

تعزيز أصالة السجلات الأرشيفية بتقنية سلاسل الكتل

مارك بيل، أليكس غرين، جون شيريدان، جون كولوموس، دانيال كوبر، تو بوي، أوليفيه تيرو، جيز هيفينز



المخلص:

يتناول هذا المقال التحديات التي تفرضها التقنيات الرقمية على الممارسات الأرشيفية الراسخة، ولا سيما سهولة تعديل السجلات الرقمية وتراجع الثقة العامة في عصر الأخبار الزائفة والمحتوى المولّد بالذكاء الاصطناعي. ويعرض المؤلفون مشروع (ARCHANGEL) الذي يستخدم تقنية سلاسل الكتل لتسجيل المجاميع الاختبارية وبيانات وصفية أخرى للسجلات المسحوبة ضوئياً أو المنشأة رقمياً، بما يتيح التحقق من سلامتها عبر عقود طويلة. ويقارن المقال ممارسات الحفظ الورقي والرقمي، ويشرح مشكلة تحويل الصيغ، والتجزئة الواعية بالمحتوى لملفات الفيديو، ومبدأ عمل سلاسل الكتل المعقدة بالإذن. ثم يناقش ثلاث مسائل برزت في ورشة عمل للمشروع: التعاون، واستمرارية التقنية، وجدواها داخل الأرشيفات، ويصف التطبيق المكتبي التجريبي والبيانات التي يكتبها. ويخلص إلى أن الأرشيف بوصفه مستودعاً للأدلة يحتاج إلى إثبات أصالة سجلاته وسلامتها بطريقة لا تقبل الطعن.

الكلمات المفتاحية: سلاسل الكتل، تقنية السجلات الموزعة، أصالة السجلات الأرشيفية، الحفظ الرقمي، الأرشيف الوطني البريطاني

مقدمة:

حُفظت السجلات منذ آلاف السنين، والطرق الحديثة لحفظ الأرشيفات الورقية مفهومة جيداً. وخلال العقدين الماضيين، شهد المجتمع تغيراً تقنياً سريعاً أدى إلى التقاط كميات هائلة من المعلومات وتخزينها على وسائط غير الورق. ومع أن الممارسات المتعلقة بالحفظ الرقمي قد تطورت خلال السنوات الخمس والعشرين الماضية، [1] فإن كثيراً منها يحاول محاكاة الممارسات الأرشيفية المصممة للمجموعات الورقية. وللتعامل مع التهديدات التي تشكلها التقنيات الجديدة على ديمومة تراثنا الرقمي، يجب أن تكون الأرشيفات أكثر استعداداً بكثير لتجريب التقنيات الجديدة. ويستكشف مشروع (ARCHANGEL) الإمكانيات التي تتيحها تقنية السجلات الموزعة (distributed ledger)

(technology, DLT)، المعروفة عمومًا باسم سلاسل الكتل، وكيف يمكنها معالجة التحديات المتعلقة بالثقة والسلامة والأصالة التي يطرحها حفظ المواد المنشأة رقميًا. وسنبدأ بوصف جوانب من حفظ الورق وما يناظرها من عمليات الحفظ الرقمي.

ممارسات الحفظ الورقي والرقمي:

تضم مخازن الأرشيف الوطني (The National Archives) نحو 200 كيلومتر من الرفوف تحمل ملايين الوثائق الورقية الأصلية. وتُحفظ هذه الوثائق في ظروف بيئية مضبوطة بدقة، مع ضبط محكم لدرجة الحرارة والرطوبة. وبالمثل، تُحفظ الوثائق الرقمية في ظروف مواتية للحفظ طويل الأمد، تقلل إلى أدنى حد من تدهور الأشرطة والأقراص الدوارة. أما ما تختلف فيه الوثائق الرقمية عن الورق فهو أنها ليست هي الأصل حقًا، إذ نُسخَت في مرحلة ما من عمرها من وسيط إلى آخر. ويصنع الأرشيف نسخًا احتياطية إضافية للحد من المخاطر في عملية الحفظ. وفي العصور الوسطى، كان النساخ يصنعون نسخًا من الوثائق، ولم يكن التحقق من أمانة النسخة ممكنًا إلا بقراءة متأنية للنسخة والأصل. أما في العالم الرقمي، فنستخدم أساليب نشأت في علم التشفير للتحقق آليًا من أنه لا يوجد بايت واحد في غير موضعه في الملف المنسوخ. فعندما يتسلم الأرشيف ملفًا، تُولّد قيمة تجزئة تشفيرية (cryptographic hash)، أو مجموع اختباري، للملف وتُخزّن في قاعدة بيانات. وتُعاد حسابات قيم تجزئة الملفات بانتظام وتُقارن بقاعدة البيانات لتحديد الملفات التالفة استباقيًا. وإذا اكتُشف تلف، أمكن استبدال الملف بنسخة احتياطية.

