Armanesia Blockchain System: Blockchain and IFPS-Based Archive System Prototype

Taufik Asmiyanto[1], Navi Putrawan[2], Yusuf Widiarta[3], Hanif Inamullah[4], & Zaidan A. Qois[5]

[1,4]Library and Information Science Department, Universitas Indonesia
[2,3,5]Armanesia.com

Correspondence email: tasmiy@ui.ac.id

DOI: 10.24252/kah/v10i2a9

(Submitted: 13-05-2022, Revised: 20-11-2022, Accepted: 20-12-2022)

ABSTRACT

Document integrity is critical to public trust in archives management. Armanesia is an innovative research project aims to develop prototype of information systems to support the management of digital archives based on blockchain technology. The project uses blockchain technology to record verification, immutability, and other metadata derived from various types of digital records. In this system, archives are permanently stored through peer-to-peer distribution and consensus verification without the need for a third party. The continuum archive cycle is based on Armanesia workflow infrastructure. The prototype is built through open-source technologies such as IPFS (Interplanetary File System) for blockchain-enabled file systems to design a system prototype using the SDLC (System Development Life Cycle) method. Armanesia technology can be applied for both public and private blockchain ecosystems.

Keywords: Blockchain; distributed ledger; decentralized system; records and archives management; interplanetary file system

1. INTRODUCTION

The field of archival science as any other information processing disciplines (library, documentation, gallery, and museum), epistemologically and practically, is affected by the acceleration of Information and Communication Technology (ICT) growth and the ongoing information revolution. ICT drives the development of this science because it is a field whose core methodological and axiological concern is processing information. This ICT existence has even changed the constellation of thinking and reasoning in this field in which information that has been interpreted merely as foundational materials in the development of knowledge (epistemic) became information organisms (inforg) that have ontological equivalence.

The reasoning gap in interpreting this information, according to Floridi (2013), requires a radical change in viewing and interpreting reality (re-ontology). The interpretation of reality that has been associated with nature, humans, and other *ontos* has changed extremely to the understanding of *ontos* as information. Information as reality, submitted by Floridi (2013), becomes the epistemological basis for developing a philosophical narrative of information.

Floridi, in the next stage presents philosophical arguments related to his view which considers information as an ontological and epistemological matter. This view is expressed in his books: *The Philosophy of Information* (Floridi, 2011) and *The Ethics of Information* (Floridi, 2013).

When information is viewed from the ontological perspective as an information organism that has the same position and place as other organisms, then information by itself has intrinsic value. A value entitled to moral appreciation because of its existence and essence. It means there is no information that, with any reason and justification, is damaged or removed from the ecosystem (infosphere). In this context, Floridi wants to offer ontological pluralism as the conceptual foundation of a science.

In the context of archive, the life cycles model which views archives as an entity that has a cycle from creation to demolition and only keeps records of useful value is clearly not in line with Floridi's view. Because, in the life cycle, archives are interpreted as material artifacts which when of value deserve to be stored and if not, deserve to be destroyed. This means that, epistemically, these narrative views that archives as information can only be embedded with extrinsic values where a value is built based on human needs. When useful to humans, all entities are preserved, but if they are no longer useful, they are valid to be destroyed. Thus, value builds solely on usability.

The view of utility value in archive management in the current context is clearly not in line with the information management ecosystem. Archives are information objects which in themselves contain not only their utility value. Rather, the inalienable primary value known as intrinsic value. In the context of digital revolution, archives can be interpreted as digital data (Floridi, 2002; 2007; (National Archives and Records Administration, 1982). In the concept of Big Data, digital data represents the argument and strengthens the justification that data existence and essence should not be perturbed. This is because data in the NBIC ecosystem (nanotechnology, biotechnology, information technology, and cognitive science) is the foundational material supporting the technology's smooth operation.

As a dynamic discipline, because archival science is a multi/interdisciplinary field, a shift in epistemological and axiological perspective is necessary. Thus, multi perspectives, traditions, metatheories, and methodologies are commonplace in scientific development. This kind of flexibility expands the epistemic movement of this science in accepting and adapting any changes that occur. Floridi's view of ontological equivalence finds its place in the context of blockchain technology. This technology assumes that data will never be removed because of the existence of data that is networked with other data (immutable). A distributed system also requires the security of data stored in nodes that run in conjunction and synchronicity (Lemieux, 2019).

