكي ومكتبة خاصة بالثغرات. ويتعين أن يوفر مورد سلسلة الكتل كخدمة سطوح بينية للنفاذ بنسق مشترك لاكتشاف الثغرات.

ب) يجب أن يقوم مورد سلسلة الكتل كخدمة بتثبيت برمجيات لمكافحة البرمجيات الضارة أو تشكيل برمجيات مزودة بالوظائف المقابلة لاكتشاف البرمجيات الضارة وإزالتها.

ج) يوصى بأن يوفر مورد سلسلة الكتل كخدمة الوقاية من الشفرات الضارة في كل عقدة من عقد سلسلة الكتل والقضاء على الشفرة الضارة قبل النفاذ إلى شبكة سلسلة الكتل.

د) يوصى بأن يوفر مورد سلسلة الكتل كخدمة لوائح بشأن آليات منع الشفرات الضارة، بما في ذلك التحديث الدوري لمكتبة الشفرات الضارة والتحقق منها والقضاء عليها بانتظام.

هـ) يوصى بأن يلزم مورد سلسلة الكتل كخدمة عميل سلسلة الكتل كخدمة بإجراء تقييم منتظم لفعالية التدابير التقنية لمكافحة هجمات الشفرات الضارة.

11.8 التدقيق الأمني

يوصى باستخدام مورد سلسلة الكتل كخدمة لواحد أو أكثر من مطوري سلسلة الكتل كخدمة لإجراء تدقيق أمني على البنية التحتية لسلسلة الكتل وشفرة المصدر والوظائف الأساسية الأخرى.

أ) يوصى بأن يختار مورد سلسلة الكتل كخدمة واحداً أو أكثر من مطوري سلسلة الكتل كخدمة لإجراء تقييم الأمن وتدقيقه فيما يتعلق بالبرمجيات الأساسية لسلسلة الكتل والشبكة وبيئات التشغيل الأخرى قبل بدء تشغيل خدمة سلسلة الكتل على الإنترنت، لضمان إمكانية التحكم في المخاطر الأمنية على مستوى البنية التحتية.

ب) يوصى بأن يكون لدى مورد سلسلة الكتل كخدمة واحداً على الأقل من مطوري سلسلة الكتل كخدمةلإجراء تدقيق أمني لشفرة المصدر، يركز بشكل أساسي على المخاطر ومشكلات الجودة على مستوى شفرة المصدر.

ج) يوصى بأن يقدم مطور سلسلة الكتل كخدمة تقرير تدقيق لشفرة المصدر إلى مورد سلسلة الكتل كخدمة بما يشمل عناصر الامتثال/الانتهاك واقتراحات لمراجعة شفرة المصدر المدرجة.

د) يوصى بأن يلزم مورد سلسلة الكتل كخدمة مطور سلسلة الكتل كخدمة بإجراء تقييم لوظائف إدارة الهوية والنفاذ لضمان عدم وجود مخاطر مثل تسرب المفتاح الخاص وتسرب معلومات المستعملين.

12.8 إدارة وظائف الأطراف الثالثة

يوصى بأن يضمن مورد سلسلة الكتل كخدمة عمل وظائف الأطراف الثالثة بشكل آمن على النحو المحدد مسبقاً.

أ) يجب أن يوضح مورد سلسلة الكتل كخدمة المتطلبات الأمنية والوظيفية للموردين الذين يمثلون أطرافاً ثالثة.

ب) يجب أن يوقع مورد سلسلة الكتل كخدمة اتفاقات التعاون لمكونات الخدمة مع موردي الخدمات الذين يمثلون أطرافاً ثالثة وتوضيح التزاماتهم ومسؤولياتهم.

ج) يوصى بأن يقوم مورد سلسلة الكتل كخدمة بمراقبة أو تدقيق مستوى خدمات الأطراف الثالثة وتقييمها بموجب الاتفاق الموقع.

13.8 أمن سلسلة التوريد

يوصى بأن يعمل مورد سلسلة الكتل كخدمة على ضمان أن تكون سلسلة التوريد الخاصة بها متينة لمواجهة موردي الخدمات الضارين وتغير الموردين.

أ) يجب أن يقوم مورد سلسلة الكتل كخدمة بتطوير سياسات وإجراءات لإدارة أمن سلسلة التوريد، بما في ذلك معايير إدارة الأمن للمشاركين في سلسلة التوريد.

ب) يجب أن يقوم مورد سلسلة الكتل كخدمة بإجراء تقييم بشكل روتيني لنقاط ضعف سلسلة التوريد في البنية التحتية، واستخدام البرامج مفتوحة المصدر في النظام.

ج) يوصى بأن يحيط مورد سلسلة الكتل كخدمة عميل سلسلة الكتل كخدمة بمخاطر سلسلة التوريد في سلسلة الكتل كنظام للخدمات.

د) يجب أن يؤكد مورد سلسلة الكتل كخدمة تنوع مورديه من البرمجيات والأجهزة التي لا غنى عنها.

الجدول 1 – المتطلبات الأمنية لسلسلة الكتل كخدمة

التهديدات الأمنية		المتطلبات الأمنية													
		التشكيلة الأمنية	إدارة الهوية والنفاذ	إدارة المفاتيح	حماية الخصوصية	أمن محركات التشفير	أمن التوصيل بين النظراء	أمن آلية الموافقة	أمن العقد الذكي	مراقبة الموارد	نظام كشف الاقتحام	التدقيق الأمني	إدارة وظائف الأطراف الثالثة	أمن سلسلة التوريد
مورد سلسلة الكتل كخدمة	1.1.7	✓	✓	✓	✓				✓			✓	✓	✓
	2.1.7					✓	✓	✓	✓		✓	✓	✓	✓
	3.1.7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	4.1.7							✓	✓	✓	✓			
	5.1.7										✓	✓	✓	✓
	6.1.7		✓	✓										
	7.1.7		✓										✓	
	8.1.7											✓	✓	✓
	9.1.7												✓	
مطور سلسلة الكتل كخدمة	1.2.7			✓	✓	✓	✓	✓		✓	✓		✓	
عميل سلسلة الكتل كخدمة	1.3.7		✓	✓										
	2.3.7	✓								✓			✓	

بيبليوغرافيا

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3530] Recommendation ITU-T Y.3530 (2020), *Cloud computing – Functional requirements for blockchain as a service*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.
<https://www.iso.org/standard/73771.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2023