وعندما نأتي إلى تقديم ملف رقمي إلى مستخدم الأرشيف، يتاح خياران. فيمكنه تنزيل الملف بصيغته الأصلية، أو تنزيله بصيغة بديلة. ومن أسباب تقديم الخيار الثاني أن البرمجيات، مع مرور الوقت، تُستبدل بإصدارات حديثة وتتغير معها صيغ الملفات. فعلى سبيل المثال، كان (WordStar) معالج نصوص شائعًا جدًا في الثمانينيات، لكن لم يعد هناك إصدار منه يعمل على الحواسيب الحديثة، وإن كانت تتوافر برامج محاكاة (emulators) أنشأها هواة. ويمكن فتح ملف (WordStar) في إصدار حديث من (Microsoft Word) بعد تثبيت وظيفة إضافية للتحويل أولًا. وهذا يبقي الصيغة حية وقابلة للاستخدام في الوقت الحالي، لكن هل يمكننا أن نضمن أن هذه الملفات ستعرض على حاسوب عادي بعد 20 عامًا أو 50 عامًا؟ وحتى في هذه الحالة، فإن معالج النصوص الحديث لا يعرض الأصل بالضرورة عرضًا أمينًا. ومن أجل الحفظ طويل الأمد، ولراحة المستخدمين، قد يصنع الأرشيف نسخًا من ملفات (WordStar) هذه ثم يحولها إلى صيغة مفتوحة يُرجّح أن تظل مقروءة بعد عقود من الآن. وقد تُتخذ إجراءات مماثلة أيضًا مع صيغ مثل الفيديو عالي الدقة، فتُحوّل إلى صيغة مضغوطة لتقليل وقت التنزيل، وذلك أيضًا لراحة المستخدم.

غير أن تغيير الصيغ على هذا النحو يطرح مشكلة: فمن الناحية التشفيرية، يختلف الملف المحوّل عن الأصل، ومن ثم تفقد المقارنة المباشرة بالمجاميع الاختبارية جدواها. وقد استخدم مزودو البرمجيات المجاميع الاختبارية سنوات طويلة ليتيحوا للعملاء التحقق من أنهم ينزلون نسخة أصلية، ويمكن للأرشيف استخدامها للتحقق من الملفات المنشأة رقميًا بالطريقة نفسها. لكننا بتغيير الصيغة نقدّم ملفًا مختلفًا من الناحية التشفيرية عن الملف الذي أودع في الأصل. فكيف نضمن أنه لم يحدث للملف تلاعب متعمد في أثناء عملية التحويل؟ من الإجابات عن هذا السؤال تقديم النسخة الأصلية والنسخة المحوّلة معًا ليتمكن مقارنة إحداهما بالأخرى. لكن ذلك بلا شك يُبطل الغرض من النسخة المحوّلة التي، كما ذكر، قد تكون بصيغة أنسب. ثم إنه إن لم تتوافر برمجيات لعرض الأصل، فإن هذه المهمة تصبح مستحيلة. ومن الحلول الممكنة لهذه المعضلة تسجيل مصدر الملف المحوّل وأصله (provenance).

وتزويد المستخدم ببرنامج التحويل (الذي لا يعتمد على عرض الملف). ويمكننا تسجيل قيم التجزئة للأصل، ولالملف ذي الصيغة الجديدة، ولبرنامج التحويل، فنعلن للملأ عملية شفافة قابلة لإعادة الإنتاج يمكن التحقق منها تحققًا مستقلًا.

