الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1407

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

التطبيقات والخدمات الآمنة (2) – أمن تكنولوجيا السجلات الموزعة (DLT)

المتطلبات الأمنية لخدمة إثبات السلامة الرقمية القائمة على تكنولوجيا السجلات الموزعة

التوصية ITU-T X.1407

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

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

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

المتطلبات الأمنية لخدمة إثبات السلامة الرقمية القائمة على تكنولوجيا السجلات الموزعة

ملخص

تحدد التوصية X.1407 التهديدات الأمنية والمتطلبات الأمنية في إثبات السلامة الرقمية القائمة على تكنولوجيا السجلات الموزعة (DLT).

ويتم تخزين الإثبات الأصلي خارج السلسلة. وتخزَّن قيم البيانات المختزلة داخل السلسلة. وتحلل التوصية ITU-T.X.1407 التهديدات الأمنية التي قد تتعرض لها خدمات إثبات السلامة الرقمية القائمة على تكنولوجيا DLT، أي تسجيل الإثبات ومصدر الإثبات. وتصف هذه التوصية أيضاً المتطلبات الأمنية التي يمكن أن تدرأ التهديدات الأمنية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1407	2022-01-07	17	11.1002/1000/14800

مصطلحات أساسية

إثبات السلامة الرقمية، تكنولوجيا السجلات الموزعة، التهديدات الأمنية والمتطلبات الأمنية.

* 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 هو 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 اختراع/حقوق تأليف برمجيات 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 قواعد البيانات المناسبة لقطاع تقييس الاتصالات المتاحة من خلال الموقع الإلكتروني لقطاع تقييس الاتصالات في العنوان http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

المتطلبات الأمنية لخدمة إثبات السلامة الرقمية القائمة على تكنولوجيا السجلات الموزعة

1 نطاق التطبيق

تحدد هذه التوصية التهديدات الأمنية والمتطلبات الأمنية للإثبات الرقمي لسلامة الكيان القائمة على تكنولوجيا السجلات الموزعة (DLT). وتوفر منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT خدمات للتوزيع والاستعلام وتتبع الإثبات الرقمي لسلامة الكيان باستخدام تكنولوجيا السجلات الموزعة.

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 للمراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى 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.1402] التوصية ITU-T X.1402 (2020)، *إطار أمني لتكنولوجيا السجلات الموزعة*.

[ITU-T X.1404] التوصية ITU-T X.1404 (2020)، *ضمان الأمن لتكنولوجيا السجلات الموزعة*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في القسم 1.4 من [b-ISO 23257] وفي وثائق أخرى:

1.1.3 السجلات الموزَّعة (distributed ledger) [b-ITU-T X.1400]: نوع من السجلات التي يمكن تقاسمها واستنساخها ومزامنتها بطريقة موزَّعة لامركزية.

2.1.3 تكنولوجيا السجلات الموزَّعة (distributed ledger technologies, (DLT)) (DLT) [b-ISO 22739]: تكنولوجيا تمكِّن من تشغيل السجلات الموزَّعة واستخدامها.

3.1.3 منصة تكنولوجيا السجلات الموزَّعة (distributed ledger technology platform) [b-ISO 22739]: مجموعة من كيانات المعالجة والتخزين والاتصالات التي توفر معاً مقدرات نظام DLT في كل عقدة في نظام DLT.

4.1.3 السلامة (integrity) [b-ISO 13491-2]: خاصية بقاء البيانات على حالها دون أن يطرأ عليها تغيير أو تلف على نحو غير مرخص به.

5.1.3 السجل (ledger) [b-ITU-T X.1400]: مخزن معلومات يحتفظ بسجلات نهائية وثابتة (غير قابلة للتغيير) للمعاملات.

6.1.3 عقد ذكي (smart contract) [b-ISO 22739]: برنامج حاسوب مختزن في نظام DLT حيث يتم تسجيل حصيلة أي تنفيذ للبرنامج في السجل الموزع.

7.1.3 تهديد (threat) [b-ISO/IEC 27000]: سبب محتمل لحدث غير مرغوب فيه قد يُلحق الضرر بالنظام أو المنظمة.

2.3 المصطلحات المعرّفة في هذه التوصية

لا يوجد.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

DDoS رفض الخدمة الموزع (*Distributed Denial of Service*)

DLT تكنولوجيا السجلات الموزعة (*Distributed Ledger Technology*)

PoS إثبات المصلحة (*Proof of Stake*)

PoW إثبات العمل (*Proof of Work*)

PBFT التسامح العملي في الأخطاء البيزنطية (*Practical Byzantine Fault Tolerance*)

5 الاصطلاحات

تستخدم هذه التوصية صيغ الأفعال التالية للتعبير عن الأحكام:

أ) "يجب" تشير إلى اشتراط مطلوب

ب) "ينبغي" تشير إلى التوصية بأمر ما

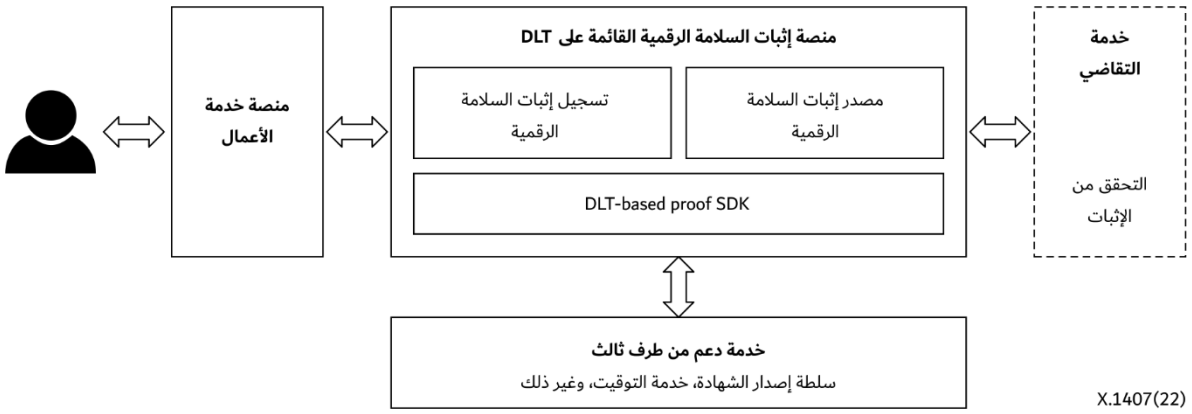
ج) "يجوز" تشير إلى السماح بأمر ما

د) "يمكن" تشير إلى الإمكانية والمقدرة على أمر ما.

