Title: Using Blockchain to Engender Trust in Public Digital Archives

Authors:
A Green, M Bell and J Sheridan: The National Archives (TNA), UK
J Collomosse, T Bui and A Brown: University of Surrey, UK
J Fawcett, O Thereaux, J Tennison: Open Data Institute (ODI), UK

Abstract
Archives are special – the homes of our collective memories. Although the archive is still widely perceived as a trusted custodian, archivists are aware that they are working in a world in which digital content is increasingly questioned. Is the archive trusted because of its people and practices or because of the sheer practical impossibility of altering or manipulating kilometres of physical records? What is the digital equivalent? The emerging challenge around trust is particularly relevant in relation to public archives preserving records of contentious histories; terms such as “fake news” and “post-truth” are frequently heard in the context of national and international politics. How do we ensure that researchers continue to trust that the records have not been tampered with, or that a document can be verified as being the same as the archived original?

The ARCHANGEL project is breaking new ground by using blockchain to record checksums and other metadata derived from either scanned physical records or born-digital records to allow verification of their integrity over decade- or century- long timespans. This data is permanently preserved through peer-to-peer distribution and consensus checking without the need for a trusted third party.

Conference Theme: Sustainable digital preservation approach and communities

Keywords: Distributed Ledger Technology (DLT), Blockchain, Trusted Archives, Document Provenance, Content Integrity and Verification

Introduction
Society needs archives to be trusted. Archivists expect to be viewed as objective custodians of the authentic record, the immutability and integrity of the records in our care, unquestioned. However, the digital age challenges this assumption. The nature of digital records means that they can be easily altered and instantly disseminated. The public are rightly less trusting of digital content in the era of fake news. While paper records may be altered, it is difficult to achieve without leaving a trace and almost impossible to do in bulk, but updating hundreds of digital documents can be the work of minutes, and achieved without leaving any obvious trace. Over the last few years it has become increasingly simple to manipulate digital content to create fake documents, photographs, audio recordings [1] and now videos. At the end of 2017, the ability to edit videos and their audio streams became widely available when the faces of adult actors were replaced with those of celebrities. [2] Opportunities for the creation and instant dissemination of “evidence” for fake news stories are now available to all.

On a less chilling note, but equally as threatening, are the changes that result from the degradation of digital objects over long periods as file formats become obsolete and content is migrated to more modern formats. This is a legitimate alteration of the digital object; part of standard archival practice and most archives would keep the original format. Nevertheless, how does a researcher prove to herself that what she received is an exact copy of what the archive holds or an authentic version of it?

The ARCHANGEL project proposes using Distributed Ledger Technology (DLT), more commonly known as blockchain, to verify the integrity and provenance of digital records

during the process of preserving the records (curation) and upon release (presentation). A word of caution is appropriate before we discuss the uses of the technology in archives: blockchain is a very new technology and is currently at the zenith of the "Gartner hype cycle". [3] We should expect to see some "growing pains" before it could be considered part of a long-term preservation infrastructure.

Outline of blockchain technology

ARCHANGEL is exploring the archival use of blockchain, a distributed, append only, ledger, best known as the technology behind cryptocurrencies such as Bitcoin although it has been investigated in the records management domain. [4, 5, 6, 7] There are various architectural approaches to blockchain and a number of technological implementations. [8, 9]. As with all new technologies, there is always the danger inherent in being an early adopter: parallel blockchain infrastructures are emerging and there is a danger that our choice of the Ethereum platform is not ultimately the one that prevails. It is also worth noting that with new technologies, there are the "unknown unknowns" and we can only wait to see them emerge as the technology matures.

Rather than attempt to explain the details of how the technology works, we will instead introduce two key features of a blockchain-based system, which are the most relevant and important for archives. Firstly it is a peer-to-peer distributed system contributed to by several (or thousands of) participants. Each participant is involved in the verification and acceptance of the data stored within the system. There are several approaches to achieving consensus [10] on which records to accept, varying according to whether the system is permissioned or un-permissioned. ARCHANGEL is considering a permissioned access model. This means that only invited participants have write access to the data. In general, a malicious actor would need to take control in some way of at least 51% of the participants of the system in order to corrupt the data and this is one of the most frequent criticisms of blockchain. In the case of ARCHANGEL however, the risk of this consolidation of computer power is mitigated by a permissioned ledger. This means that contributors are known (so not anonymous), and if 51% of them colluded to commit fraud by changing the blocks, that activity and the partners responsible would be identified by all the remaining partners. Without the distribution of the blockchain, the owner of the database could just start again without anyone else being aware that something had changed and there would be no trace of what was available before.