Blockchain technology has become a hot topic discussed recently in the archival community. Creating a workflow that is trusted to verify the authenticity of a document is a challenge in archival science. The application of blockchain technology started in 2008 with the introduction of the digital currency, Bitcoin, which is known as Cryptocurrency (Kernahan et al., 2021). Aside from the controversy surrounding the legitimacy of Bitcoin as a digital currency, the technological basis of Bitcoin that is blockchain has qualities that are applied in various industries, mainly archives management, due to its nature of transparency and recording every activity.

The archives industry has the principles of being accurate, reliable, and authentic. However, often what is found in the implementation scope is not following the principles of being accurate, reliable, and authentic. Various factors make the archival fieldwork not

following the principles. Among them is the inappropriate use of access through the archive information system owned by an organization, incompatibility of user authority, redundant documents, and problems with media and storage space.

The unsystematic management of archives can cause archives and data stored after creation to be unkempt, lost, or even unwantedly copied (forgery). The requirement for a sustainable and effective system must be started with the initial problems. To solve these issues, Armanesia is a public/private distributed ledger-based archival information system application. The notion of Armanesia is an application that can be utilized for archiving purposes in various industries, including government archives, banking, supply-chain management, oil and gas, energy, and the academic sector.

2. METHODS

This paper use System Development Life Cycle (SDLC) to build a prototype of Armanesia's system by adopting open-source technology. Kinds of literature related to blockchain technology and the implementation of blockchain in records and archives management were reviewed to create a conceptual framework of Armanesia. The concept building, as well as the experiment of prototype building of Armanesia's system, is expected to find a basic concept, workflow, and system wireframe of blockchain-based records and archives management system and interplanetary file system as a solution of trust issues in the field of archival.

3. RESULTS AND FINDINGS ANALYSIS

The blockchain system concept consists of a social, data/archive, and technical layer. These three layers have points that determine the sustainability of the archive and blockchain ecosystem. The fundamental underlying the Armanesia system is the Three-layer trust model of blockchain technology adopted from Lemieux (Victoria Louise Lemieux, 2018).

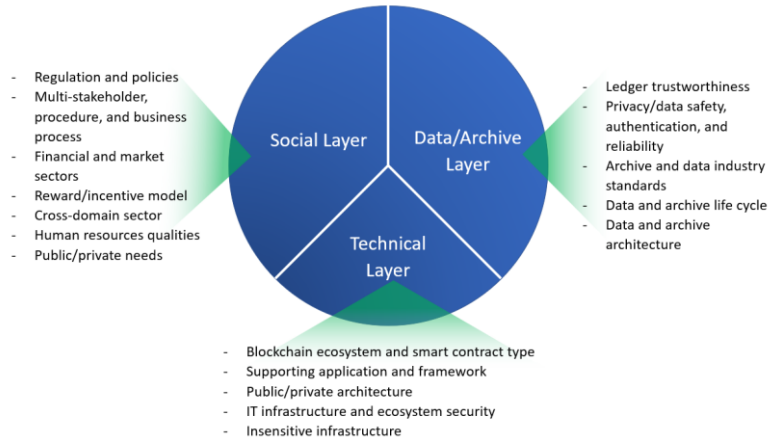

Figure 1. Armanesia fundamentals (Lemieux, 2018)

Figure 1 is a design diagram consisting of three main layers that form the blockchain ecosystem, covering the technical, social, and archival domains that enable blockchain to operate as a system of trust. Therefore, blockchain design is said to depend on three interacting "layers of trust": the social layer, the layer in which social actors interact with each other and determine how much information they need, and in a customized form (for example, by

convention, how much from the blockchain system and how much from other sources outside the system) to be able to trust and take action based on trust. A data layer, that supplies the information that social actors have decided they need from the blockchain system to give them the confidence to act. The technical layer, the technical means by which social actors interact and create, store, and obtain information about those interactions as untameable and undeniable evidence of facts about actions (Victoria Louise Lemieux, 2018). Each of these layers works together, intending to achieve trusted transactions.

Blockchain technology has good compliance features with practical permanence. When data is saved to the blockchain, it cannot be changed or deleted. This is one of the main features that allow blockchain to be used to move any digital asset. Armanesia attempts to solve problems for institutions that have historical records with low to high frequency, for example in the financial and regulators sectors. Keeping a single permanent shared record on the blockchain reduces the need for duplication, which can represent both space and process efficacy for an organization or government. This will also speed up the regulatory review process as there is no need for repeated reconciliations. A business unit can monitor regulatory updates and update its records based on the Armanesia blockchain regulations. Each compliance document can be recognized or dismissed based on regulations. Each approved document will be stored in a general ledger and can be shared and verified as needed.