6 نظرة عامة

تعتبر عملية إثبات سلامة بيانات معينة تحدياً عندما تكون البيانات متناثرة عبر أنظمة مختلفة. وبالإضافة إلى ذلك، قد تتطلب عملية التحقق من السلامة البحث في العديد من قواعد البيانات أو الأنظمة، أو البحث يدوياً في نسخ ورقية. ويؤخذ على هذه الحالة خلو التسلسل التاريخي الكامل للمعاملة؛ ومن ثم قد يؤدي ذلك إلى تأخيرات وجهود وتكاليف إضافية واتخاذ القرار الخطأ.

وتتمثل تكنولوجيا السجلات الموزعة (DLT) في سجلات لامركزية منيعة على العبث تشكل مستوى من الثقة ضرورياً لتبادل القيمة دون الاستعانة بوسطاء. وهي تعتمد على قواعد بيانات لامركزية توفر سجلات تعاونية شفافة قابلة للتحقق وقابلة للتدقيق بشأن سلامة كل المعاملات. وهكذا، فإن ميزات التكنولوجيا DLT التي يمكن تتبعها والمنيعة على العبث توفر حلاً لإثبات السلامة الرقمية حيث لا يمكن تزوير البيانات الأصلية أو المساس بها دون وسيلة لاكتشاف التغييرات.



الشكل 1 – رسم توضيحي لإثبات السلامة الرقمية القائمة على تكنولوجيا DLT

تتضمن السيناريوهات الأساسية في منصات إثبات السلامة الرقمية القائمة على تكنولوجيا DLT تسجيل الإثبات ومصدر الإثبات. حيث يستهل المستخدم في منصة خدمة الأعمال نداء خدمة إثبات رقمي ويسجل الإثبات في نظام DLT ويختزن اختزال التواقيع الرقمية المستخرجة من خلال عقد تسجيل إثبات الملكية الفكرية. وتعتمد عملية التحقق من سلامة الإثبات على التحقق من قيمة اختزال الإثبات ومقارنة الاختزال مع الاختزالات المختزنة في نظام DLT. وعلاوةً على ذلك، ولضمان الاستخدام القانوني للإثبات الرقمي وحماية حقوق المستخدم، يتم توفير خدمة الاستعلام والتحقق الرقمي لأغراض التحقيقات الجنائية بشأن التقاضي عبر الإنترنت.

وعلى الرغم من أن ميزات DLT، التي يمكن تتبعها والمنيعة على العبث، تمكّن من تحكم واستغلال أفضل لسلامة السجلات، فإن هناك تهديدات أمنية في اعتماد نظام DLT. وبعض التهديدات موجه إلى المستخدمين، وبعضها إلى الإثبات الرقمي، والبعض الآخر إلى عمليات تسجيل الإثبات والمصدر. لذلك، من الضروري والمفيد تلخيص التهديدات الأمنية في فئات مختلفة بناءً على تحليلات الأنشطة الداخلة في إثبات السلامة الرقمية القائم على نظام DLT. وبناءً على تحليل هذه التهديدات، تم تحديد مجموعة من المتطلبات الأمنية.

7 أصحاب المصلحة والعمليات الخاصة بإثبات السلامة الرقمية القائمة على تكنولوجيا DLT

1.7 أصحاب المصلحة

1.1.7 أصحاب المصلحة الداخليون

ينبغي أن يشمل أصحاب المصلحة الداخليون ما يلي:

أ) المستخدم

ب) منصة خدمات الأعمال

ج) منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT.

2.1.7 أصحاب المصلحة الخارجيون

يشمل أصحاب المصلحة الخارجيون ما يلي:

أ) مقدمو الدعم من الجهات الخارجية، بما في ذلك منظمات إصدار الشهادات (CA) وخدمة التوقيت وخدمات أخرى؛

ب) الوكالات التنظيمية، بما في ذلك الوكالات القضائية الوطنية والمنظمات الأخرى ذات الصلة بالتقاضي.

2.7 عمليات إثبات السلامة الرقمية القائمة على تكنولوجيا DLT

1.2.7 تسجيل إثبات السلامة الرقمية

تشمل العمليات الرئيسية لتسجيل إثبات السلامة الرقمية القائمة على تكنولوجيا DLT ما يلي:

أ) يتفاعل المستخدم مع منصة خدمة الأعمال، وقد يولد الاحتياجات لحماية مصداقية المعلومات المتعلقة بالأعمال، وترسل منصة الأعمال الميزات المستخرجة من المعلومات الأصلية إلى منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT؛

ب) تقوم منصة إثبات السلامة الرقمية القائمة على DLT بتوليد أدلة إلكترونية انطلاقاً من الميزات المستخرجة وخاتم التوقيت والمعلومات الضرورية الأخرى؛

ج) تولد منصة إثبات السلامة الرقمية القائمة على نظام DLT قيمة اختزال فريدة للأدلة الإلكترونية من خلال وظائف اختزال التجفير (مثل SHA256)؛

د) تستحدث منصة خدمة الأعمال توقيعاً رقمياً لقيمة الاختزال باستخدام المفتاح الخاص للمالك؛

هـ) تحيل منصة خدمة الأعمال سجل الإثبات إلى عنوان العقد الذكي في السجلات الموزَّعة؛

و) تتحقق منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT من اكتمال التوقيع الرقمي والمعلومات وتقوم بتنفيذ العقد الذكي وتوليد تسجيل في السجل؛

ز) يرزَّم تسجيل الإثبات في كتلة جديدة وترسل الكتلة الجديدة إلى الشبكة.

2.2.7 مصدر إثبات السلامة الرقمية

تتضمن العملية الرئيسية لمصدر إثبات السلامة الرقمية ما يلي:

أ) يستعلم المستخدم عن إثبات السلامة الرقمية على أساس السجلات الموزعة؛

ب) في حالة التقاضي عبر الإنترنت، تقوم منصة التقاضي بإجراء تحقيق جنائي للإثبات الرقمي القائم على التسجيلات في السجلات الموزَّعة.

8 التهديدات الأمنية لخدمة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT

يحلل هذا البند التهديدات الأمنية التي تستهدف أصحاب المصلحة، أي المستخدم ومنصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT والعمليات الداخلة في إثبات السلامة الرقمية القائمة على تكنولوجيا DLT، أي تسجيل إثبات السلامة الرقمية ومصدر إثبات السلامة الرقمية. والتهديدات التي تتعرض لها مكونات البروتوكول والشبكة والبيانات في التطبيقات القائمة على تكنولوجيا DLT موصوفة بالتفصيل في التوصية [ITU-T X.1401].