هذا حل واحد، لكن هل توجد طريقة لإثبات أن ملفين بصيغتين مختلفتين لا يزالان متطابقين دون مقارنتهما جنبًا إلى جنب؟ يحاول مشروعنا التصدي لهذا التحدي في ملفات الفيديو، إذ إن مقارنة مقطعي فيديو طويلين إطارًا إطارًا مهمة شاقة، فضلًا عن آلاف المقاطع. ويستخدم باحثون في مركز الرؤية الحاسوبية بجامعة سري (University of Surrey Computer Vision Centre) الشبكات العصبية العميقة (deep neural networks) لتوليد قيم تجزئة للفيديو واعية بالمحتوى (content-aware hashes). ولا تزال التقنية تجريبية، لكنها قادرة على إنشاء قيمة تجزئة لا تتغير بتغير الصيغة، بينما تتغير تغييرًا أكبر إذا جرى التلاعب بالملف بطرق أخرى، كحذف إطارات منه مثلاً. ويمنحنا هذا وسيلة للمقارنة الآلية بين ملفي فيديو بصيغتين مختلفتين، وتقديم ضمان بأنه لم يحدث شيء للمحتوى في أثناء عملية التحويل. ومن حالات الاستخدام الواضحة كشف الأفعال الخبيثة أو الاحتيالية التي تستهدف المواد المؤرشفة، لكن ثمة حالة استخدام أكثر اعتيادية وأرجح حدوثًا بكثير، هي كشف التلف في أثناء عملية التحويل؛ ومرة أخرى، فإن مسائل الحجم والموارد تجعل أداء هذه المهمة يدويًا أمرًا مستحيلًا.

وينشر سجل التدقيق القابل لإعادة الإنتاج (audit trail) وقيمة تجزئة الملفات الواعية بالمحتوى، ينبغي أن يكون ذلك كافيًا لإثبات أن محتوى الملفات لم يتأثر بحيازة الأرشيف لها. لكن هل هذا صحيح؟ هل يضمن الأرشيف حقًا، بنشره هذا الضمان على موقعه الإلكتروني وحده، أنه لم يعدل المحتوى الأصلي للملف؟ الإجابة المباشرة هي أن الأرشيف مؤسسة موثوقة ترعى سجلات الحكومة الوطنية منذ مئات السنين. غير أننا نعيش أزمنة مضطربة من الأخبار الزائفة ونظريات المؤامرة، في عصر «ما بعد الحقيقة» (post truth) الذي تتدنّى فيه ثقة الجمهور بالجهات الرسمية. [2] ويكاد يكون من المستحيل أيضًا الوثوق بالمحتوى الرقمي. فالتلاعب بوثيقة ورقية أو صورة مطبوعة دون ترك أثر يتطلب عمل شخص ذي خبرة كبيرة؛ أما تغيير صورة رقمية فلا يحتاج إلا إلى خمس دقائق مع (Photoshop). [3] ويمكن تحرير آلاف الوثائق النصية من سطر الأوامر في دقائق.

وقد نشأ في السنوات الأخيرة خطر أكبر في صورة تقنيات الذكاء الاصطناعي المولدة للمحتوى. فقد طوّر الباحثون بالفعل تقنية تستنسخ صوت الشخص بأمانة وتقرأ به أي نص مكتوب؛ والتزييف العميق (deep fakes) الذي استُخدم لإدراج وجوه المشاهير في مقاطع فيديو إباحية دون حاجة إلى أي خبرة؛ [4] والأشد إثارة للقلق أن منظمة (OpenAI) عرضت نموذج ذكاء اصطناعي جديدًا يسمى (GPT-2)، يكتب نصوصًا تحاكي محاكاة تامة أسلوب كتابة أي شخص إذا أعطي عينة قصيرة منه. وتُعد هذه التقنية الأخيرة خطيرة إلى حد أن مطوريها يرفضون إتاحتها حتى يفهموا آثارها فهمًا كاملًا. [5]

حل سلاسل الكتل:

