Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation

Arko Djajadi[1], Karunia Suci Lestari[*2], Linda Evan Englista[3], Aldi Destaryana[4]
[1,2,3,4]Magister Informatics Engineering in Universitas Raharja, Tangerang, Indonesia
E-mail: [1]arkodjajadi@raharja.info, [*2]**suci@raharja.info**, [3]linda@raharja.info,
[4]aldi.destaryana@raharja.info

Abstract

*The security and confidentiality of data are very important for institutions. Meanwhile, data fabrication or falsification of official documents is still common. Validation of the authenticity of documents such as certificates becomes a challenge for various parties, especially those who have to make decisions based on the validity of the document. Scanning-based signatures on printed and digital documents are still relatively easy to counterfeit and yet still difficult to distinguish from the original. The traditional approach is no longer reliable. Solutions to these problems require the existence of data security techniques, seamless online verification of the authenticity of printed documents, and e-certificates quickly. The objective of the study is to model the e-certificate verification process via blockchain and proof-of-stake consensus methods and use MD5 encryption. The data or identity listed on the e-certificate is secured with an embedded digital signature in the form of a QR code and can be checked for the truth online. A combination of technologies capable of suppressing or removing counterfeiting of digital assets will accelerate digital transformation across spectrums of modern life. The resulting architectural model can be used as a starting point for implementing a blockchain-based e-certificate verification and validation automation system.***

Keywords *— Website Architecture, Digital Signature, Blockchain, E-certificate, Security Validation*

1. INTRODUCTION

The security and confidentiality of data in an institution are of critical importance because it contains information related to many valuable things. If the data is intercepted or leaked, it can be misused by unauthorized persons and can harm many parties. So it takes data security to protect existing data so as to minimize data leakage.

In some other cases, data confidentiality is not the main issue, such as in the case of the authenticity of a published certificate, ID card, or similar documents. Being easily verifiable and trustable is of more importance, as generally, such documents tend to be open for public sharing. The next level is that all published documents are truly legitimate and clearly distinguishable from modified or falsified versions of the same documents. Here data security technologies play even more strategic usage.

The COVID-19 pandemic makes all enactments and social interactions geared toward minimized physical touch by exploiting all potential technologies to achieve fully automated and computerized systems or digital systems that facilitate access without direct contact between document creators and recipients. Now more than ever before, ballroom conferences are transformed into online systems by using video conferences known as web-based seminars or known as webinars. Webinars are new externally forced innovations in organizing seminars that generally take place directly (face-to-face)[1]. Webinars are one way to answer the challenges of educational knowledge in the era of industrial revolution 4.0. A webinar is one of the e-learning or electronic education programs. Webinar refers to the asynchronous method of online education in which people gather at a given time to listen, observe, and participate in the presentation of a topic[2].

In addition to the material obtained from the webinar, webinar participants also need a certificate as proof of participation as a seminar or webinar participant. Webinar certificates are designed to be e-certificates to facilitate distributing certificates to participants without direct contact between recipients and webinar event organizers. E-certificate is a right that must be obtained by each participant as proof of participation in webinar activities[3].

Currently, many places sell services in making changes to documents or certificates, so many people feel aggrieved due to the actions of these irresponsible parties. Today, many institutions or companies issue documents or certificates in digital or electronic form, making them easy to manipulate. Such as participant name changes and signature falsification, and when scanning is relatively easy to falsify, even though it has gone through the validation and verification process of a system that is sometimes indistinguishable from the original document. To minimize fraud or falsification of e-certificates, the certificate must have a fast automation system with its own security and prove the validity of the e-certificate obtained is true to the original owner of the e-certificate. Designing a system architecture becomes an important part of creating a software engineering model so that until the formation of a complete information system. The system architecture is defined as mapping and planning for information needs in an organization or company[4]. Automation and artificial intelligence (AI) are changing the nature of work[5]. Currently, the creation of system architecture models is done using software also for the manufacture of prototypes. So that the architecture was created to create a website verification and validation of the e-certificate.