Blockchain uses decentralized data storage, which has advantages over centralization in terms of security and efficiency. In Figure 2 an example diagram is given as an analogy of centralization and decentralization. Centralization carries the concept of data storage that is dependent on third parties. Data from a user is stored in third-party storage. Therefore, the user will have to trust the third party fully. The risk is that if any stored data is taken over by users who do not have the authority/permission, data leaks or hacking can occur. But in blockchain technology, users will place their data on the decentralized storage concept. It will be challenging for hackers to map the database that is being stored if they attempt to steal or alter data within the blockchain ecosystem. Because each piece of data will be checked in the blocks that are available on each node in the event of theft or database alterations.

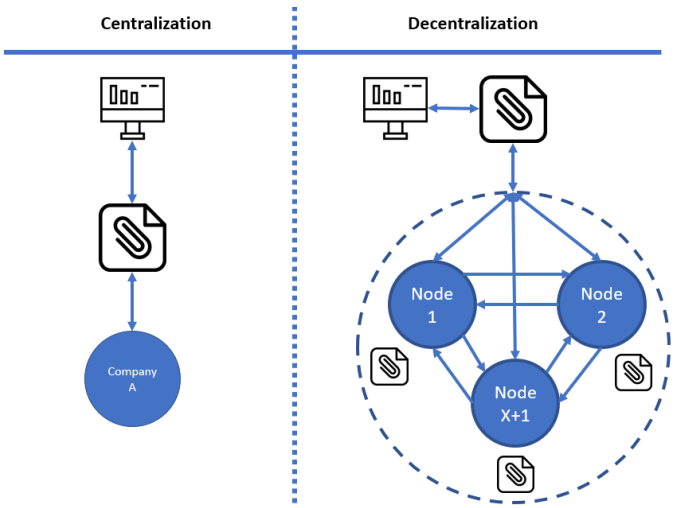

Figure 2. Concept of Centralization and Decentralization Data Storage (figure by authors)

Files, data, and archives can be easily removed and verified using one of the features in the Armanesia system, namely a ledger or what is known as a general ledger. An authority or an organization can issue a certificate and provide users with a receipt that they can share with any third party to prove the certificate's authenticity and the document. When a third party receives a receipt (in the form of a specific ID), they can easily check its authenticity in the Armanesia general ledger. Armanesia will provide the following features:

1) Transparency. Both parties interested in viewing the credentials of a document can view them on the user-customized Armanesia blockchain. This ensures that only authorized people can decide who has access to this information.
2) Immutability. Blockchain is the most secure source for storing information today. They depend on network integrity to ensure the authenticity of stored information. Thus, documents stored on the blockchain cannot be changed.
3) Using the latest storage network protocol – IPFS Technology. Armanesia's first step in developing a blockchain ecosystem. IPFS is a new storage protocol technology that has better features than independent HTTP.
4) Continuum Storage Model. Information and documents stored on the Armanesia blockchain use a continuum archive cycle, which means the stored information will never be recycled to maintain authenticity and track record since the information was created.
5) Disintermediation. Using the Armanesia blockchain to store and share document credentials to help go through the need for a central controlling authority that manages and maintains records. This makes the entirety of the credential storage process more trustworthy as there are no intermediaries or third parties involved that might be able to manipulate the data/information/documents/archive.
6) Collaboration and Reliability. Once information is available on the Armanesia blockchain, it is much easier to assume ownership, and therefore safer to share information without fear of information being falsified.

The making of the foundational technology of Armanesia using framework and programming language based on an open-source license. In simple terms, the workflow of Armanesia is depicted in Figure 3.

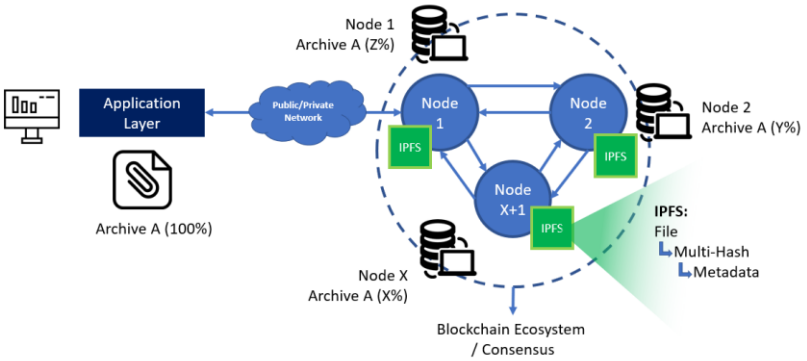

Figure 3. Armanesia simple workflow (figure by author)