The second feature of blockchain is immutability, partly a result of the distributed nature just discussed but primarily thanks to cryptography. This immutability is one of blockchain's strengths but also one of its weaknesses in the sense that anything put on the blockchain can never be removed or changed. This has serious ramifications for privacy and security, which need to be considered before anything is written to this technology. The name blockchain comes from the fact that transactions, or records, are packaged together in blocks (for example, all transactions occurring in a specific time period go into one block), which are chained together chronologically. The contents of a new block are verified and if the majority of participants agree, this block is stored in the system and considered the latest block in the chain. The cryptography comes in at this point. Each new block has a checksum calculated for it but before this is done, the checksum of the previous block is added to the new block. This means that in order to change the contents of a block (thus generating a new checksum) one would also need to update the subsequent blocks in the chain. As we have already mentioned, this would be impossible to achieve without collusion with 51% of the other participants, and due to the distributed nature, it would be done in plain sight of the other 49%.

These two features provide the technological underscoring of trust since once a record's checksum and metadata is written to a blockchain, it is practically impossible to change or remove that record. If the digital record is tampered with, the checksum will change and when compared to the archived copy a user can verify that it has been altered. This of course presents some challenges of its own since this is not a feature we are used to in current systems and we have to think hard about what data we are willing to write to a system that is copied many times, can be potentially publically viewable, and where errors cannot be overwritten. These give us reasons to be cautious. At the IRMS 2018 conference, Heyward-Mills highlighted the incompatibility of blockchain with GDPR and the right to be forgotten. [11] This issue was also raised when presenting our project at "The Future of Blockchain Technology" Mini-Conference. [12]

In the case of the ARCHANGEL system therefore, we will store the minimal amount of data required to aid verification and searchability of digital objects, given the aforementioned public and immutable nature of the data storage. The primary piece of information for verification is the checksum of a digital object.