With the application of digital signatures and cryptography using the Blockchain method, digital signature data in e-certificates is databases and encrypted normally and can be stored in a decentralized digital data storage. Cryptography is the science that learns how to keep our messages or documents secure, it cannot be read by unauthorized parties[6]. Blockchain is a continuously evolving, secure, and shared system in which each data user keeps a copy of the record and can only be updated if all parties involved in the transaction agree to the update[7]. Blockchain has become one of the most widely used methods for securing data storage and transmission by decentralized applications. Blockchain applications range from Internet of Things applications to digital rights management, pharmaceuticals, financial transactions, and securing commerce[8]. Bitcoin was the first user of Blockchain[9] technology in addition to being used in securing bitcoin transactions, Blockchain technology also utilized securing the authenticity level of Diploma[10], transcript value[11], verifying authenticity in a written work of certificate archiving poem[12], improving security in transacting in crowdfunding platforms[13], certificate security[14][15][16][17], lecturer certification program[18], as Smart Digital Signature [19] , design of product tracing system[20], utilization in education[21][22], as security of STNK and SIM[23], used in content copyright data system[24], E-voting[25], security of the presence system [26] , and can be used in the security of e-commerce transaction process[27]. Blockchain is also applied with other technologies such as IoT and smart cities[28],[29],[30]. Adoption of blockchain technology continues to increase in various fields such as healthcare, asset surveillance, digital rights management, financial services, smart vehicles, supply chain, IoT, etc.[31]. And digital signatures function in testing the integrity and authentication of a digital document and can detect document changes from manipulation[32]. Signature verification and forgery detection is the process of automatically and directly verifying a signature to determine if it is authentic. There are two main types of signature verification: static and dynamic. Static or offline verification requires the signature to be verified after the document is created, whereas dynamic or online verification happens when someone digitally signs the document on her tablet or similar device[33]. So that it can be proven if the document is actually issued or made by the organizer of the seminar or training.

In the world of technology, the existence of blockchain technology is a very dramatic improvement for collecting, distributing and managing information, and blockchain is also a decentralized database. Blockchain is decentralized and permissionless[31]. Blockchain has 3 (three) main structures that can make this technology can make transactions quickly, namely: Block, Chain & Network[32]. The main benefits of this blockchain technology include Decentralization, Transparency, Immutability, and security and privacy[34].

In verification of this document using the proof of stake method as well as MD5 encryption. Proof-of-Stake (PoS) is a protocol developed as an energy-efficient alternative to PoW. Instead of calculating resources, executives are selected based on bets, or contributions to the blockchain network[35]. Proof-of-Stake (PoS) aims to replace consensus paths in distributed systems. Rather than solving the proof of work, the nodes producing blocks must provide proof that they have access to a certain number of coins before they are accepted into the network[12]. Blockchain platforms NXT and PeerCoin use PoS consensus, and Ethereum is moving to PoS consensus. HLF uses the Practical Byzantine Fault Tolerance (PBFT) consensus, which tolerates Byzantine faults (such as malicious nodes)[31]. Proof of Stake has speed and consumes less power than Proof of Work. Proof-of-Stake (PoS) is applied in several studies on consensus mechanisms in the fundamentals of[36] applications, performance and security evaluation[24], mining games in performing strategy[37], performance and scalability in the communication of a group[38], and maintaining privacy[39].

In order to maintain the integrity or authenticity of electronic documents, cryptographic algorithms are combined with multiple methods of message algorithms using MD5, MD5 encryption, used in various fields for maintenance and data integrity proof is a one-way cryptographic function that[40]. Encryption is used to ensure the confidentiality of security services. Encryption is the process of encoding plaintext into ciphertext (either unintelligible or understandable data). Decryption is the reverse process of converting ciphertext into plaintext.. The encryption and decryption process can be implemented using symmetrical or asymmetric cryptography[41]. Hash is a one-way mathematical function to protect data integrity. It works by calculating a unique fixed-sized value called a "hash value" for each variable input. The hash function is one-way, which means the original data cannot be recalculated from a unique output. Its security strength lies in its one-way characteristics, which are used to protect data integrity[41].

The QR code contains a digital signature of data such as title holder name, registration number, role number and total score, and is signed by the university authorities. To verify the digital signature, you must use a specific smartphone app that scans the QR code and authenticates the certificate. After many articles surveyed from previous studies agreeing on document authentication using digital signatures and QR Codes[42]-[46], digital signatures in the field of cyberlaw as evidence[47], as well as in universities [48] in the issuance and verification of e-certificates in webinars[49] using web applications[50] to save computing resources by eliminating unnecessary storage and network use[51]. Research that uses QR Codes as proof of the validity of documents in the field of education[52], Validate issued certificates so that certificates can be checked for authenticity and suitability of information contained in digital certificates[53][54][55][56], as a means of digital signature to identify a sender, as well as to prove the legitimacy of the owner of a digital document so that an authentic digital signature (valid) [57][58], Diploma[59] authenticity authentication, as E-Payment protection in E-Commerce[60], is used for attendance presence[61], and is implemented in student identity cards to make it easier for students to check real data updates about personal identity, college status history, and appropriate study history on the forlap.dikti.go.id[62]. So this research for the validation of e-certificate authentication also uses digital signature and QR Code as certificate number and QR Code to make it easier to go to the e-certificate verification and validation website. So that with the Blockchain using QR Code can prove if the certificate is correctly signed digitally by the organizer of a webinar event that is neatly registered.