1.8 التهديدات الأمنية بالنسبة للمستخدم

1.1.8 تزوير هوية المستخدم

تقدم المستخدمون المسجَّلون طلبات غير قانونية باستخدام هويات مزورة للحصول على أذون لا تتطابق مع هوياتهم.

2.1.8 تسرب المفتاح الخاص

تشمل تهديدات تسرب المفتاح الخاص في سجل ما أساساً الهجمات البرمجية على العملاء والهجمات المادية (مثلاً، كشف مفاتيح مطبوعة للآخرين). ويمكّن تسرب مفتاح خاص المستخدمين الآخرين من الدخول إلى منصة الإثبات القائمة على تكنولوجيا DLT، مما يعرض أمنها للخطر. والتهديد بتسرب المفتاح الخاص موصوف بالتفصيل في الفقرة 2.3.6 من التوصية [ITU-T X.1401].

3.1.8 فقدان المفتاح الخاص

تشمل تهديدات فقدان المفتاح الخاص أساساً هجمات البرمجيات الخبيثة والهجمات المادية (مثلاً، فقدان مفاتيح خاصة مطبوعة على الورق)، وما إلى ذلك. وقد تؤدي هذه السلوكيات إلى الكشف عن خصوصية المستخدم مما يمكّن المستخدمين ذوي النوايا السيئة من الدخول إلى منصة الإثبات القائمة على تكنولوجيا DLT، وتدمير أمنها. والتهديد بفقدان المفتاح الخاص موصوف بالتفصيل في الفقرة 3.3.6 من التوصية [ITU-T X.1401].

4.1.8 الكشف عن الخصوصية

قد تتضمن معلومات إثبات المالك معلومات شخصية حساسة مثل الاسم ومعلومات الهوية، وقد تكون هناك مشكلة في تسرب خصوصية المستخدم أثناء عملية تسجيل الإثبات. والتهديد بالكشف عن الخصوصية موصوف بالتفصيل في الفقرة 1.3.6 من التوصية [ITU-T X.1401].

2.8 التهديدات الأمنية بالنسبة لتسجيل الإثبات

1.2.8 تزوير الإثبات

وفقاً لخوارزمية استخراج الميزات الخاصة بالإثبات الرقمي، يمكن للمهاجمين أن يحددوا قيم ميزات مختلفة لمحتوى مماثل للمستند الأصلي. وعلى هذا النحو، يمكن للمهاجمين كتابة محتوى غير قانوني في السجلات الموزعة.

2.2.8 العبث بالإثبات

يستطيع المهاجم ذو النية السيئة العبث بإثبات المستند الأصلي أو إتلاف سلامة الإثبات وتوفره، مما يؤدي إلى تدوين الإثبات المتلاعب به في السجلات الموزعة. ويمكن أن تؤدي هجمات خوارزمية التجفير غير التناظرية إلى نقل وتخزين غير آمنين. وهجوم خوارزمية التجفير غير التناظرية موصوف بالتفصيل في الفقرة 5.1.6 من التوصية [ITU-T X.1401].

3.2.8 الهجوم بالاعتماد على خاتم التوقيت

قد تتلاعب الهجمات بخدمة خاتم التوقيت لمنصة الإثبات القائمة على تكنولوجيا DLT، مما يؤدي إلى عجز المنصة عن الحفاظ على تسلسل أحداث تسجيل الإثبات على وجه الدقة، وبالتالي إلى عدم القدرة على توفير أساس فعال للتحقيق الجنائي بشأن مصدر الإثبات.

4.2.8 الهجوم بأغلبية 51%

عندما يتمكن المهاجمون من أكثر من 51% من قوة الحوسبة، يمكنهم بناء سلسلة جديدة. ومن شأن السلسلة الجديدة أن تبطل إثبات السلسلة الرئيسية. وعلاوة على ذلك، قد يؤدي الهجوم بأغلبية 51% إلى نجاح تسجيل المتعدي. والهجوم بأغلبية 51% موصوف بالتفصيل في الفقرة 1.1.6 من التوصية [ITU-T X.1401].

5.2.8 الهجوم بالرشوة

عندما يرشو المهاجمون ذوو الموارد الكافية عُقداً لديها حقوق التصويت، يمكنهم الإضرار بحقوق ومصالح شبكة السجلات الموزعة للإثبات. وعلى هذا النحو، يكتب المهاجمون معلومات إثبات غير قانوني في شبكة السجلات الموزعة للإثبات. والهجوم بالرشوة موصوف بالتفصيل في الفقرة 1.1.6 من التوصية [ITU-T X.1401].

6.2.8 الهجوم بحجب الكتلة

يستطيع المهاجم، في منصة إثبات قائمة على تكنولوجيا DLT استناداً إلى خوارزمية إجماع إثبات العمل (PoW)، حجب كتلة قام باستغلالها واستغلال الكتلة التالية سراً إذا كان يملك القدرة الكافية على ذلك. ومن خلال تحرير أكثر من كتلة واحدة عندما يقوم مستغلون آخرون بتوليد كتلة ما، يمكن للمهاجم أن يجعل المستغلين الآخرين يهدرون طاقتهم. والهجوم يستهدف مشغل منصة يقبل

التحقق الصفري. ويمكن بذلك إبطال إثبات السلسلة الرئيسية. وقد يؤدي أيضاً إلى نجاح تسجيل المتعدي. والهجوم بحجب الكتلة موصوف بالتفصيل في الفقرة 1.1.6 من التوصية [ITU-T X.1401].

7.2.8 الهجوم بالقفز بين السلاسل

يستطيع المهاجم التبديل بين سلاسل الكتل المختلفة من خلال الاستفادة من خوارزميات الضبط الصعبة في السلسلة. ويمكن أن يؤدي ذلك إلى مكافأة غير عادلة للمهاجمين مع خسارة للمستخدمين الآخرين. وقد يتسبب أيضاً في زيادة كبيرة في قوة الحوسبة الفعلية في المجموعة المستغِلة. وقد يؤدي أيضاً إلى نجاح تسجيل المتعدي. والهجوم بالقفز بين السلاسل موصوف بالتفصيل في الفقرة 1.1.6 من التوصية [ITU-T X.1401].