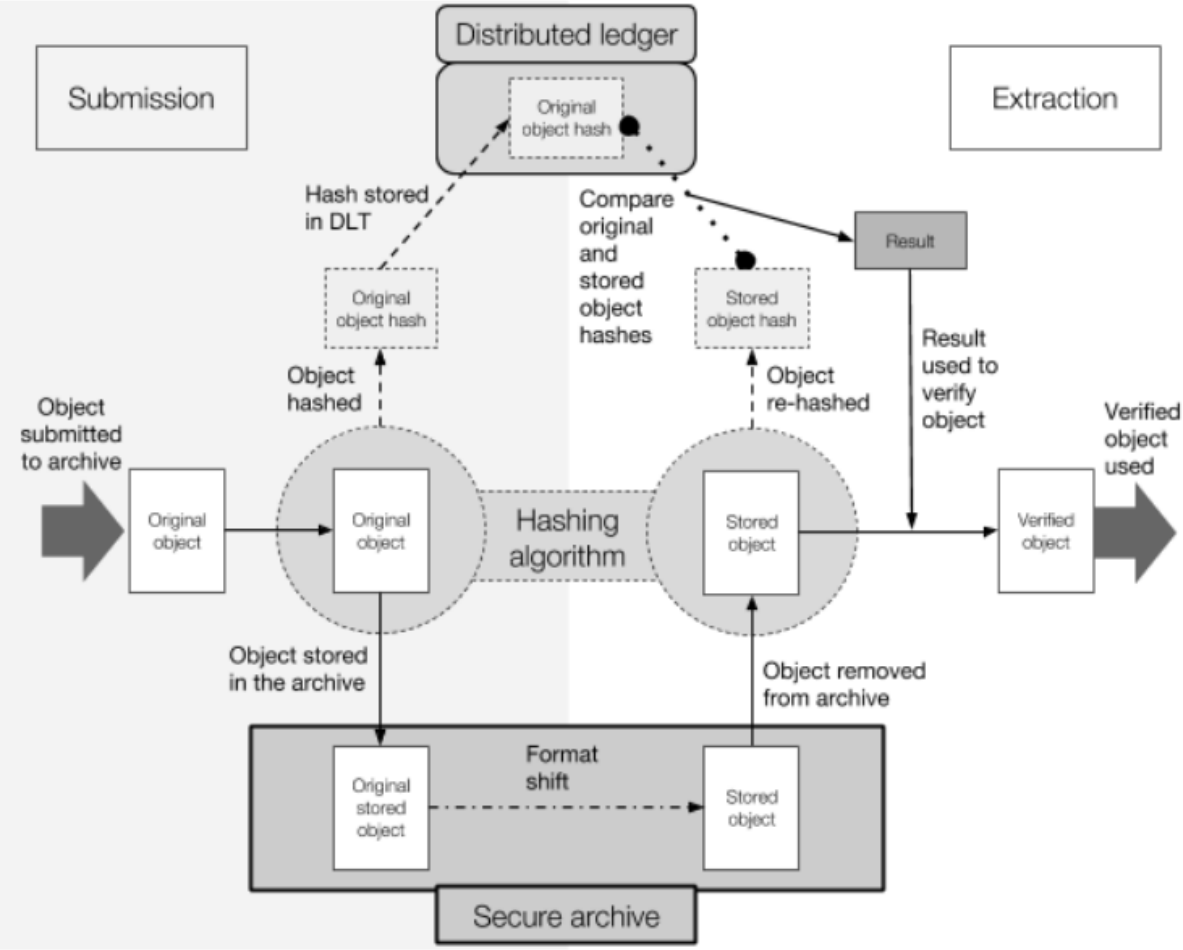

Figure 1. Architecture of the proposed ARCHANGEL platform. Records are processed to extract content evidence, which is stored immutably within a blockchain alongside metadata identifying both that content, and the algorithm used to extract the evidence. A record's integrity and provenance can be checked at any time by re-extracting and comparing the content evidence to that in the blockchain.

We asked ourselves, from what object we should derive the checksum for inclusion in the blockchain? In common with many other digital archives, The National Archives has an OAIS [13] type repository and as such we use the information packages described in the reference model, i.e. Submission Information Packages (SIPs), Archival Information Packages (AIPs) and Dissemination Information Packages (DIPs). However, as the purpose of the project

was to enable researchers to check that the record they received was the one deposited in the archive, the OAIS information packages did not help us: the file in the AIP (considered the archived record) might have a different checksum to the file in the DIP that was delivered to the user. There will be a sound reason for this difference: possibly the latter was a presentation copy of a different format produced for ease of rendering (for example an MXF video file converted to MPG4 to reduce the size of the download). Alternatively, the file had been migrated to a modern format as the archived format is now at risk of obsolescence (for example WordPerfect may be migrated to Open Document format). This would therefore not demonstrate to the researcher that the two records were identical.

In light of this, we think the next phase of the project, which addresses the possibilities of hashing content rather than the object, may be of particular use. A content hash of an image or video looks like a cryptographic hash: a long stream of digits. However, unlike a cryptographic hash where changing a single pixel would result in an entirely different hash value, a small change in the object will result in a small change in the content hash. A format shift should in theory result in a content hash that is identical or very similar to the original hash.

Removing frames from a video, or a person from an image, however, would be instantly detectable as the content hash would be distinctly different. This technique provides the possibility of detecting fraud in visual content while still allowing for the manipulation of the digital objects themselves for preservation or presentation purposes. It also guards against faulty transcoding on the part of the software, for example, where content is truncated or chunks dropped during transcoding due to malformed content or invalid formats, thereby helping the archivist ensure that any migration of format has completed successfully.

How blockchain engenders trust [14]

Enables archives to be defenders of the record

In an era when the technologies to alter digital content are becoming increasingly pervasive, it is not surprising that the public has less trust in all things digital. Blockchain offers a shield that archives can use to defend the records as authentic. By enabling researchers to compare the checksum and identifying metadata of the record to that recorded on the blockchain, they can see proof that no changes (deliberate or accidental) have been made to the record since it was preserved in the archive. This method provides the researcher with proof that the record can be trusted as evidence sourced from the archive. ARCHANGEL enables a shift from an institutional underscoring of trust to a technological one.