To verify e-certificates designed a QR code digital signature verification website in Blockchain-based e-certificates to prove the validity of e-certificates obtained by webinar participants. The verification website view asks the user to upload the e-certificate file to be verified, in addition in the same view displays the amount of real data of the verified e-certificate document. After uploading the e-certificate file on the QR Code digital signature verification website in the e-certificate successfully uploaded and the e-certificate verified, it will be displayed the output of the system containing transaction information that is considered valid by consensus. In this research designed the e-certificate verification website model in the form of a prototype and hopefully in the next research can be developed again. And validated by using MD5 in recognizing the validity of the document or certificate. In the creation of the prototype in this study using Figma, the display can be arranged and adjusted to make it easier to understand for users who will verify the digital signature in the webinar e-certificate obtained.

The purpose of this research is to create a website model for verification and validation of blockchain-based e-certificate data using QR codes that can prove the e-certificates received by webinar participants to avoid falsification of digital assets in order to follow the acceleration of digital transformation. This website architecture can also later be used as proof of the validity of the e-certificate obtained from the webinar organizer, so that if the digital signature in the e-certificate is correctly issued by the organizer then the display of encryption will be displayed on behalf of the participant's name in the verified e-certificate.

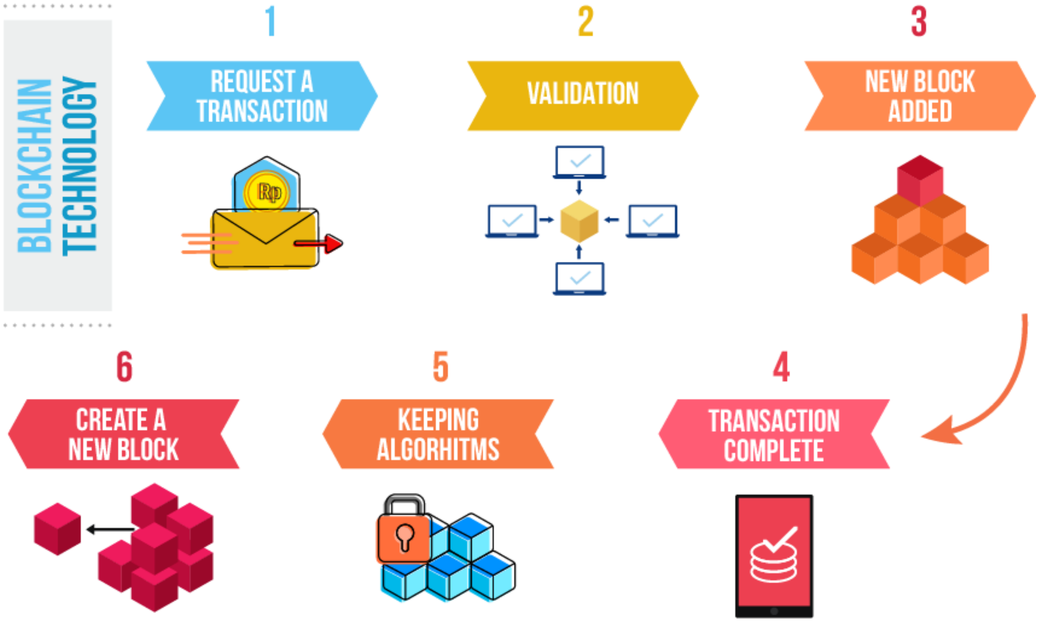


Figure 1. Six basic steps in creating a complete blockchain transaction

2. RESEARCH METHOD

Verification of web-based Blockchain-based e-Certificate Validation is carried out in 4 research stages, including requirement identification, planning, design of prototypes/architectures, and the last stage of prototype review that has been designed that can be seen in the image below:

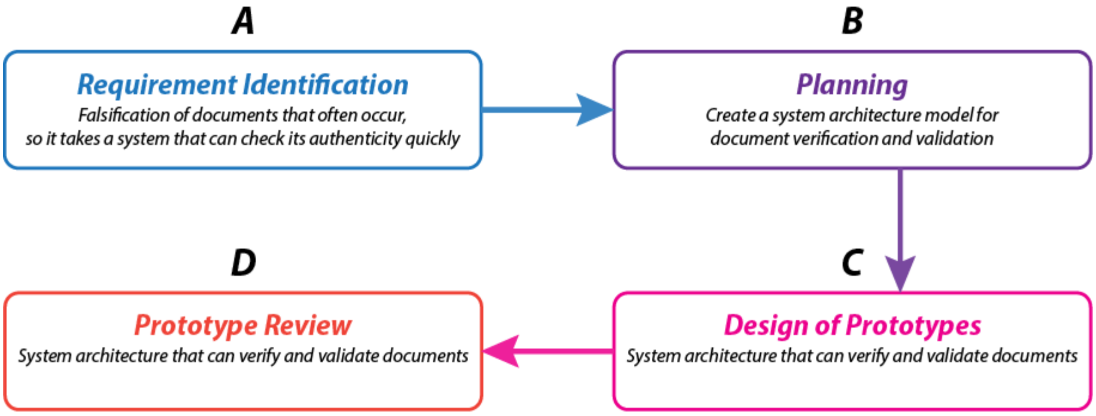

A
Requirement Identification
Falsification of documents that often occur, so it takes a system that can check its authenticity quickly
B
Planning
Create a system architecture model for document verification and validation
C
Design of Prototypes
System architecture that can verify and validate documents
D
Prototype Review
System architecture that can verify and validate documents