وهنا نعتقد أن تقنية السجلات الموزعة يمكن أن تكون جزءًا من التصدي لهذا السيل من المحتوى الزائف المولّد حاسوبيًا. فقد طوّرت في الأصل لتمكين المعاملات المالية بين أطراف لا تقوم بينها ثقة مسبقة. وعند وصف هذه التقنية، من السهل الفرق في تفاصيلها التقنية، ولا سيما التشفير، لكن الأوضح أن ننظر إليها على أنها قاعدة بيانات ذات سمتين مهمتين: فهي سجل (ledger) لا يقبل تغيير المدخلات السابقة، وتُضاف إليه المدخلات الجديدة فقط (append only)؛ وهي موزعة، أي إن لدى كل طرف في الشبكة نسخة منها. وهذا يعني أنه عندما تضاف معلومات المصدر والأصل وقيمة تجزئة المحتوى المذكورة آنفًا إلى سلسلة الكتل، لا يمكن حذفها أو تحريرها.

فهني توفر تعزيزًا تقنيًا للثقة، لا حاجة إليه إلى أن تتآكل الثقة، وعندها يكون قد فات أوان تطبيقه بأثر رجعي. فالأرشيف قبل كل شيء مستودع للأدلة، لكن إذا لم يكن المحتوى موثوقًا حتى مع بقاء المؤسسة موثوقة، فإن الغرض منه يصبح موضع شك. وما نخزنه في السجل الموزع هو دليل الدليل؛ إذ يتألف من بصمات رقمية لتاريخ الأمة مولدة بالتشفير أو بغيره.

ونريد للأرشيف أن يكون قادرًا على إثبات أننا لم نعدّل السجلات التي أوتمتًا على رعايتها، بأكثر الطرق شفافية وثباتًا. وفي أعقاب عرض (OpenAI) لنموذج (GPT-2) وبعض التقنيات المماثلة الأخرى التي يمكن بها وضع كلمات على لسان أي شخصية عامة، بما في ذلك الصحفيون والسياسيون، قد توفر تقنية السجلات الموزعة طبقة من الحماية من التزييف. فيمكن حساب قيم تجزئة للمقالات والمقابلات والخطب ونحوها، وتوقعها رقميًا، وكتابتها في الوقت الفعلي في سلسلة كتل، بما يوفر سجلًا محتومًا زمنيًا غير قابل للتغيير يشهد على ما قيل. أما المحتوى المولّد حاسوبيًا الذي ينتجه فاعلون خبيثون فسيفتقر إلى سلسلة الأدلة هذه الموصلة إلى المصدر المزعوم لادعاءاتهم.

كيف تعمل:

المبدأ الذي تقوم عليه سلاسل الكتل هو أن إعادة كتابة السلسلة الرئيسة من السجلات كتابة خبيثة تتطلب شخصًا يسيطر على 51% على الأقل من القدرة الحاسوبية. وذلك لأن كل كتلة في السلسلة تتضمن رابطًا تشفيريًا بالكتلة السابقة. ومن ثم فإن إعادة كتابة معاملة في كتلة ما تتطلب إعادة حساب جميع الكتل اللاحقة. ولما كانت السلسلة تتقدم دائمًا إلى الأمام، فلا يستطيع اللاحق بها فعليًا إلا كيان يملك موارد حاسوبية تفوق ما لدى سائر المشاركين. وبديهي أنه كلما زاد عدد المشاركين، صعب على أي أحد أن يسيطر بهذه الطريقة. ويصدق هذا خصوصًا على شبكة (ARCHANGEL) التي تستخدم سلسلة كتل مقيدة بالإذن (permissioned blockchain)، أي إن جميع المشاركين يُدعون إلى الانضمام بصفتهم مؤسسات موثوقة في حد ذاتها. وهذا يعني أيضًا أن إخفاء الهوية (أو شبه إخفائها) المصهود في شبكات سلاسل الكتل النموذجية غير موجود، ومن ثم يمكن نسبة أي سلوك مريب إلى مشاركين بعينهم.