Demonstrates archives' willingness to be transparent in their practices

As archives work to preserve the massive amount of digital material generated by public bodies, they are careful to ensure that the record and its metadata are not (unknowingly) altered and to record any actions taken to provide an audit trail of the work of curation and preparation for presentation.

We are investigating how archivists would use the technology throughout their processing of the records. Each curatorial action would generate an entry on an audit trail, which not only records evidence of the digital objects their actions created, but also the checksums of the technology used to perform those actions. The archive can always make available the original object but often the presentation copy is in a different format to aid access. As long as it is technologically practical, a user could reproduce the process used to generate the presentation copy. An object such as a video, however, will most likely have been through the same reformatting process as thousands of others. If that process is trusted, perhaps through independent verification, then users of the archive could have more trust in the

presentation copy. By making a transparent audit trail available, it also encourages trust in archives' role as custodians, while demonstrating their use of best practice. It is clear that blockchain would need to be integrated in an automated way with the work of digital archivists to be of practical use. Only by embedding the technology into the workflow, ideally as part of preservation systems, could the technology be used in a way that engenders trust.

Demonstrates archives' engagement with emerging technologies

Archives are not generally viewed as digital institutions nor as a digital profession. The National Archives is committed to becoming a digital archive by instinct and design, leading work to change how people think about archives. There are many areas where archives are actively engaged with digital technology, from the preservation of born-digital records to researching the uses of machine learning for appraisal, selection and access. Involvement in the practical application of blockchain clearly demonstrates archives' interest in and openness to the possibilities of new technologies. In March this year the project team held a workshop with attendees drawn from government, commercial legal and university research document management areas. For many it provided their first exposure to this new technology, and all were keen to remain involved in the project and willing to test further iterations of the platform prototype.

Demonstrates the collaborative nature of the digital archives community

A major benefit for the archival community (and other heritage organisations) of using blockchain technology, is that as a decentralised platform, collaboration is fundamental to its success. To be an operational permissioned blockchain we feel at least seven archives would need to form a consortium to ensure that a majority of contributors reached consensus on the content of a block. Only then can the blockchain guarantee that the record has not been tampered with to the satisfaction of the public. This requirement is key: without other organisations taking part, the technology gives us no more surety than a centralised database. While key to the trustworthiness of the archival blockchain, there is a risk that if one institution (and then another…) decided to leave, perhaps to use a different blockchain technology with other partners, the credibility of our blockchain is undermined. A blockchain is reliant on a sufficient number of partners taking part to ensure both the longevity and trustworthiness of the ledger, without these, it could not be considered a reliable source of validation. Partners are key!

Given the computational power and the associated costs currently required to operate a blockchain, the archives (or other public bodies) are initially likely to be national institutions. Incentives for participation will therefore need to be strong to encourage collaboration at this level but would have the added benefit of ensuring that no individual country could attempt to alter the records.

Archives have an excellent track record of supporting each other and collaboration is key to the success of digital preservation approaches, the OAIS reference model being the best example of this. Although the model covers interaction between archives and briefly refers to federated and cooperating archives, in practice digital archives are generally single, independent repositories. Reconciling OAIS with blockchain's distributed approach would go some way towards developing a more collaborative and resilient archival network, providing new ways for archives to manage their key risks.

In presenting this project at two events [15] and attending another [16] we heard a mixture of views expressed: there is certainly confusion about how the technology works and what it does, and a feeling in some areas that the huge amounts of paper records still to be tackled are the priority. There is also healthy scepticism about its use in archives, but also curiosity and excitement about the potential of the technology for the profession.

Conclusion and Next Steps

ARCHANGEL is currently a fully functional prototype in line with Phase 1 of the project. In the rest of the project, we plan to supplement the checksum algorithm from SHA-256 with content-aware hashing for video files. This will allow us to explore making checksums that are sensitive to tampering or degradation but not to less destructive alterations such as changes to the codec or the video's brightness. In addition we are exploring the possibility of using the W3C proposed PROV standard [17] to allow verification of different versions of a record created by both preservation and presentation actions (for example when migrated to a different format) so the changes can still be traced back to the original archived record.

A Distributed Ledger is nothing without multiple participants, so the project is actively recruiting other archives to join a prototype DLT system. There are further opportunities to explore and we feel that ARCHANGEL could be used to ensure the future sustainability and proper stewarding of archives in this era of digital transformation.