Figure 2. Research Methods

It uses a blockchain security method in which blockchain users are uniquely identified by public key certificates. In public settings, the user first generates a key pair (the default option is ECDSA based on Elliptic Curve Secp256k1). That hash function serves as a transaction address or account number in the cryptocurrency system. PoW mining is not cheap. This process consumes a lot of energy and is said to use enough electricity to power a small country like Denmark. Staking is essentially a locked account with a specific balance that represents a miner's commitment to keep the network healthy. Assuming the function returns stake, miner M can generate new blocks by solving a puzzle of the form:

$$H(n\|H(b))<s(M).t.$$

It turns out that the larger s(M) is, the easier it is to find n.

Ethereum's upcoming PoS protocol is implemented in the form of smart contracts. This is called Casper and allows miners to become validators by depositing Ether into Casper accounts. The contract selects reviewers based on their deposit amount and suggests the next block. However, its peculiarity is that it forces validators to behave correctly, with the penalty of losing the entire deposit each validator bets on whether a particular block will be validated in the future. If the block is confirmed, the validator receives a small reward. But otherwise the validator loses the deposit. This mechanism avoids the unacceptable problem of validators being able to contribute blocks on different branches. Tezos implements a simplified version of Casper. In this version, contract purchases become an authority and can approve changes to the underlying blockchain. Tezos aims to provide a scalable blockchain where soft and hard forks are blockchain-specific features[63].

2.1. Architecture — diagram block: input box, process box, output box

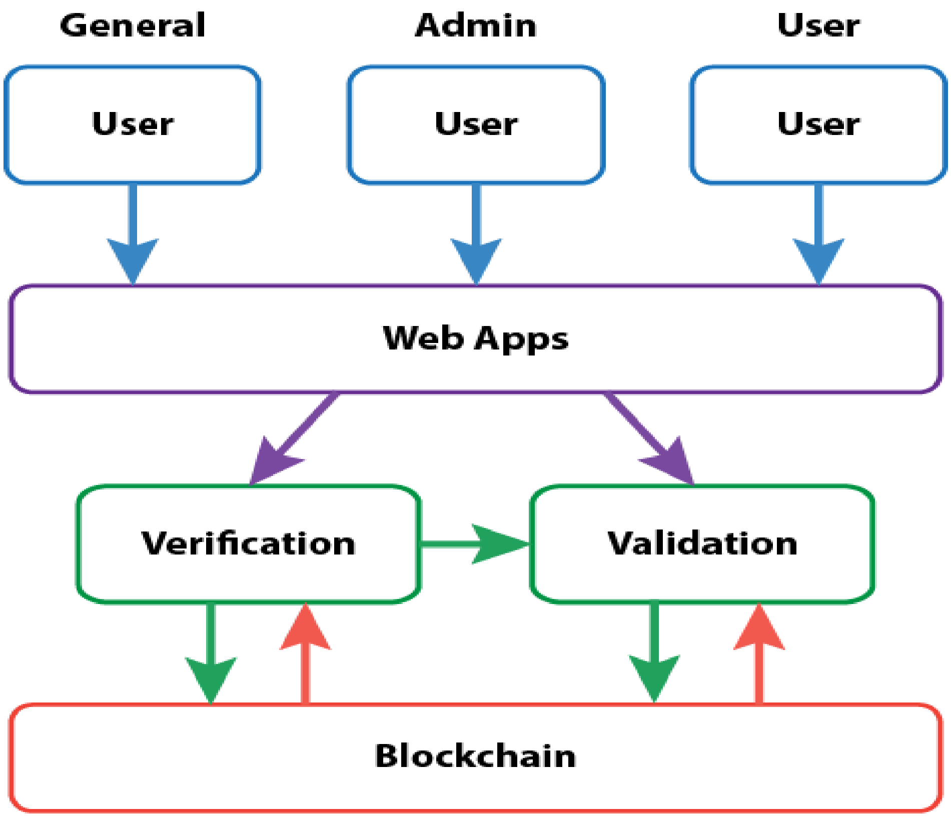
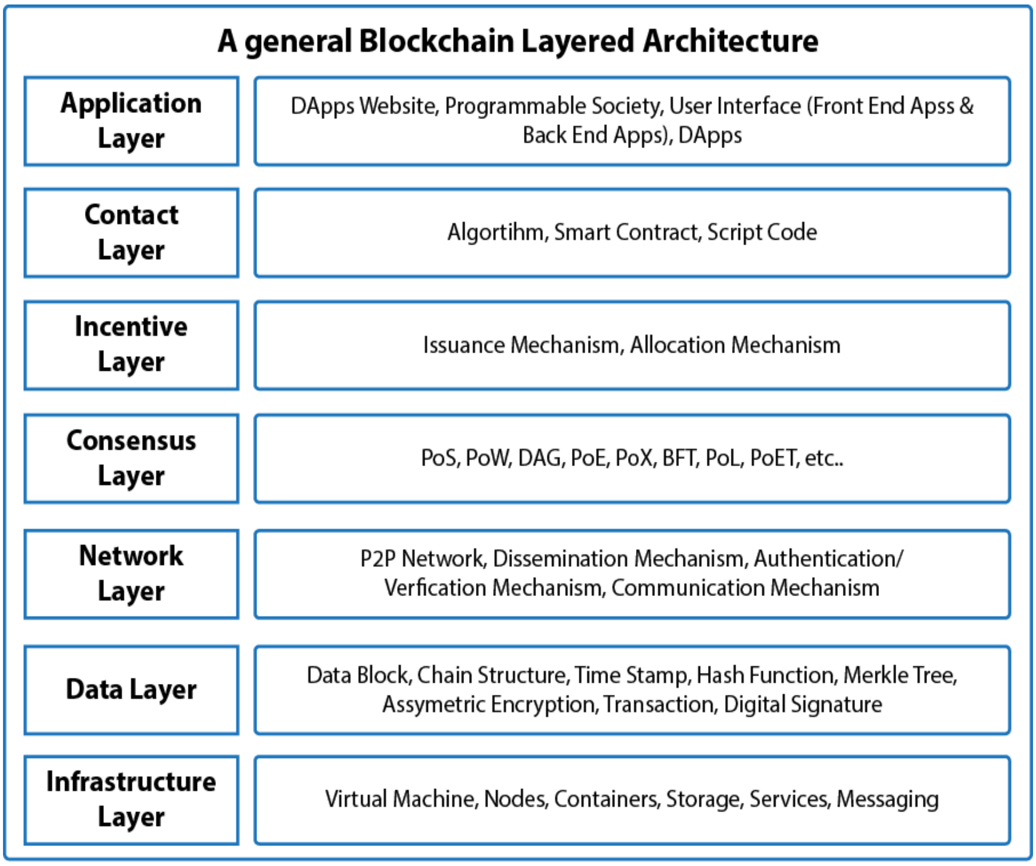