8.2.8 الهجوم برفض الخدمة الموزع

يستطيع المهاجم، في منصة إثبات قائمة على تكنولوجيا DLT، تعطيل الشبكة من خلال هجمات خدمة رفض الخدمة الموزع (DDoS)، حيث الهجوم التعددي وهجوم الكسوف من الأساليب الشائعة. وقد يؤدي هذا إلى نجاح تسجيل الإثبات الخبيث. والهجوم التعددي موصوف بالتفصيل في الفقرة 3.2.6 وهجوم الكسوف في الفقرة 1.2.6 من التوصية [ITU-T X.1401].

9.2.8 الهجوم باختطاف بروتوكول بوابة الحدود (BGP)

يستطيع المهاجم أن يستغل بروتوكول بوابة الحدود المختطف وعُقد الشبكة للسجلات الموزعة المقسومة إلى جزأين أو أكثر. ونتيجة لذلك، يتم تقسيم النظام DLT إلى سلسلتين متوازيتين أو أكثر. وفي هذا الوقت، يمكن إجراء تسجيل الإثبات وتسجيل الإثبات الخبيث في فروع موازية. وبعد توقف الهجوم، يجري توحيد السجل الموزع للإثبات مع أطول سلسلة رئيسية، ويتم تجاهل الفروع الأخرى، وتصبح جميع سجلات الإثبات في هذه السلاسل غير صالحة، مما قد يؤدي إلى نجاح تسجيل الإثبات الخبيث.

3.8 التهديدات الأمنية بالنسبة لمصدر الإثبات

1.3.8 الهجوم بكتابة المعلومات الخبيثة

جميع بيانات المعاملات في النظام DLT غير قابلة للإزالة. وبعد كتابة المعلومات في النظام DLT لا يمكن حذفها. وقد يكتب المهاجمون معلومات خبيثة في السجلات الموزعة من خلال شن هجمات في العقود الذكية، مثل الهجمات المتعلقة بالاستثناءات التي تم التعامل معها بشكل خاطئ، على النحو الوارد وصفه في الفقرة 2.1.6 من التوصية [ITU-T X.1401]. وتولد المنصة كتلاً جديدة مما يؤدي إلى هجمات بالكتل الاقتحامية ويؤثر بالتالي على أداء منصة الإثبات القائمة على تكنولوجيا DLT.

2.3.8 الكشف عن معلومات الإثبات

ينبغي، في مصدر الإثبات، استخدام خوارزمية لتجفير معلومات الإثبات وتخزينها. ومن المهم ضمان أمن خوارزمية التجفير. وقد تؤدي هجمات خوارزمية التجفير غير المتناظرة إلى حالة غير آمنة لمنصة الإثبات القائمة على تكنولوجيا DLT. وهجوم خوارزمية التجفير غير المتناظرة موصوف بالتفصيل في الفقرة 5.1.6 من التوصية [ITU-T X.1401].

9 المتطلبات الأمنية لإثبات السلامة الرقمية القائمة على تكنولوجيا السجلات الموزعة (DLT)

تصف هذه الفقرة المتطلبات الأمنية لإثبات السلامة الرقمية القائم على تكنولوجيا DLT استناداً إلى تحليل التهديدات الأمنية الموضحة في الفقرة 7. وبالإضافة إلى ذلك، تصف هذه الفقرة المتطلبات الأمنية لأصحاب المصلحة، أي المستخدم ومنصة إثبات السلامة الرقمية والعمليات الداخلة في خدمات إثبات السلامة الرقمية القائم على نظام DLT، وهي بالتحديد تسجيل الإثبات الرقمي ومصدر الإثبات الرقمي. والمتطلبات الأمنية للبيانات والشبكة والإجماع والتطبيق موصوفة بالتفصيل في الفقرات من 1.8 إلى 4.8 من التوصية [ITU-T X.1402].

1.9 المتطلبات الأمنية للمستخدم

1.1.9 حماية هوية المستخدم

جرى تحديد المتطلبات الأمنية التالية بشأن تجنب تزوير الهوية من أجل منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT.

أ) ينبغي أن تحدد منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT سلطة التشغيل لمختلف المستخدمين. وينبغي أن تسمح المنصة للمستخدم باستخدام المفتاح الخاص لتوقيع المعلومات وإرسالها إلى النظام DLT. وينبغي أن يسترجع النظام DLT المفتاح العام بناءً على التوقيع ويحدد المستخدمين بناءً على المفتاح العام ويصادق على عمليات المستخدم؛

ب) عندما يسجل مستخدم ما في المنصة، يجب على المنصة أن تقوم أولاً بتدقيق معلومات هوية المستخدم، وقد تخصص بعد ذلك تسمية لكل مستخدم؛

ج) ينبغي أن تكتب منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT جميع عمليات كل مستخدم في السجلات الموزعة؛

د) ينبغي أن تشترط منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT توفر وظيفة مصادقة الهوية لكل تسجيل إثبات، بما في ذلك التحكم في النفاذ وكلمة المرور والتوقيع الرقمي والتعرف بالقياس الحيوي، وما إلى ذلك.

2.1.9 حماية المفتاح الخاص

جرى تحديد المتطلبات الأمنية التالية المتعلقة بحماية المفتاح الخاص لمنصة الإثبات القائمة على تكنولوجيا DLT.

أ) ينبغي أن تمنع منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT تسرب المفتاح الخاص – وينبغي لمشغل منصة الإثبات القائم على تكنولوجيا DLT أن يمنع الشفرة الخبيثة من التسلل لدى عميله؛

ب) ينبغي أن تمنع منصة إثبات السلامة الرقمية القائمة على تكنولوجيا DLT فقدان المفتاح الخاص – وينبغي لمستخدمي منصة الإثبات القائم على تكنولوجيا DLT الاحتفاظ بالمفتاح الخاص في مكان آمن وتجنب ترك المفاتيح الخاصة على وسائط مادية وغير مادية يسهل النفاذ إليها (من قبيل ورق الطباعة، مثلاً) دون أي آليات حماية – وتشمل الإجراءات المضادة المحتملة شفرات أرقام تعرّف الهوية الشخصية وكلمات المرور وبصمات الأصابع وغيرها من معلومات القياس الحيوي، وما إلى ذلك.

3.1.9 حماية الخصوصية

ينبغي أن تعتمد منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT تدابير الحماية الأمنية ذات الصلة في روابط معالجة المعلومات الخاصة بجمع معلومات المستخدم وتخزينها واستخدامها ومشاركتها ونقلها والإفصاح عنها علناً، وما إلى ذلك، لمنع استقاء معلومات المالك على نحو غير قانوني وإساءة استخدامها وتسربها، ولتعزيز حماية الحقوق والمصالح المشروعة للمالك.