Figure 4 shows layers or parts that form the Armanesia system. In this part, each process is explained as follows:

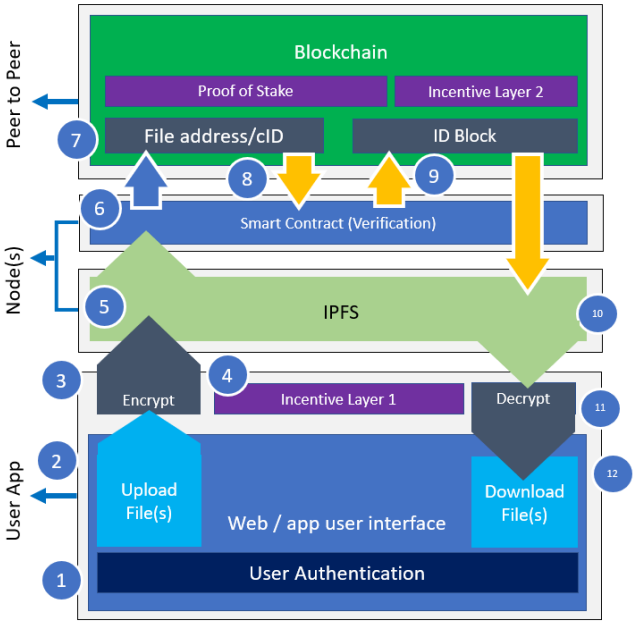

Figure 4. Armanesia advanced workflow (figure by author)

1) Users begin to authenticate on the User App in order to make transactions to upload or download files. This collection of component functions is also known as the Application Layer which functions for various business process needs of users or organizations. In this application layer as a functional basis of the overall application benefit for industrial needs (such as health, military, monetary, academic, governance, etc.). This section can provide an API (Application Programming Interface) so that the application can connect with third parties if needed. The technology used to create the application layer can vary according to user needs, but the Armanesia standard uses ReactJS, JSON, and the PHP framework.
2) Users can upload files after a successful authentication process. The file types supported by Armanesia have standard supported formats, such as PDF, JPEG, PNG, DOCX, and ZIP. Other formats can be customized as needed.
3) The encryption process is immediately carried out by the application layer as soon as the user uploads the file. The type of encryption carried out in this phase uses SSL/TLS collaboration available on the webserver client.
4) If a superuser (organization) has a monetization or incentive model in its application, it will go through this process first. This part is called Incentive Layer 1. This is not an incentive reward from Proof of Stake if activated.
5) The file will be stored on a node (computer) that is connected to the IPFS network system. IPFS network can be configured and selected in both private and public networks. Each connected node will store the file separated from its own hash file. The percentage of file fractions will be determined by the IPFS system. To find which peer is hosting the searched content (discovery), IPFS uses a Distributed Hash Table or DHT. The hash table is a database of keys to values. A distributed hash table is a table that is shared across all peers in a distributed network. IPFS uses the SHA-256 hash type by default.

6) The consensus layer uses Binance Smart Chain. Binance Smart Chain reaches approximately 3 seconds of block time using a Proof-of-Stake consensus algorithm. In particular, this uses something named Proof of Staked Authority (or PoSA), where participants put BNB at stake to become a validator. If they propose a valid block, they will receive a transaction fee from the transactions included in it. This process will later be connected to Incentive Layer 2.
7) After the verification stage is reached, the file will get a file address/cID which is stored in interconnected blocks. The following is an example of a cID generated from a file:

Figure 5. File address/cID

8) The steps to download files are done by first identifying the file's cID. Users can select the file through human-readable text in the application layer. Once the file is selected, the system will verify the file consensus.
9) Once the file has been verified properly, then the next downloading process is the system will map the block ID in the blockchain.
10) The file saved in IPFS will approve of downloading.
11) The file will undergo a description process to be able to be used by the user.
12) The file is successfully downloaded to the user's computer.

4. DISCUSSION

According to the findings of this research about Armanesia's prototype system, this part will discuss the implication and implementation of Armensia system, which is Application Warfare, Armanesia's Blockchain System implementation, Armanesia eVerify Application Implementation Simulation, and File tracing on Blockchain Network.

Armanesia Application Wireframe

The user interface of the application created in the Armanesia system will have a clean-design concept that eases users to stay productive even though they use new technology. Therefore users will remain familiar with and can learn quickly using a record management application in general.