Figure 3. Architecture System Verification and Validation Document



A general Blockchain Layered Architecture

Application Layer	DApps Website, Programmable Society, User Interface (Front End Apss & Back End Apps), DApps
Contact Layer	Algortihm, Smart Contract, Script Code
Incentive Layer	Issuance Mechanism, Allocation Mechanism
Consensus Layer	PoS, PoW, DAG, PoE, PoX, BFT, PoL, PoET, etc..
Network Layer	P2P Network, Dissemination Mechanism, Authentication/ Verfication Mechanism, Communication Mechanism
Data Layer	Data Block, Chain Structure, Time Stamp, Hash Function, Merkle Tree, Assymetric Encryption, Transaction, Digital Signature
Infrastructure Layer	Virtual Machine, Nodes, Containers, Storage, Services, Messaging

Figure 4. A general Blockchain Layered Architecture

Blockchain technology is open source and allows users to develop applications using a common application programming interface Smart contracts on the blockchain can automatically generate transactions, make decisions, and store data. All nodes in the system can automatically process and validate data using a specific consensus protocol. Blockchains are automatically maintained and verified by the protocol without manual intervention. Consensus is required to validate transactions and update the general ledger Blockchain systems are inherently secure. Because these systems use asymmetric encryption. Asymmetric encryption consists of a set of public keys that are visible to everyone and a set of private keys that are visible only to the owner. Encryption is used to ensure the confidentiality of security services. Encryption is the process of encoding plaintext (data you understand) into ciphertext (data you do not understand). Decryption is the reverse process of converting ciphertext into plaintext. The encryption and decryption process can be performed using either symmetric or asymmetric cryptography. A hash is a one-way mathematical function for protecting data integrity. It works by calculating a unique fixed-size value called a "hash value" for each input of the variable. Hash functions are one-way. In other words, it is not possible to back-calculate the original data from the unique outputs[3]. Its security strength lies in its one-way property used to protect data integrity.

- Blockchain-based business applications represent the application layer.
- Contact layer describes the programming approaches available on the blockchain.
- Nodes involved in managing applications receive incentives according to the mechanisms listed in the incentive layer.