2.9 المتطلبات الأمنية لتسجيل الإثبات

1.2.9 تجنب تزوير الإثبات

جرى تحديد المتطلبات الأمنية التالية المتعلقة بتجنب تزوير الإثبات الرقمي لمنصة الإثبات القائم على تكنولوجيا DLT.

أ) ينبغي أن توفر منصة الإثبات القائم على تكنولوجيا DLT خوارزميات إجماع مع مستوى من ضمان الأمن (LoSA) وقوة آلية إجماع (CMS) [ITU-T X.1404]، من قبيل التسامح العملي في الأخطاء البيزنطية (PBFT)، لتجنب تزوير الإثبات الرقمي؛

ب) ينبغي أن ترصد منصة الإثبات القائم على تكنولوجيا DLT قوة الحوسبة الفعلية للشبكة، لكشف التغيرات غير الطبيعية ومنع الهجمات بالقفز بين السلاسل؛

ج) ينبغي أن تعزز منصة الإثبات القائم على تكنولوجيا DLT صعوبة خوارزميات بناء القيمة الذاتية مع ضمان أن تكون كفاءة تشغيل النظام ضمن حدود معقولة.

2.2.9 تجنب العبث بالإثبات

جرى تحديد المتطلبات الأمنية التالية المتعلقة بتجنب العبث بالإثبات الرقمي لمنصة الإثبات القائم على تكنولوجيا DLT.

أ) ينبغي أن تستخدم منصة الإثبات القائم على تكنولوجيا DLT تجهيزات مجفرة؛

ب) ينبغي أن تستخدم منصة الإثبات القائم على تكنولوجيا DLT خوارزميات التجفير لضمان النقل الآمن لمعلومات الإثبات. وينبغي أن تستخدم خدمات الطرف الثالث ذات الصلة خوارزميات التجفير لضمان التخزين الآمن لمعلومات الإثبات. ينبغي أن تختار المنصة وخدمات الطرف الثالث ذات الصلة خوارزميات التجفير المناسبة، والتي ينبغي أن تكون حلاً وسطاً بين تكلفة الأمان وتكلفة الحوسبة وطول المفتاح – وربما تختار زيادة طول المفاتيح لتعويض المخاطر الناجمة عن زيادة قوة الحوسبة.

3.2.9 حماية تسجيل الإثبات

جرى تحديد المتطلبات الأمنية التالية المتعلقة بالتحكم بأمان التسجيل من أجل منصة الإثبات القائم على تكنولوجيا DLT.

أ) ينبغي أن تتزامن منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT مع خدمة توقيت طرف ثالث موثوق به؛

ب) ينبغي أن توفر منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT تحذيرات بشأن هجوم يتهدد الأمن ومواطن الضعف والشفرات الخبيثة وتحليل التهديدات وتسرب البيانات، بالإضافة إلى معلومات استخباراتية أخرى عن التهديدات، وأن تحدد المشكلات الموجودة في المنصة من خلال مسح مواطن الضعف واختبار الأمن التلقائي؛

ج) ينبغي أن توفر منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT مصادقة الهوية والتحكم في النفاذ للتخفيف من مخاطر الهجمات التي تتهدد الأمن، من قبيل العبث الخبيث والهجوم عن بُعد؛

د) ينبغي، بالنسبة لتطبيقات الأجهزة المتنقلة، أن توفر منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT أساليب حماية أمنية، من قبيل التعزيز وتشويش المصدر لمنع التحليل العكسي وفك التجميع ودمج الشفرات الخبيثة؛

هـ) يمكن للمنصة أن تستخدم تكنولوجيا نقطة الرصد للكتابة إلى العميل من خلال تشفير صارم بحيث يقبل العميل جميع المعاملات الفعالة قبل نقطة الرصد، وبذلك يمنع الهجوم بأغلبية 51% – ينبغي لنقطة الرصد ما يلي: إضافة آلية إجماع محسنة لإثبات المصلحة (PoS) مع تدابير هامش وجزاء؛ تحديد خاتم توقيت للمعاملة؛ تحديد استيقان للعُقد الموثوقة من جهة خارجية لاستيقان الهوية؛ عدم قبول التأكيد الصفري.

و) يمكن أن تقوم المنصة بنشر ترشيح المنافذ لتنظيف حركة المرور غير الطبيعية، والدفاع الأمني السحابي والدفاع العالي من أجل استبانة نظام اسم الميدان (DNS)، في النظام لتوفير التنفيذ الآمن، وينبغي أن تنظم حجم كتلة البيانات لتجنب الهجمات الاقتحامية؛

ز) ينبغي أن توفر منصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT جمع الأدلة وتتبع الأحداث الأمنية وتحليل الأسباب، وتوفر أيضاً أساليب لاحتواء الهجمات.

3.9 المتطلبات الأمنية لمصدر الإثبات

1.3.9 الحماية من كتابة المعلومات الخبيثة

حرصاً على ضمان أمن مصدر الإثبات، ينبغي لمنصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT أن توفر ما يلي:

أ) تنظيم حجم كتلة البيانات لمنع العُقد من توليد الكتل الاقتحامية؛

ب) التأكد من أن الكيانات غير المخولة والمجهولة لا يمكنها البحث عن بيانات الحسابات وبيانات المعاملات في عُقد نظام السجلات الموزعة، أو النفاذ إلى هذه البيانات؛

ج) استخدام مكتبات تضمن سلامة الحسابات، من قبيل SafeMath؛

د) إجراء مراجعة للشفرات لتجنب تدفق الأعداد الصحيحة والاستثناءات التي تم التعامل معها بشكل خاطئ لمنع الهجمات في العقود الذكية؛

هـ) استخدام مولِّدات عشوائية لا يمكن التنبؤ بها لمنع المستخدمين ذوي النوايا السيئة من التحكم في نتائج العقود الذكية؛

و) ينبغي أن يكون تصميم التحكم في النفاذ أثناء وضع البرنامج صارماً قدر الإمكان لمنع العبث بملكية وظائف العقد الذكي من قبل المهاجمين للحصول على أعلى سلطة تشغيل.