أسئلة حول سلاسل الكتل:

استكشفت ورشة عمل للمشروع عُقدت في مارس 2018 طائفة من الأسئلة حول التقنية واستخدامها على النحو الذي يتصوره المشروع. وقد منحنا الحاضرون من مجالات إدارة السجلات، والأرشيفات، والقانون، والأوساط الأكاديمية، وموردي أنظمة الحفظ الرقمي، رؤية ممتازة للمخاوف المختلفة والاستخدامات المحتملة لسلاسل الكتل. وبرزت ثلاثة مجالات رئيسة:

- التعاون
- استمرارية التقنية
- جدوى التقنية داخل الأرشيفات.

التعاون:

التعاون أساسي للقيمة التي تقدمها تقنية سلاسل الكتل. فنجاح سلسلة كتل (ARCHANGEL) يتوقف على الحاجة إلى عدد من المشاركين من أكبر عدد ممكن من المؤسسات المختلفة. فمن دون حد أدنى من المشاركين، نرى أنه سبعة على الأقل، تكون الثقة التي تولدها التقنية معرضة لخطر الضياع. وفي بيئة تشغيلية مستقبلية، نأمل أن نشرك مشاركين من خارج قطاع الأرشفة، مثل المؤسسات الإخبارية وغيرها من مجموعات الشفافية التي لا تقتصر على توفير رقابة خارجية، بل لها أيضًا مصلحة في ضمان المعاملات. ولا يمكن لسلسلة الكتل أن تبقى لتوفر الأدلة للمستخدمين إلا بالمحافظة على حد أدنى من المشاركين طوال عمرها. وهذا النهج الموزع في ضمان الثقة مثال آخر على الممارسة القديمة المتمثلة في اعتماد مؤسسات الذاكرة بعضها على بعض. فالقدرات الأرشيفية ظلت طويلًا موزعة ومشاركة من حيث المعرفة العملية، وتطوير الأدوات وصيانتها، والموارد الأرشيفية الرئيسية (مثل PRONOM) [7] و (LOCKSS) [8]. وبالنسبة إلى المؤسسات التي تحتفظ بأرشفات الويب، تتداخل المجموعات نفسها ويشارك المحتوى، إذ تزود الأرشيفات بعضها بعضًا بالمحتوى لسد الثغرات في مجموعاتها.

ولأن التحدي كبير، ولأن الأرشيفات صغيرة نسبيًا بوصفها مؤسسات، فإن هذا النهج هو مفتاح الفوز في سباق التسليح التقني بين الأرشيفات والأطراف التي تستخدم الأدوات لتزييف إرثنا الرقمي. وإذا نجح هذا النهج في الخدمات الموزعة، فمن المثير التفكير في ما يمكن توزيعه أيضًا في المستقبل.

استمرارية التقنية:

تقنية السجلات الموزعة تقنية جديدة نسبيًا، وهي حاليًا في ذروة دورة التوقعات المبالغ فيها لدى (Gartner) (Gartner hype cycle). [9] والتقنية تتقدم، لكنها أبعد ما تكون عن النضج، ويُرجَّح أن تمر بصعوبات النمو في السنوات المقبلة. ويُعد أول «تفرّع جذري» (hard fork) في (Ethereum) عام 2016 مثالًا جيدًا على تحديات التغيير التقني في نظام موزع. و(Ethereum) واحدة من عدد من المنصات التي تستخدم تقنية السجلات الموزعة، وقد اختيرت للمشروع لأنها من أيسر المنصات وصولًا لتنفيذ العقود الذكية (smart contracts)، وهي في جوهرها أجزاء من شيفرة حاسوبية قابلة للتنفيذ يمكنها أن تولّد نشاطًا تلقائيًا عند استيفاء شروط معينة، ككتابة كتلة في سلسلة الكتل عند التحقق من صحتها. وقد أسفر هذا التفرّع الجذري عن نسختين من منصة (Ethereum)، وأثار قرار الانقسام على هذا النحو خللاً كبيرًا في مجتمع (Ethereum). وبالنسبة إلى الأرشيف الوطني، فإن طول العمر أمر حاسم. وهذا يعني أن التقنية يجب أن تبقى عقودًا، لا سنوات فحسب، لتكون ذات فائدة أصلًا. فضلًا عن ذلك، لا ينبغي عدّ أي تقنية قائمة على التشفير آمنة على مدى زمني طويل، إذ تدوم أنظمة التشفير عادة نحو 20 عامًا قبل أن يُخترق أمنها. والحوسبة الكمومية (quantum computing) تلوح أيضًا في الأفق، وقد تجعل بعض خوارزميات التشفير الحالية متقدمة. ثم إن مصدر القلق ليس استمرارية التقنية وحدها، بل الشبكة الموزعة نفسها. فكما سبقت مناقشته، يعتمد نظام السجلات الموزعة على وجود مشاركين كثيرين. ومع ازدياد شعبية التقنية، سيكثر الموردون المتنافسون، فقد يرغب المشاركون في الانتقال إلى منصة مختلفة. وثمة عائق أولي، إذ لا فائدة من الانتقال منفردًا، لكن من الممكن أن تنقسم الشبكة إذا فصلت مجموعة كبيرة بما يكفي من المشاركين منصة مختلفة. ولحسن الحظ، ثمة جهود جارية لوضع معايير للتشغيل البيئي بين المنصات، قد تخفف من هذه المشكلة. [11]

