Information security in archival science

Teodora Licheva
New Bulgarian University
Sofia, Bulgaria
teodora_licheffa@abv.bg

Abstract: *The article with the title "Information security in archival science" focuses on the need for the state archives system to be able to meet the modern needs of archival information users, individuals and legal entities. Modernization and updating of archives cannot happen without using the new technological possibilities. At the same time, a challenge of the modern society of rapidly developing and changing information technologies is to what extent can digital information be trusted? Archival institutions have the opportunity to participate in the creation of the so-called a new architecture of security, trust and reliability.*
The article is divided into an introduction, presented a model of the development and implementation of blockchain technology in the National Archives of South Korea, conclusion and literature.
Keywords*: BLOCKCHAIN, INFORMATION SECURITY, ARCHIVE*

1. Introduction

Blockchain is an innovative database technology. It is a digital ledger and the information is distributed in a "chain of blocks".

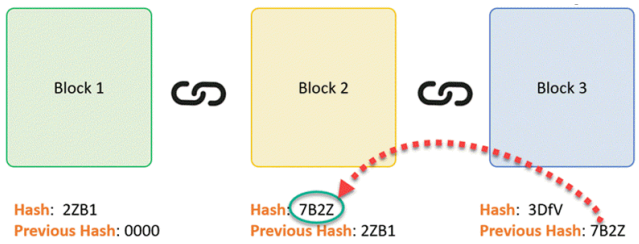

Fig.1 *Blockchain technology*[1]

The blockchain system consists of the following elements:

1. Information that is stored in a block;

2. Hash. This binding element is unique and is passed on to the next block. There is a role of fingerprint;

3. The hash of a previous block is the last piece in a blockchain.

Blockchain is a data storage platform that, once stored, cannot be changed. This function is achieved by distributing authority and monitoring by all participating members in the system, rather than using centralized control.

The inherent property of blockchain decentralization meets the most important value in record management and is neutral to all external forces. Blockchain platforms are an extremely attractive technology in the field of record and archive management.

Data authenticity and integrity are essential attributes of records and archives management. Integrity is a necessary condition for maintaining authenticity. And although there are many practical constraints (e.g. budget, technology and time), it is necessary for national archive and archival institutions to apply blockchain to their management systems and create a long-term plan to achieve such application.

In this article, I will focus on the results of a research project of the National Archives of South Korea, which was conducted from 2019 to 2021.[2]

2. Presentation of blockchain technology from the point of view of information security

Thanks to the Korean government's policy of investing in digital transformation, NAK Blockchain has developed the NAK document storage platform for research and development (R&D).[3]

In 2019, NAK developed a blockchain recording platform using a hyperledger[4] system. As early as the following year, R&D was conducted to implement archival practices for recording and storing documents using the platform. In 2021, research continues to verify the integrity of input data from the multiple government administration systems in South Korea.

To understand the rationale behind the introduction of blockchain technology, we must first understand the digital environment of the Korean government[5]. In 2001, the Korean government passed the E-Government Act and began to electronically convert paper-based government activities. Various types of paper documents such as government taxes, criminal justice records, social security and financial documents have been digitized and a number of information systems have been created for their use and management[6]. Since the early 2000s, the Korean government has provided a significant budget to create various business systems to convert large amounts of paper records into digital versions.

Thanks to these investments, there are now more than 16,000 information systems used by government administrations and institutions involved in the digitization of paper records. The types and number of electronic records through these systems are growing significantly. NAK archivists, who are responsible for the preservation of public records, face increasing difficulties in ensuring the authenticity of these new types of records with traditional records management methods. This is the main reason why NAK employees are looking for a solution and are interested in innovative technologies, including blockchain technology.

It is the responsibility and obligation of archival institutions to maintain authenticity and deliver unaltered documents to future generations, regardless of the type of public record. Durability is the minimum requirement for all electronically created records to maintain authenticity from creation to end of life. In particular, the bitstream[7] of the records must not be changed, except in cases where it is determined that it is no longer possible to maintain the current state of the records and they must be properly converted to another format.

Extremely rare are cases that involve changes in the storage format due to a change in record-keeping policy, a change in the method of providing information, a change in the information itself if there is a change in the method of authentication, and other factors.