2.3.9 حماية معلومات الإثبات

حرصاً على ضمان أمن معلومات الإثبات، ينبغي لمنصة إثبات السلامة الرقمية القائم على تكنولوجيا DLT:

أ) أن تستخدم التجهيزات المجفرة لتخزين معلومات الإثبات من خارج السلسلة؛

ب) أن تختار خوارزميات تجفير مناسبة، وينبغي أن تكون حلاً وسطاً بين تكلفة الأمان وتكلفة الحوسبة وطول المفتاح – وقد يقع الخيار على زيادة طول المفاتيح لتعويض المخاطر الناجمة عن زيادة قوة الحوسبة؛

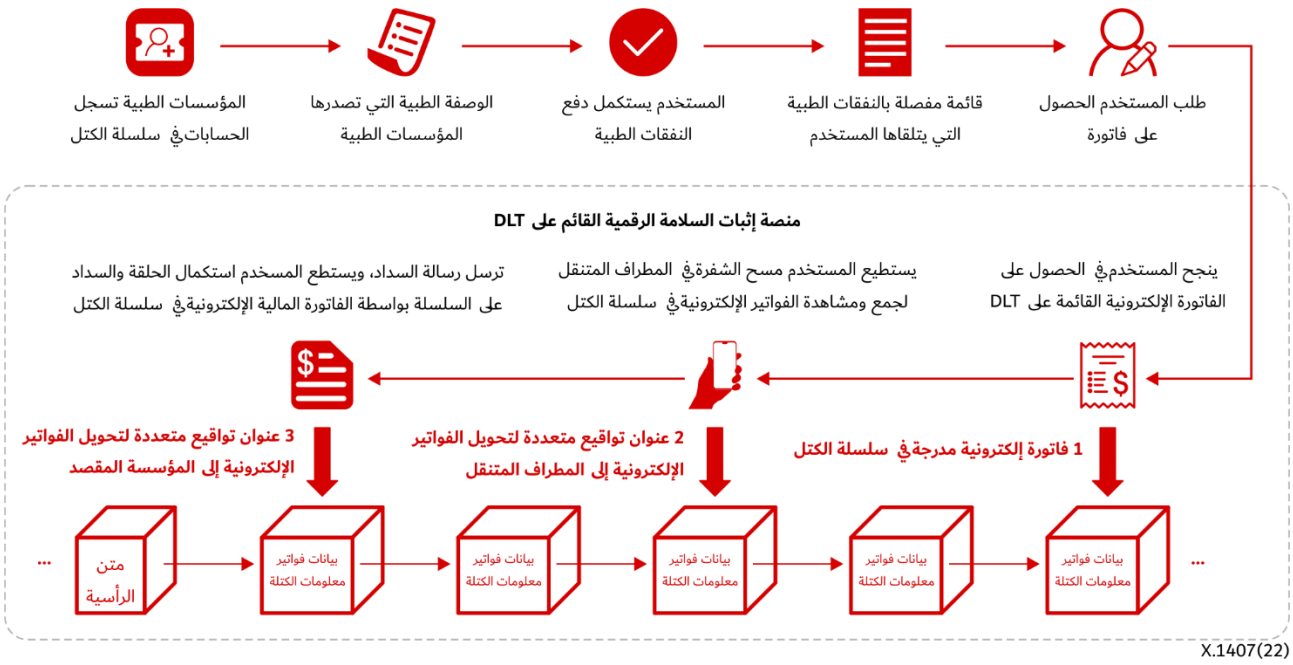
ج) أن تستخدم آلية فعالة للتحكم في النفاذ لضمان النفاذ القابل للتحكم إلى معلومات الإثبات.

التذييل I

حالة استخدام الفوترة الإلكترونية القائمة على تكنولوجيا السجلات الموزعة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

في ظل آلية الإجماع، لا يمكن التحقق إلا من الفواتير المكتوبة من قبل السلطات الضريبية والموافقة عليها، ولا يمكن تأكيد الفواتير المكتوبة بواسطة أي عُقد أخرى، ومن ثم ضمان مصداقية الفواتير. وباستخدام العقود الذكية، تحدث المعاملات والفوترة في آن واحد، وتتم مدفوعات المستهلك والفوترة بسلاسة. وثمة لمحة عامة عن هذه العملية في الشكل 1.I. للاطلاع على التفاصيل، يرجى الرجوع إلى الممارسة الموصى بها في المعيار [b-IEEE 2142.1-2021] للفوترة الإلكترونية باستخدام تكنولوجيا سلسلة الكتل.



الشكل 1.I – لمحة عن حالة استخدام الفوترة الإلكترونية القائمة على تكنولوجيا DLT

توصف حالة استخدام الفواتير الإلكترونية القائمة على تكنولوجيا السجلات الموزعة من قبل المؤسسات الطبية على النحو التالي:

أ) تقوم المؤسسات الطبية بتسجيل حساب في سلسلة الكتل والتوصيل بنظام الفوترة القائم على تكنولوجيا DLT وتعيين شروط الفوترة في السلسلة

ب) تُصدر المؤسسة الطبية وصفة طبية

ج) يكمل المستخدم دفع النفقات الطبية مشفوعة بوصفة طبية

د) يتلقى المستخدم قائمة مفصلة بالنفقات الطبية بعد إتمام الدفع

هـ) يتقدم المستخدم بطلب فوترة

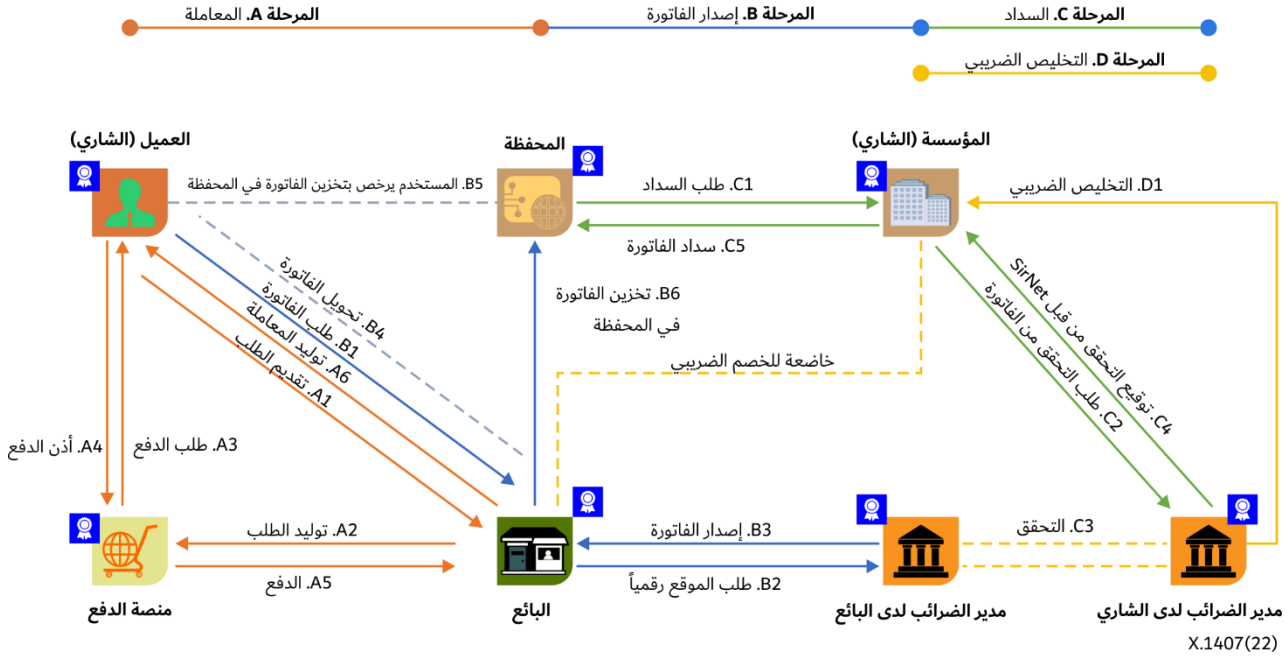
و) ينجح المستخدم في الحصول على فاتورة إلكترونية في سلسلة الكتل