جدوى التقنية داخل الأرشفات:

مناهج الحفظ الرقمي في طور التطور، وتتفاوت من أرشيف إلى آخر، إذ إن لكل منها أولويات مختلفة ومستويات أتمتة مختلفة. ولكي تكون سلسلة كتل (ARCHANGEL) مجدية، لا بد من إمكان دمج البرمجيات في تلك العمليات القائمة ومسارات العمل المؤتمتة، ففي كل نقطة يمكن أن يُجرى فيها تغيير على السجل، ينبغي إرسال المجموع الاختباري والبيانات الوصفية إلى سلسلة الكتل. ولن يوفر تسجيل المجاميع الاختبارية وغيرها من البيانات الوصفية في سلسلة الكتل المصدر والأصل اللذين يمكن للمستخدمين والأرشفيين الوثوق بهما إلا إذا أُجري في نقاط محددة سلفاً من العملية.

تطبيق سلسلة كتل (ARCHANGEL):

طوّر مشروع (ARCHANGEL) تطبيقاً مكتبياً تجريبياً (prototype desktop application) تطوع عدد من المؤسسات الأرشيفية لاختباره. وسيمكّن ذلك فريق المشروع من فهم كيفية ملائمة العمليات الأرشيفية المتنوعة لمؤسسات في أنحاء العالم تعمل بمستويات أتمتة مختلفة. وسيكشف أيضاً عن المسائل المتعلقة بتطبيق البرمجيات في بيئات تقنية مختلفة، وجدوى دمجها مع العمليات الأخرى، بما يتيح فهمًا أفضل لفوائد هذه التقنية التي لم تُستخدم في الأرشفات من قبل.

وللبحث في هذه الأسئلة وفهم كيفية استخدام سلاسل الكتل لإثبات أصالة السجلات، أنشأ مشروع (ARCHANGEL) بيئة اختبار خاصة على (Ethereum). وسيتيح ذلك للمشاركين الانضمام في سلسلة كتل مقيدة بالإذن. وسيستخدمون الشبكة لرفع بيانات وصفية عن سجلاتهم، والتحقق من صحة البيانات الوصفية التي ترفعها المؤسسات المشاركة الأخرى، والتمكن من البحث في النتائج وعرضها على سلسلة الكتل.

وعند تصميم التطبيق، كان على فريق المشروع أن يقرر البيانات التي سٌكتب في سلسلة كتل (ARCHANGEL). ولما كانت البيانات المكتوبة في سلسلة الكتل لا يمكن حذفها أو تعديلها، فإن الطبيعة الحساسة لبعض السجلات الأرشيفية تعني أن السجلات نفسها، بما في ذلك أسماء ملفاتهما في بعض الحالات، لا يمكن إتاحتها. ويعني ذلك أن التطبيق لا يكتب في سلسلة الكتل، إلى جانب المجاميع الاختبارية، إلا المعرّف الفريد للملف، وحجمه بالبايت، وصيغة الملف في صورة (PUID) (المعرّف الفريد في (PRONOM): (PRONOM Unique Identifier)).