- The Consensus Layer provides various consensus algorithms for blockchain applications.
- The network layer consists of data propagation and data inspection mechanisms and distributed network mechanisms.
- Timestamped data blocks are part of the data layer. Chain structures, Merkle trees, cryptography, and hash functions are used to manage the security of these blocks[39].

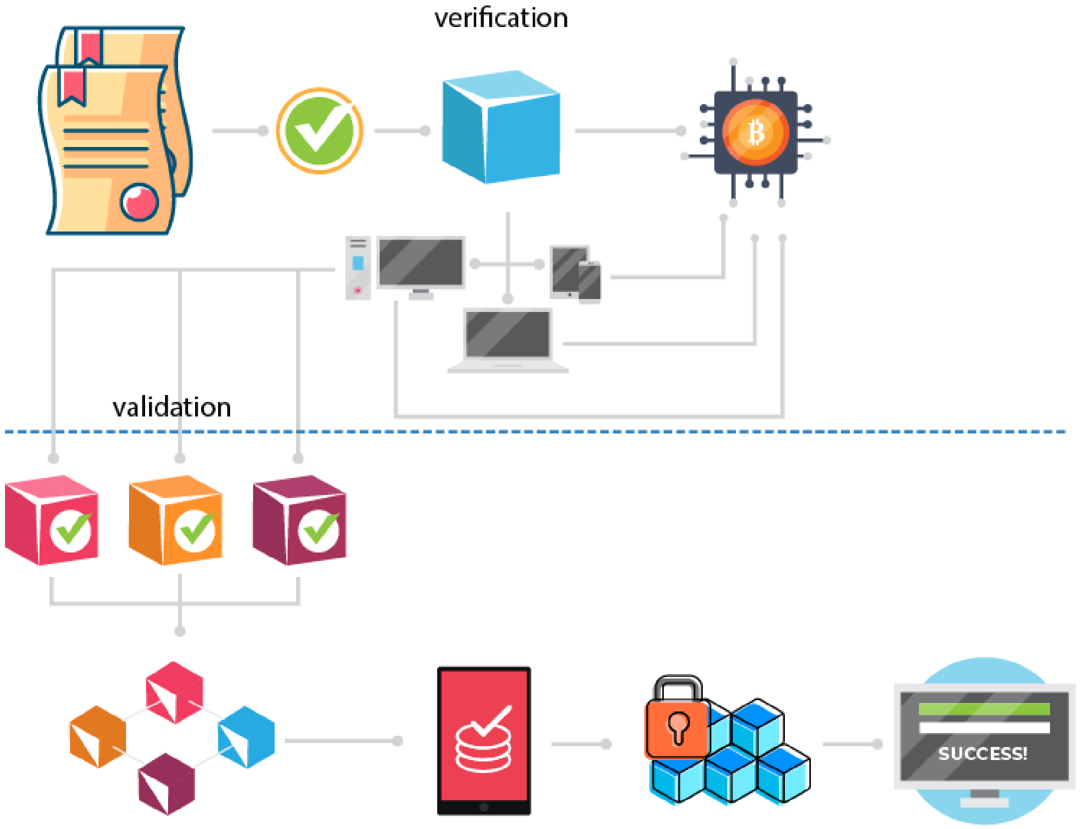


Figure 5. E-Certificate Validation and Verification Process Architecture

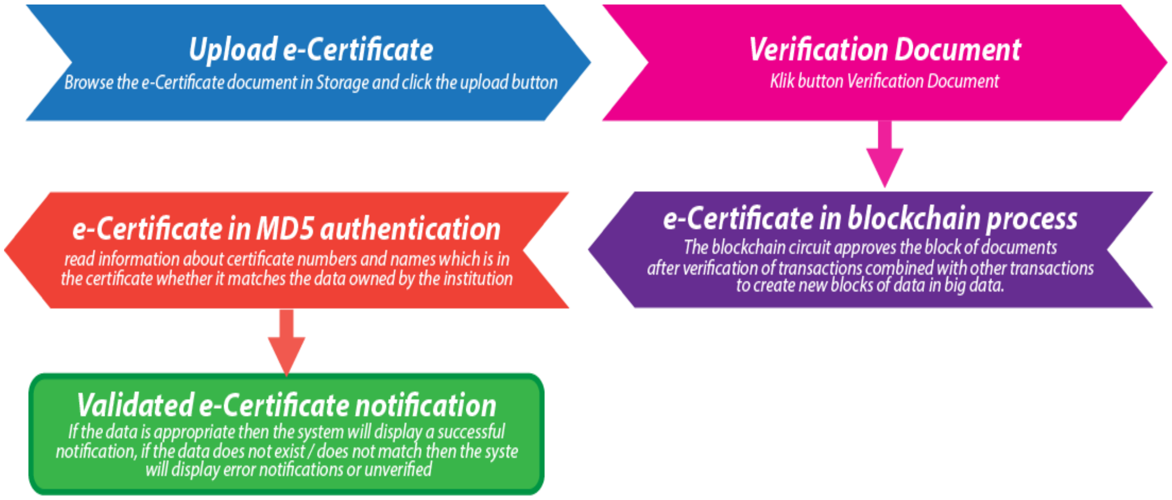

Upload e-Certificate
Browse the e-Certificate document in Storage and click the upload button
Verification Document
Klik button Verification Document
e-Certificate in blockchain process
The blockchain circuit approves the block of documents
after verification of transactions combined with other transactions
to create new blocks of data in big data.
e-Certificate in MD5 authentication
read information about certificate numbers and names which is in
the certificate whether it matches the data owned by the institution
Validated e-Certificate notification
If the data is appropriate then the system will display a successful