ز) يستطيع المستخدم مسح الشفرة في المطراف المتنقل لاستلام ومشاهدة الفاتورة الإلكترونية في سلسلة الكتل

ح) يمكن للمطراف المتنقل إرسال رسائل السداد، ويمكن للمستخدم استخدام الفاتورة الإلكترونية في سلسلة الكتل لإكمال التداول والسداد في السلسلة.

ويمكن أن تتضمن عملية الفوترة القائمة على الدفع المراحل التالية:

- المرحلة A: المعاملة
- المرحلة B: إصدار الفاتورة
- المرحلة C: السداد
- المرحلة D: التخليص الضريبي



الشكل 2.I – مخطط انسيابي لحالة استخدام الفوترة الإلكترونية القائمة على تكنولوجيا DLT

في مرحلة المعاملة، عندما يتقدم العميل (أي الشاري) بطلب، يقوم مزود الخدمة (أي البائع) بتوليد الطلب عبر منصة الدفع، ثم تؤكد منصة الدفع الطلب بعد استلام ترخيص العميل، ويتم توليد الإيصال عند إجراء معاملة الدفع. ويمكن أن يكون الإيصال في شكل كتلة دفع عبر سلسلة دفع أو سجل في قاعدة بيانات مركزية.

وفي مرحلة إصدار الفاتورة، يقوم بإصدار الفاتورة مسؤول ضريبة المنشأ (Origin TAX) لدى التاجر بناءً على طلب العميل، من محفظة العميل مثلاً، ويتم استخدام إيصال الدفع باعتباره خرج المعاملة غير المنفق (UTXO) لإصدار الفاتورة. وتشتمل العُقد المشاركة على عُقد الإجماع الأساسية المثبتة في الطبقة الأساسية للسجل بالإضافة إلى عُقد التحقق المبسَّط من الدفع (SPV)، مثل عقدة التاجر وعقدة المحفظة الشخصية، وما إلى ذلك.

وفي مرحلة السداد، تعمل المؤسسة المرتبطة بالعملاء (CAE) كعقدة SPV تتحقق من الفاتورة عندما يستهل العميل عملية السداد، ويعاد دفع الفاتورة في المحفظة الشخصية باعتبارها UTXO.

وفي عملية التخليص الضريبي TAX، تنضم عُقد مسؤول الضرائب في الوجهة وعقدة CAE SPV إلى العملية، وتستخدم الفاتورة بمثابة UTXO لسداد ضريبة القيمة المضافة VAT.

وهناك عدة مزايا لنظام الفوترة الإلكترونية باستخدام تكنولوجيا DLT وهي كما يلي:

1 التأكد من أن الفاتورة أصلية وأن كامل عملية تحصيل الفاتورة وإصدارها وتداولها وإدخالها وسدادها قابلة للتتبع.

2 بيانات الفاتورة غير قابلة للعبث، ويشارك مكتب الضرائب وجهة إعداد الفواتير وجهة التداول وجهة السداد معاً في عملية مسك الدفاتر.

3 الفوترة الإلكترونية القائمة على تكنولوجيا DLT لا تحتاج إلى قرص ضريبي ومعدات خاصة. وبالنسبة للفواتير التقليدية، فإنها تتطلب عدة أقراص ضريبية لكل متجر في حالة سلسلة من المتاجر؛ ويتم سداد الفواتير الإلكترونية القائمة على تكنولوجيا DLT تلقائياً بواسطة برمجية تخطيط الموارد المؤسسية (ERP) ولا يترتب على تعدد المتاجر أي تكلفة إضافية.

4 بالنسبة للفواتير التقليدية، وإذا لم يتمكن عدد الفواتير المعتمدة من قبل السلطات الضريبية من تلبية احتياجات العمل بسبب زيادة مؤقتة في حجم الأعمال، يمكن لدافع الضرائب أن يتقدم بطلب إلى السلطات الضريبية للحصول على فواتير إضافية. غير أن توفير الفواتير القائمة على تكنولوجيا DLT يتم بناءً على الطلب ولا يحتاج إلى عمليات تطبيق إضافية.

5 يتطلب الأمر الوقت والجهد لجمع وشراء أوراق الفوترة التقليدية من مكتب الضرائب؛ أما الفواتير الإلكترونية القائمة على تكنولوجيا DLT فهي غنية عن الورق.

التذييل II

حالة الاستخدام للتحقق من الشهادات الأكاديمية القائمة في تكنولوجيا السجلات الموزعة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

التحقق من الشهادات عملية تستغرق وقتاً طويلاً، إذ إنها قد تتطلب أياماً أو أسابيع. ويهتم أرباب العمل باستيقان المؤهلات ويمضون الكثير من الوقت في التواصل مع الجامعات للتحقق من سلامة الشهادات ولضمان حصول المتقدمين على مؤهل لا تشوبه شائبة. ومن شأن سلسلة الكتل أن توفر الشفافية وأن تبسّط التشارك في الاطلاع على الشهادات المستيقن بها مع مجموعة متنوعة من أرباب العمل أو أي جهات أخرى.

ويستطيع أرباب العمل إثبات سلامة الشهادة الأكاديمية باستخدام تكنولوجيا DLT. وتوفر هذه التكنولوجيا مصدراً آمناً معترفاً به لتخزين مؤهلات الطلاب، ويمكن النفاذ إليه من قبل مجموعة متنوعة من المؤسسات والجامعات. ويوفر سجلاً عمومياً ثابتاً، حصيناً من التغييرات التي قد تطرأ على المؤسسة أو من فقدان سجلاتها الخاصة.