الخاتمة:

تطرح البيئة الرقمية تحديات كثيرة أمام الممارسة الأرشيفية التقليدية. ففي مجال الحفظ، فإن نهج ضمان بقاء السجل الورقي الأصلي دون مساس تقريباً ما دام في عهدة الأرشيف يكاد يضمن ضياعه في حالة السجلات الرقمية. فمن دون تجديد وسائل التخزين، والفحص وإعادة الفحص بحثاً عن التغيرات على مستوى البايت، وإنشاء نسخ بصيغ مختلفة، ثمة خطر حقيقي من أن يضيع تراثنا الرقمي. وفضلاً عن ذلك، ومع أن الثقة بالمؤسسات الأرشيفية لا تزال مرتفعة، فإن السهولة التي يمكن بها تعديل الملفات الرقمية تعني أن الأرشفات لا يمكنها الاعتماد على سمعتها وحدها لضمان أصالة السجلات التي في عهدها.

قد يُحتج بأن سلاسل الكتل ربما تكون حلاً لمشكلة لم توجد بعد، لكن ثمة بالفعل خدمات متاحة توفر تخزيناً للسجلات الرقمية لا يمكن الكتابة فوقه أو حذفه مدة زمنية محددة سلفاً. [12] وسيُطعن في جدارة الأرشيفات بالثقة، وسيكون قد فات الأوان لإثبات حرصها في الحياة بتطبيق حل بعد سنوات من تسلم السجلات. والأرشيف، بوصفه مستودعاً للأدلة وركيزة مهمة من ركائز الديمقراطية، يحتاج إلى أن يكون قادراً على إثبات أصالة السجلات التي يحتفظ بها وسلامتها بطريقة لا تقبل الطعن.

وثمة مزيد من الدروس التي ينبغي تعلمها، وسيواصل مشروع (ARCHANGEL) استكشاف جدوى شبكة سلاسل الكتل وتحدياتها وفرصها، من خلال شبكة (Ethereum) التجريبية والمؤسسات المشاركة من أنحاء العالم.

المراجع:

- Transparency International. <https://www.transparency.org.uk/> (accessed 20 May 2019).
- 1. "The technical registry, PRONOM," The National Archives, <http://www.nationalarchives.gov.uk/PRONOM/Default.aspx> (accessed 15 May 2019).
- 2. "Gartner Hype Cycle," Gartner, <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle> (accessed 15 May 2019).
- 3. "Amazon S3 Object Lock Overview," AWS, <https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock-overview.html> (accessed 15 May 2019).
- 4. John D. Garrett et al., "Preserving digital information: Report of the task force on archiving of digital information," (PDF). Commission on Preservation and Access and the Research Libraries Group (1996), <https://archive.org/details/PreservingDigitalInformationTaskForceReport1996> (accessed 15 May 2019).
- 5. Louella-Mae Eleftheriou-Smith, "Donald Trump says interview with The Sun criticising Theresa May is 'fake news' even though it was recorded," i, July 13, 2018, <https://inews.co.uk/news/politics/donald-trump-the-sun-theresa-may-fake-news/> (accessed 15 May 2019).
- 6. John Swain, "Trump inauguration crowd photos were edited after he intervened," The Guardian, September 6, 2018, <https://www.theguardian.com/world/2018/sep/06/donald-trump-inauguration-crowd-size-photos-edited> (accessed 15 May 2019).
- 7. Stephen Maher, "Fake video is a big problem. In 2019, it gets worse," MSN, December 28, 2018, <https://www.msn.com/en-ca/money/topstories/fake-video-is-a-big-problem-in-2019-it-gets-worse/ar-BBRwxZ4> (accessed 15 May 2019).
- 8. Alex Hearn, "New AI fake text generator may be too dangerous to release, say creators", The Guardian, February 14, 2019, <https://www.theguardian.com/technology/2019/feb/14/elon-musk-backed-ai-writes-convincing-news-fiction> (accessed 15 May 2019).

9. The LOCKSS Program, <https://www.lockss.org/> (accessed 15 May 2019).
10. A working group on the Interoperability of blockchain and distributed ledger technology systems (ISO/TC 307/SG 7) has been set up, <https://www.iso.org/committee/6266604.html> (accessed 15 May 2019).