NAK adopts a long-term storage strategy that combines migration and encapsulation to ensure the authenticity of digital documents, their security and non-tampering. The storage strategy aims to convert digital record objects into PDF and encapsulate them by adding electronic signatures as well as recording metadata. NAK refers to these encapsulated objects as NAK Encapsulated Objects (NEOs)[8]. Converting most types of electronic documents to NEO is usually not difficult, but converting large objects, such as audiovisual recordings, and a number of objects such as data sets in information systems, is actually not easy at all. Thus, NAK was unable to apply authentication strategies, such as NEO, to audiovisual recordings or datasets.

In 2020, NAK decided to use blockchain audit trail technology[9] to solve the authenticity problem of audiovisual recordings. In this way, the security of the network and information resource is guaranteed. Next year, National Archives officials are auditing measures to ensure the integrity of documents, using blockchain auditing technology to monitor transactions in the data sets created in these systems. Based on this solution, NAK promotes R&D projects that have developed a blockchain system for audiovisual records and an authenticity dataset.

The organization of the National Archives of South Korea to use blockchain technology consists of two phases of research and development. In the first case, the use of blockchain transaction auditing technology to ensure the authenticity, authenticity and reliability of audiovisual archives. The second case is the use of blockchain technology to verify that the data sets of multiple information systems built by government institutions are managed without falsification or manipulation.

In addition to existing electronic documents, the former offers a method of maintaining authenticity suitable for a new type of record called an audiovisual record, and the latter datasets. In addition to the fact that each R&D case deals with a different type of record, the location and environment in which each record physically exists should also be noted. Audiovisual records are transferred and managed by the Central Archives Management System (CAMS) and Multimedia Asset Management (MAM), which are managed by NAK. In contrast, datasets are managed in two main ways according to record evaluation. The first is a method of transferring records to NAK, such as audiovisual records, and the second is a method of self-management of records by the institution that creates them. When the data sets are transferred to the NAK, a newly designed and built system can manage them without considering the system before the transfer. Therefore, this study focuses on self-administered datasets. In the NAK transfer method, a new system can be designed and built freely. However, in the method of self-management from the source institution without transfer to NAK, there is a limitation that it should not affect the information system, including the current data sets, and it should be applicable to different information systems[10].

2.1. Applied concept

The ISO 15489[11] standard establishes the basic concepts and principles of records management. According to ISO 15489, records must maintain the characteristics of authenticity, integrity, reliability and usability throughout the management process. To demonstrate that these four characteristics are preserved in records management processes, the metadata that is used in records is managed along with the records themselves[12]. Dr. V. Memljo[13] distinguishes three separate stages in the development process of the concept of recording archives in the blockchain. In the first stage, the integrity of the authentic records is ensured by separately establishing a blockchain platform as a cryptographic mirror system to the records preserved within the existing information system currently in use. In the second stage, tasks are performed together with record management within a system by developing and implementing the new work system itself as a blockchain platform. In the final stage, tokens ensure the integrity of non-electronic records by attaching to the records and tracking the specific tokens that can be recognized by the blockchain platform[14].

NAK currently creates and manages audiovisual records in three distinct formats – original, copy for use and preservation, and the MAM system.

A blockchain system has been developed for the authenticity of audiovisual recordings.

The hyperledger variant of the blockchain system and the prototype code are used to verify the authenticity of the records[15]. This code is provided only if the request is approved and authorization is required when disclosing inside information.

2.2. Authenticity check

Archives should be able to provide part of a whole record and in different formats, depending on the needs of the users as well as the service policy. Audiovisual records can also be changed in different formats according to the needs of users of archive information, and blockchain should be able to verify and track all change transactions and provide authentic verification services.

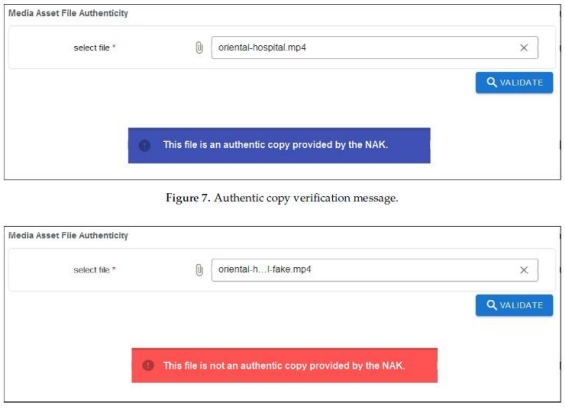

Figure 7. Authentic copy verification message.