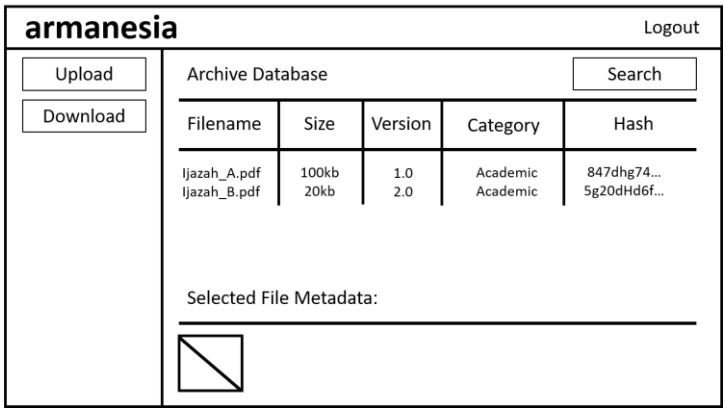

Figure 6. Armanesia application wireframe

Armanesia Blockchain System Implementation

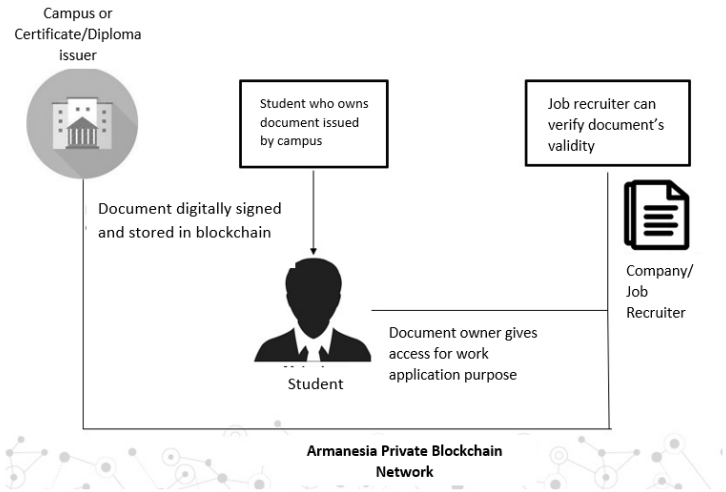

Figure 7. Armanesia Application Wireframe

Armanesia eVerify is one of the main features of Armanesia which functions as a verifier for documents that will be uploaded to be accessible by third parties if permitted by the document owner. This feature can obtain the authenticity of documents, by tracing if any files are changed or manipulated.

In this blockchain implementation concept, a simulation will be carried out for useful features for educational institutions with graduates or students who will apply for work at a company. The workflow of the above graph is described as follows:

1) The campus entity as a certificate or diploma issuing agency signs the validity of student graduation documents electronically or digitally which is stored on the Armanesia private blockchain network.
2) The student entity as the document owner receives the file published by the campus that is automatically registered to the student account so that the student can access the document electronically.

3) Corporate entities can access the address of the unique ID (hash) of each certificate or diploma document that the student has given access or address.

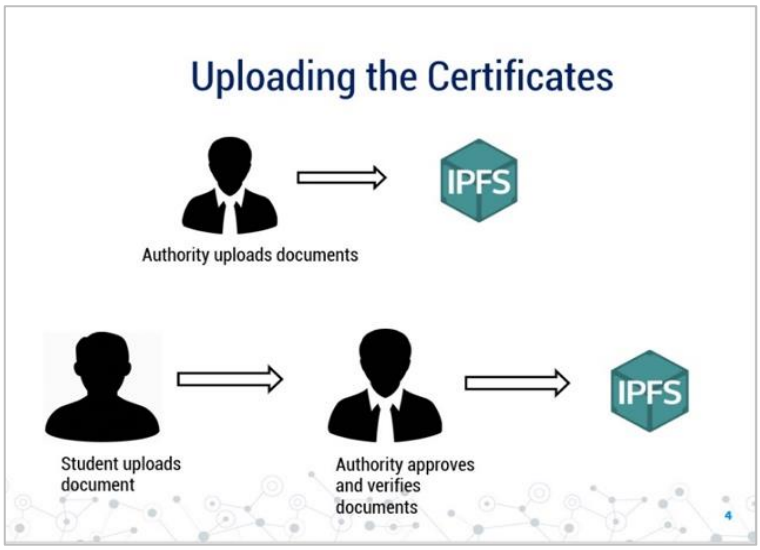

Figure 8. Document upload workflow process

Every file uploaded to eVerify Armanesia uses the IPFS system which functions as a decentralized storage system. Any entity that uploads documents such as campus, students, and companies; will enter the IPFS Armanesia network that has been configured.