notification, if the data does not exist / does not match then the syste
will display error notifications or unverified

Figure 6. E-Certificate verification steps on the Website

2.2. Flowchart Automation validation of e-certificates with blockchain

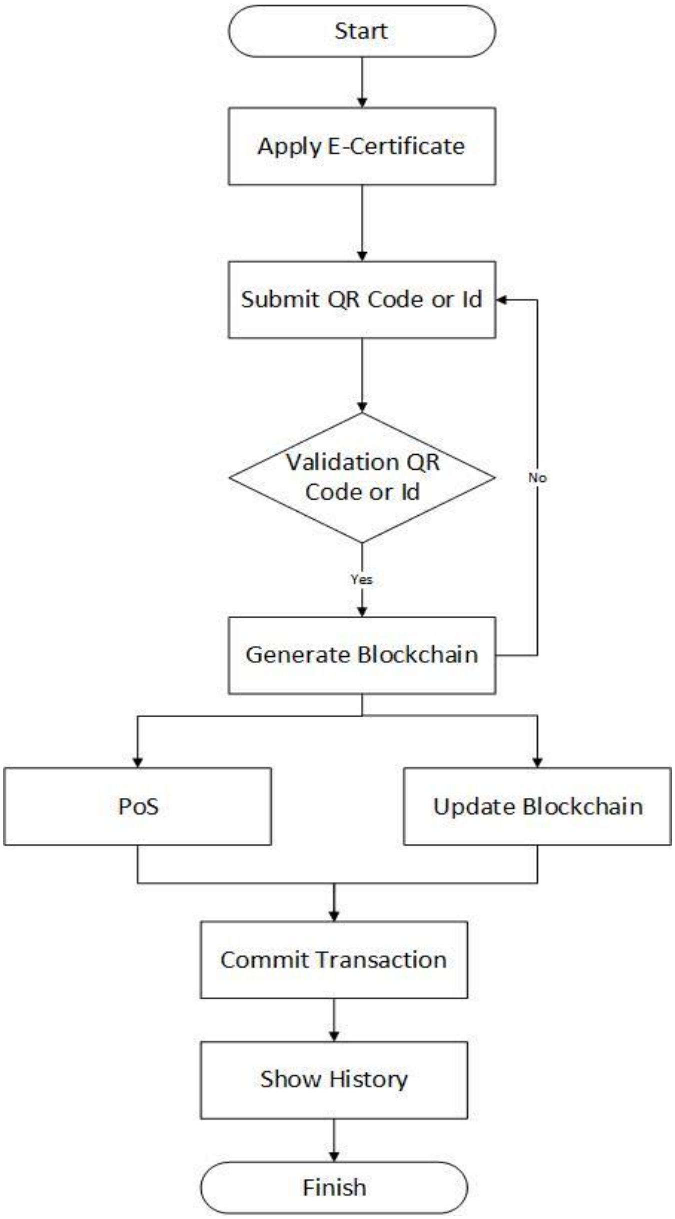


Figure 7. Automation Validation of e-certificates with blockchain

2.3. Flowchart Automation of e-certificate verification with blockchain

The design contains 3 main components/models. They are for authentic details, Apply for new ones, Check authenticity. Here is the entire project stream in the form of a flowchart. Below are the tasks mentioned that are available in the system: This system is such a design as soon as you open the no login /Registration option. Users can use this software/portal to authenticate their certificates, apply for new certificates, and to upload newly issued certificates. When you upload a certificate, it creates a database for users. Users can use it to check the authenticity of certificates as part of the recruitment process and file an action against fake ones[64].