ويتكون هذا النمط من المكونات التالية:

المستخدمون

- جهة الإصدار (الجامعة)
- المتلقي (الطلاب)
- المتحقق (أرباب العمل)

الأنظمة

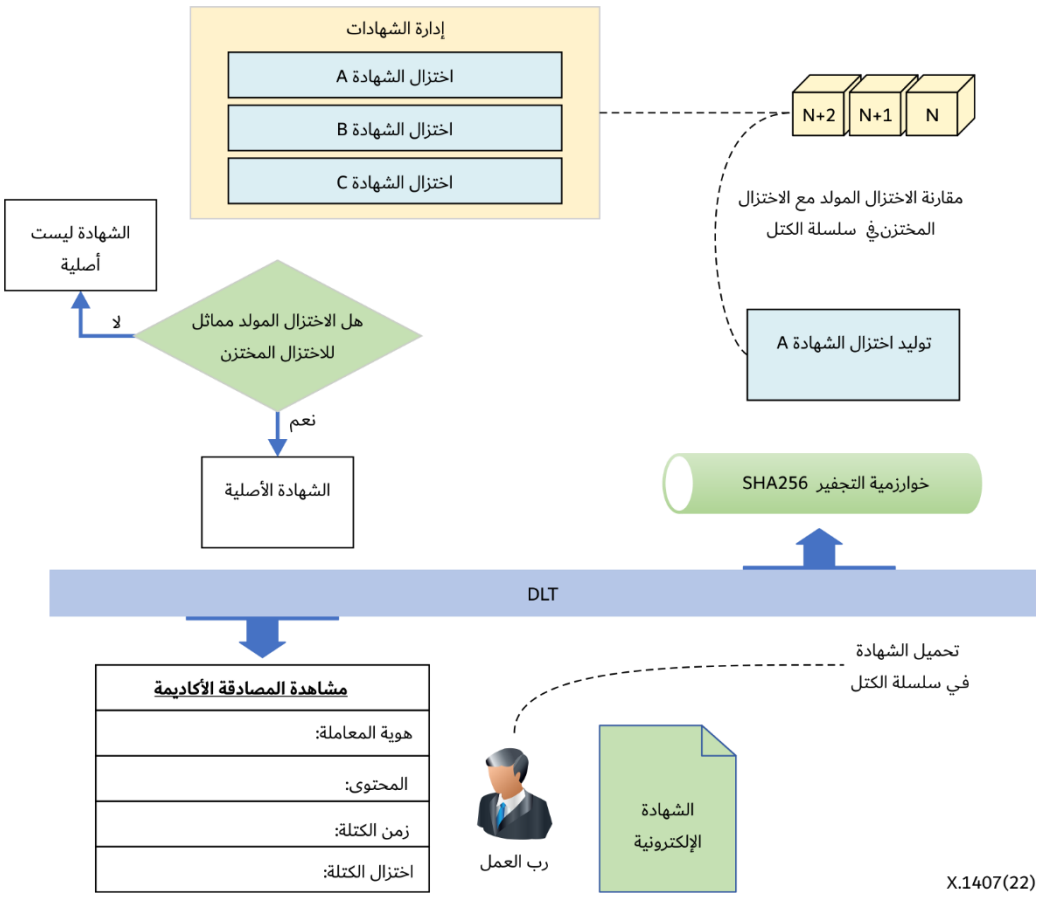
- عُقد الجامعات
- منصة سلسلة الكتل

البيانات

- اختزال الشهادات
- ملف الشهادات الإلكترونية

وتعتمد عملية التحقق من سلامة الشهادة على التحقق من قيمة اختزال الشهادة ومقارنة الاختزال مع الاختزال المختزن في سلسلة الكتل كما هو موضح في الشكل 1.II. وتشمل الخطوات ما يلي:

- تصدر الجامعة شهادة إلكترونية جديدة للطالب وتحمّل الملف في منصة النظام DLT.
- يقوم النظام DLT باختزال وتخزين ملف الشهادة.
- لإظهار إثبات السلامة، يقوم الطالب أو رب العمل بتحميل مستند الشهادة في منصة DLT.
- يقوم النظام DLT باختزال المستند ثم يقارن قيمة الاختزال المولدة مع الاختزال المختزن في سلسلة الكتل.
- إذا تطابق الاختزال المولد مع واحد من الاختزالات المختزنة في سلسلة الكتل عندئذ تكون الشهادة أصلية.



الشكل 1.II – لمحة عن حالة استخدام للتحقق من الشهادة الأكاديمية القائم على تكنولوجيا DLT

فوائد استخدام تكنولوجيا DLT لاستيقان الشهادات الأكاديمية:

- تتغلب على الصعوبات الحالية في عملية التحقق والاستيقان.
- تستطيع تجميع كل الجامعات في منصة واحدة.
- تشجع أرباب العمل على العمل مع الجامعات بطريقة منهجية.
- تساعد على حفظ المعلومات الأصيلة والكاملة وتقاسمها كمصدر واحد للوقائع.
- توفر الوقت والجهد والتكلفة.

بيبليوغرافيا

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

[b-ISO 13491-2] ISO 13491-2:2017(en), *Financial services – Secure cryptographic devices (retail) – Part 2: Security compliance checklists for devices used in financial transactions.* <*https://www.iso.org/obp/ui/#iso:std:iso:13491:-2:ed-4:v1:en*>

[b-ISO 23257] ISO 23257:2022, *Blockchain and distributed ledger technologies – Reference architecture. [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>

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

[b-IEEE 2142.1-2021] IEEE 2142.1-2021, *IEEE Recommended practice for e-invoice business using blockchain technology*. <https://standards.ieee.org/ieee/2142.1/7590/>

[b-ISO 56000] ISO 56000:2020, *Innovation management — Fundamentals and vocabulary*. <https://www.iso.org/standard/69315.html>

[b-ISO 5807] ISO 5807:1985, *Information processing — Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts*. <https://www.iso.org/standard/11955.html>

[b-Kaur] Kaur, S., Chaturvedi, S., Sharma, *A. Kar, J. (2021), A Research Survey on Applications of Consensus Protocols in Blockchain*, Security and Communication Networks, Vol. 2021, Article ID 6693731, January, pp. 1-22. https://doi.org/10.1155/2021/6693731

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، 2022