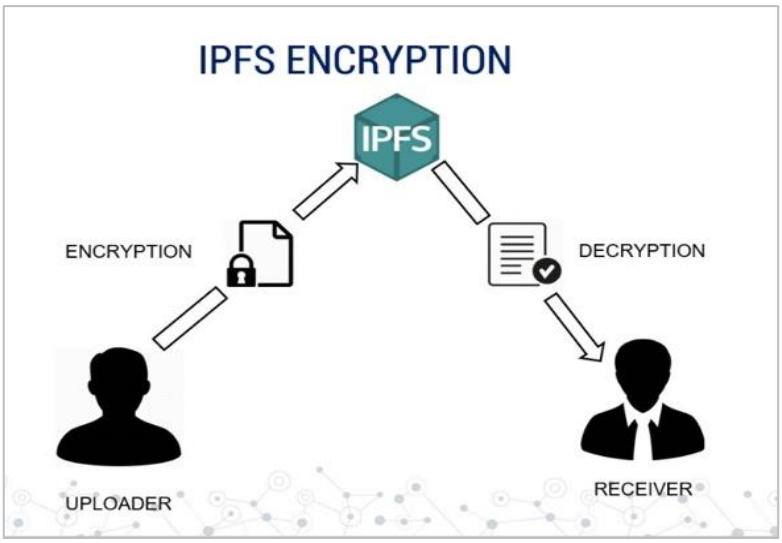

Figure 9. Document encryption process

Documents uploaded to the eVerify system will first be encrypted before entering the IPFS system. Document encryption is carried out as an effort so that documents are not easily accessed by parties who are unrelated or do not have authority over a document.

Armanesia eVerify Application Implementation Simulation

In the Armanesia eVerify application workflow experiment, the user must carry out some steps. Some of the stages include creating a new account on MetaMask with three different user roles, such as campus, students, and company where students apply.

Figure 10. Armanesia eVerify Interface

MetaMask is one of the most popular browser extensions that function as a way of storing Ethereum and other ERC-20 Tokens. This extension is free and secure and allows web applications to read and interact with Ethereum or other blockchains. MetaMask will be used as a way of logging in to the Armanesia eVerify application.

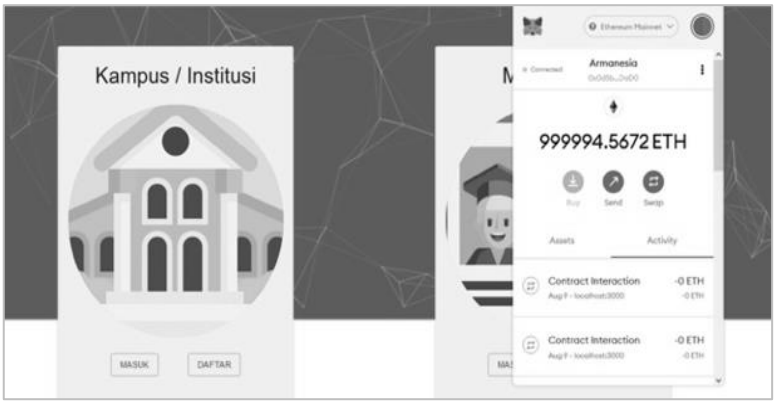

Figure 11. Armanesia eVerify login interface with MetaMask

In this simulation, several types of accounts will be created by first registering on MetaMask with access to Armanesia eVerify as follows:

Table 1. Preparation to access eVerify

RPC	http://bc.armanesia.com:8545
Chain id / Network id	1630
URL	https://verify.armaensia.com
Wallet Network	Armanesia

User roles that have been created for this simulation have various functions for several authorities are as follows:

Table 2. Account ID

Role	Account ID
Campus	0x22A956125c646a52c0dC1c12f57C7B541717eD7d
Student	0x90fBb27DE2C22CC85c1823510E0FdB6aba6C079b
Company	0x9c6b1586eb39e49Cc29aa949e461c9B7A93830a2

Table 3. Private Key

Role	Account ID
Campus	0xae7d03900a3d677cdfb9c4297a9703abca57826e5491dc3defb39044ea5bb944
Student	0xae7d03900a3d677cdfb9c4297a9703abca57826e5491dc3defb39044ea5bb944
Company	0xaf8968b3e1b9e9e2b4a63e92a7a91e33fdd972abf368480cf1bf28d632a1b386

At this simulation stage, an experiment has also been done to use a Google account that has been linked to id_role to log in to the Armanesia eVerify application.