Fig.2 *The interface of a developed authentication service*

2.3. Execution

To test the effectiveness of the proposed model, NAK staff are using Loopchain[16] as a blockchain platform[17], with prototype code available online[18].

It is difficult to introduce a public blockchain into the public domain due to the presence of confidential or private information that should not be exposed to the public sector and needs to be protected from detractors. For this reason, private blockchain is suitable for public administration, involving several participating institutions or authorized groups of administrations with similar activities. The larger number of participating nodes provides more security and stability, and the participation of private blockchain nodes should be increased by establishing the control of government administrative organizations, such as close cooperation.

3. Conclusion

Administrative information systems in South Korea were established after the enactment of the E-Government Act in 2001, and the e-Government Support Project was promoted. This document proposes a method for verifying the integrity of administrative datasets. When administrative information systems were first created, there was no blockchain technology and therefore this system was not set. For different types of DBMS, a method for checking integrity should be offered in a consistent and unified manner. It is best to adopt a mirror system method with a small amount of integrity information and metadata such as hash values for real datasets.

With the advent of blockchain technologies and the creation of an administrative information system in the future, it must be designed to store data sets on the blockchain. The transaction of creating, reading, updating and deleting in the database should not reflect the actual data by blocking with the blockchain through a smart contract, but should put the end goal in the direction where the actual data itself is stored in the blockchain.

4. Literature

1. ISO 15489-1. Information and documentation-records management part 1. In Concepts and Principles; ISO: Geneva, Swiss, 2016; pp. 4–6

2. Jung, C.-S. The Theory of Electronic Government, 1st ed.; Seoul Economic Management Publishing Company: Seoul, Korea, 2007; pp. 99–128

3. Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]

4. National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017

5. Wang, H.; Yang, D. Research and Development of Blockchain Recordkeeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090

6. https://www.guru99.com/blockchain-tutorial.html#1

[1] https://www.guru99.com/blockchain-tutorial.html#1
[2] Wang, H.; Yang, D. Research and Development of Blockchain Record-keeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090
[3] Research and development and developments in science
[4] An open source blockchain platform and collaborative approach to distributed ledgers. By developing standards and a comprehensive blockchain framework, Hyperledger has received support from organizations including Cisco, American Express and IBM. https://www.hyperledger.org/
[5] Wang, H.; Yang, D. Research and Development of Blockchain Recordkeeping at the National Archives of Korea. Computers 2021, 10, 90. https:// doi.org/10.3390/computers10080090
[6] Jung, C.-S. The Theory of Electronic Government, 1st ed.; Seoul Economic Management Publishing Company: Seoul, Korea, 2007; pp. 99–128.
[7] Binary sequence, bit stream. A sequence of bytes.
[8] National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017.
[9] The so-called audit trail. A series of computer event records for an operating system, application, or user activities. It is an analysis of managerial, operational and technical control.
[10] National Archives of Korea. Technical Specification for Long-Term Preservation Format ver. 2.1. Standard; NAK 31:2017(v2.1); NAK: Daejeon, Korea, 2017.
[11] Records Management Standard.
[12] ISO 15489-1. Information and documentation-records management part 1. In Concepts and Principles; ISO: Geneva, Swiss, 2016; pp. 4–6.
[13] Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]
[14] Lemieux, V.L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 2271–2278. [CrossRef]
[15] NAK-DLT. Available online: https://github.com/Hosung-wang/NAK-DLT (accessed on 12 July 2021).
[16] An enterprise blockchain platform where only identified users can participate in the network.
[17] LOOPCHAIN. Available online: https://www.iconloop.com/en/loopchain (accessed on 21 July 2021).
[18] Prototype for Verifying Integrity of Dataset using Blockchain. Available online: https://github.com/likeba/VID (accessed on 21 July 2021).