Archives now operate in a world where digital content is not as trusted as the paper records they hold. The ARCHANGEL project uses blockchain to record the checksums of objects, which can then be used in the future to verify the authenticity of those digital objects. The technology ensures these records are immutable and allows archives to be transparent in their practices by publishing to a distributed, publically viewable, data store. By publishing not only checksums of files but also of computational functions, they can make available a reproducible audit trail of the archival processes which generated a digital object, thereby mitigating against the file transformations which may occur during long term preservation. The public can gain reassurance that archives are not only following best practice but that by engaging with emerging technologies they can address societal concerns about the authenticity of digital records. In this way, ARCHANGEL engenders trust in the records and their custodians.

Acknowledgements:

ARCHANGEL is funded by EPSRC Grant Ref: EP/P03151X/1 under the UKRI Digital Economy Programme.

References:

[1] Bob Yirka. 2018. Upgraded Deep Voice can mimic any voice in mere seconds. (March 6 2018). Retrieved April 10, 2018 from https://techxplore.com/news/2018-03-deep-voice-mimic-mere-seconds.html

[2] Sean Rameswaram. 2018. The Deep Fake from Today, Explained. Retrieved April 10, 2018 from http://www.stitcher.com/s?eid=53531939

[3] Retrieved June 8 2018 from https://en.wikipedia.org/wiki/Hype_cycle

[4] Victoria Lemieux. 2016. Trusting records: is Blockchain technology the answer?, *Records Management Journal*, Vol. 26 Issue: 2, 110-139, DOI: https://doi.org/10.1108/RMJ-12-2015-0042

[5] Victoria Lemieux. 2016. Blockchain for Recordkeeping; Help or Hype? Retrieved April 10, 2018 from https://www.researchgate.net/publication/309414276_Blockchain_for_Recordkeeping_Help_or_Hype. DOI: 10.13140/RG.2.2.28447.56488

[6] InterPARES Trust Project: Hrvoje Stančić et al. 2018. Model for Preservation of Trustworthiness of the Digitally Signed, Timestamped and/or Sealed Digital Records (TRUSTER Preservation Model). Retrieved April 10 2018 from https://interparestrust.org/assets/public/dissemination/TRUSTERPreservationModel%28EU31%29-Finalreportv.1_.2_.pdf

[7] Rob Begley. 2017. Information & Records Management and Blockchain Technology: Understanding its Potential. Unpublished Masters dissertation. Northumbria University, Newcastle. Survey was available from https://www.linkedin.com/pulse/survey-blockchain-technology-information-records-robert-begley/
[8] Satoshi Nakamoto. 2017. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved April 13 2018 from https://bitcoin.org/bitcoin.pdf.
[9] Ethereum. 2018. Retrieved April 13 2018 from https://www.ethereum.org/
[10] Amy Castor. 2018. A (Short) Guide to Blockchain Consensus Protocols. (March 4 2017). Retrieved April 10 2018 from https://www.coindesk.com/short-guide-blockchain-consensus-protocols/
[11] IRMS conference held in May 2018 in Brighton, England
[12] Retrieved June 12 2018 from https://blockchainubc.ca/2018/05/04/blockchain-101-next-to-the-blockathon-for-social-good/
[13] Technical Committee: ISO/TC 20/SC 13. 2012. Space data and information transfer systems - Open archival information system (OAIS) - Reference model ISO 14721:2012 (CCSDS 650.0-P-1.1)
[14] John Collomosse et al. 2018. ARCHANGEL: Trusted Archives of Digital Public Documents. Retrieved June 8 2018 from https://arxiv.org/abs/1804.08342
[15] Memory, Identity and Trust Conference in Dundee, Scotland retrieved June 8 2018 from https://www.dundee.ac.uk/cais/conference/memoryidentityandtrust2018/ and “The Future of Blockchain Technology” Mini-Conference in Vancouver, Canada retrieved June 8 2018 from https://blockchainubc.ca/event/the-future-of-blockchain-and-talentinnovation-showcase/
[16] IRMS conference held in May 2018 in Brighton, England

[17] W3C. 2013. An Overview of the PROV Family of Documents. Retrieved April 10 2018 from https://www.w3.org/TR/prov-overview