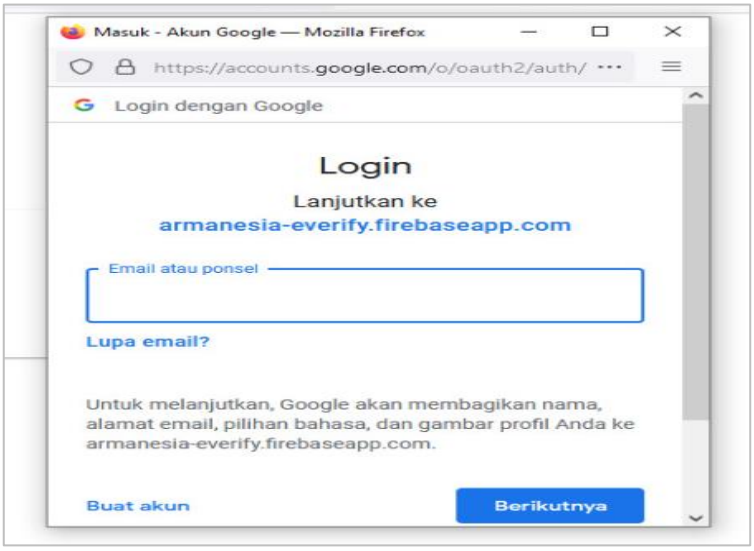

Figure 12. Login using a Google account

Student Role Function

Figure 13. Student role

The company's blockchain address must fill this form. This form is found on the student dashboard page when applying to the intended company, which provides document access to the company. When student users login to the Armanesia eVerify application dashboard, students can upload and then send the files needed to apply for jobs such as portfolios, Curriculum Vitae, or electronic diplomas to companies. For students to send their files, they need blockchain address information from each company that will be addressed.

Campus Role Function

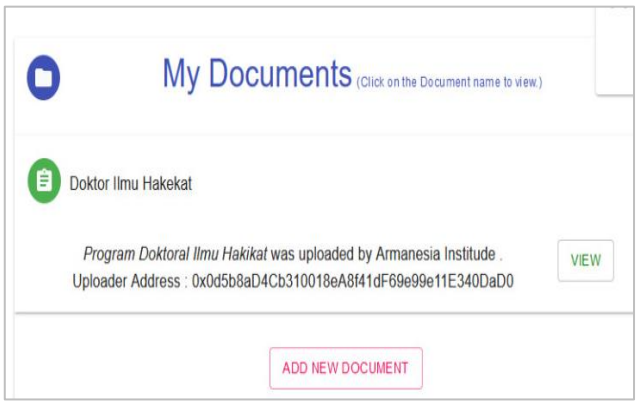

Figure 14. Campus sole

Documents that will be sent by students who will apply for jobs to companies, that have been given addresses, can also be seen by campus role users. So that the identity and content of the document can have proper validation automatically before being sent to the company.

Company Role Function

When the student has sent the files to the blockchain address of the intended company, the company will receive the files from the blockchain, by sending a notification to the user that a document has entered the company's application dashboard. The received document is accompanied by details of the sender's address such as name and hash_address. Suppose there

are documents that are changed or manipulated, in the form of renaming, or content. In that case, the system will automatically track the history of these changes on the Armanesia blockchain general ledger.

Figure 15. Company role

File Tracing on Blockchain Network

The flow of document delivery on Armanesia eVerify can be tracked systematically by entering the sending hash address into the Armanesia blockchain explorer system. The data displayed is the hash address of the institution (receiver) and student (sender).

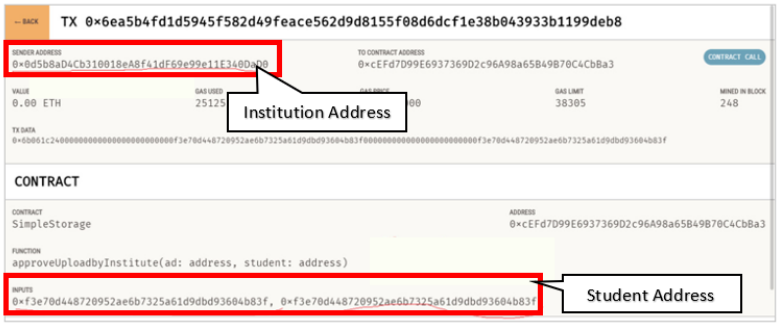

Figure 16. Document tracing on the Armanesia network blockchain explorer

Blockchain explorer is a software that uses API and blockchain nodes to draw various data from a blockchain and then uses a database to arrange the searched data and to present the data to users in a searchable format (Blockchain.com, 2021).

The implementation of blockchain explorer has been commonly used for crypto transactions, for example, to search Bitcoin transactions, users can visit https://www.blockchain.com/explorer and use the search bar to learn more about a specific Bitcoin address, transaction hash, or block number by entering to the search field column (Blockchain.com, 2021).

5. CONCLUSION

Armanesia's archival information system intends to introduce archive management technology using the blockchain ecosystem. The advantages of blockchain are, of course, the ability to meet the principles of archival science, which are accurate, reliable, and authentic, considering that blockchain has advantages in immutability and verification, which is currently very much needed by the archive and record industry. The fundamental underlying Armanesia is the Three-layer trust model of blockchain technology adopted from Lemieux, an archivist in the blockchain field. Armanesia can be utilized in various industrial fields, including agriculture, health care, education, and the military. Armanesia's development also largely depends on the archiving community from business, academia, and other fields to ensure that its capabilities and technological framework meet both present and future demands.

REFERENCES

Bailey, S. (2007). Taking the road less travelled by: The future of the archive and records management profession in the digital age. *Journal of the Society of Archivists*, *28*(2), 117–124. https://doi.org/10.1080/00379810701607777

Bell, M., Cooper, D., Green, A., Bui, T., Sheridan, J., Thereaux, O., Collomosse, J., & Higgins, J. (2019). Underscoring archival authenticity with blockchain technology. *Insights: The UKSG Journal*, *32*. https://doi.org/10.1629/uksg.470

Blockchain.com. (2021). *Blockchain*. Blockchain.Com. https://www.blockchain.com/explorer

Bushey, J., Demoulin, M., & McLelland, R. (2015). Cloud Service Contracts: An Issue of Trust / Les contrats de service d'informatique en nuage: Une question de confiance. *Canadian Journal of Information and Library Science*, *39*(2), 128–153. https://doi.org/10.1353/ils.2015.0009

Cheng, E. C. K. (2018). Managing records and archives in a Hong Kong school: a case study. *Records Management Journal*, *28*(2), 204–216. https://doi.org/10.1108/RMJ-02-2017-0004

Floridi, L. (2011). *The Philosophy of Information*. Oxford University Press Inc.

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press Inc.

IFPS. (n.d.). *IFPS Docs*. Retrieved February 10, 2022, from https://docs.ipfs.io/concepts/content-addressing/#identifier-formats

Keller, J. R. (2018). *Blockchain's potential role in the future of archiving*. Open Data Institute. https://theodi.org/article/blockchains-potential-role-in-the-future-of-archiving/

Kernahan, A., Bernskov, U., & Beck, R. (2021). Blockchain out of the box - Where is the blockchain in blockchain-as-a-service? *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 4281–4290. https://doi.org/10.24251/hicss.2021.520

Lemieux, Victoria L, Hofman, D., Batista, D., & Joo, A. (2019). *Blockchain Technology and Record Keeping*. 139. http://armaedfoundation.org/wp-content/uploads/2019/06/AIEF-Research-Paper-Blockchain-Technology-Recordkeeping.pdf

Lemieux, Victoria Louise. (2017). Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems : An Archival Theoretic Evaluation Framework. *Future Technologies Conference (FTC) 2017*, *June*, 1–11. https://www.researchgate.net/profile/Victoria_Lemieux/publication/317433591_Blockchain_and_Distributed_Ledgers_as_Trusted_Recordkeeping_Systems_An_Archival_Theoretic_Evaluation_Framework/links/593aa6450f7e9b3317f4d860/Blockchain-and-Distributed-Ledgers-as

Lemieux, Victoria Louise. (2018). Blockchain Technology for Recordkeeping Help or Hype? *Blockchain Technology for Recordkeeping*, *1*(October). https://doi.org/10.13140/RG.2.2.28447.56488

Maday, C., & Moysan, M. (2014). Records management for scientific data. *Archives and Manuscripts*, *42*(2), 190–192. https://doi.org/10.1080/01576895.2014.911686

Richards, L. L. (2018). Records management in the cloud: From system design to resource ownership. *Journal of the Association for Information Science and Technology*, *69*(2), 281–289. https://doi.org/10.1002/asi.23939.