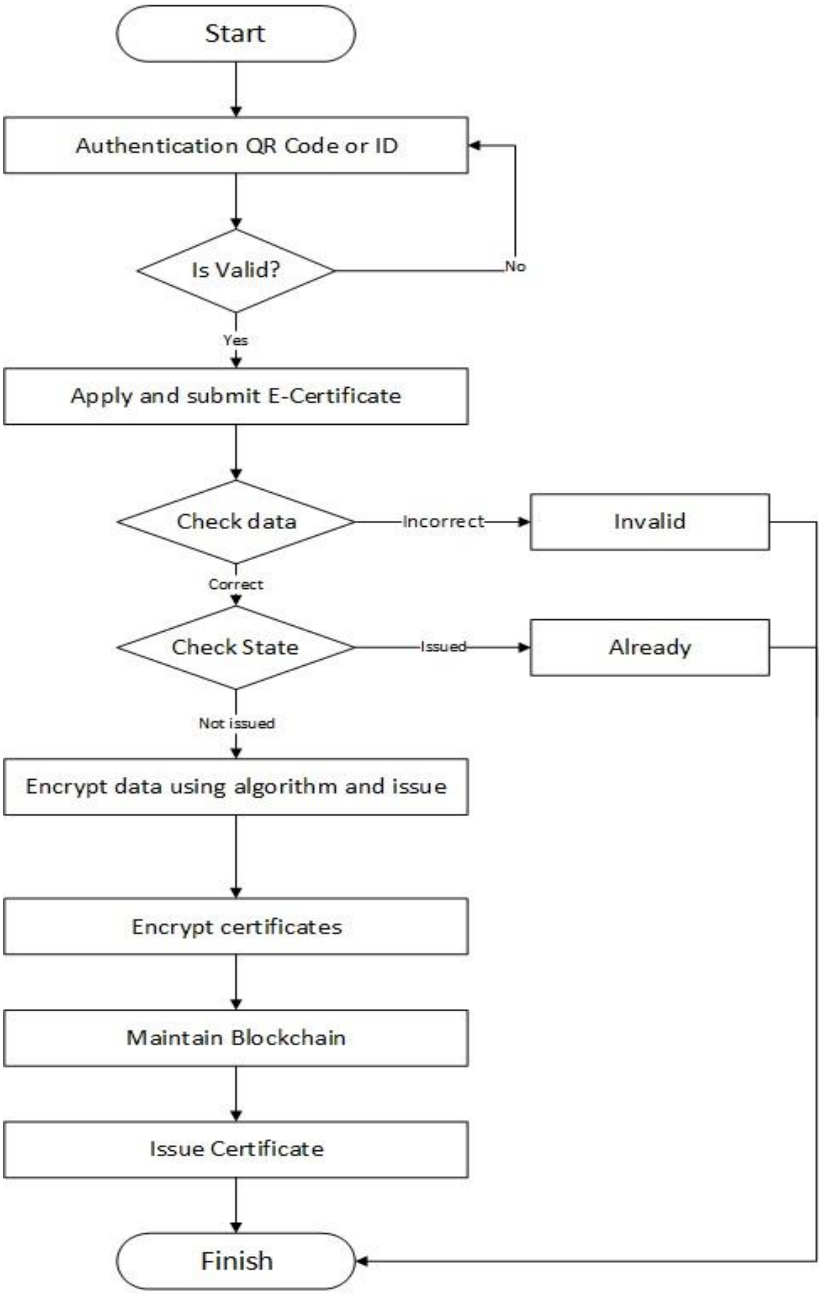


Figure 8. Automation of e-certificate verification with blockchain

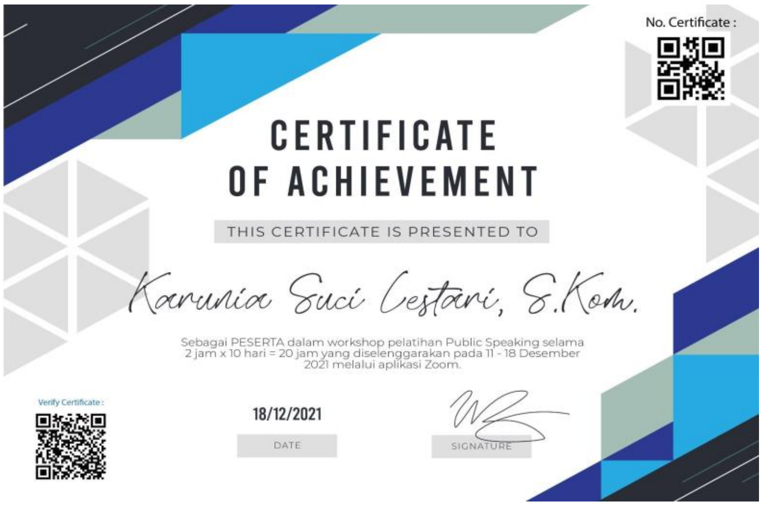
3. RESEARCH RESULTS AND DISCUSSION

Blockchain systems use a “one-way” mathematical function, often called a “hash function,” that maps frequently changing variable-sized data to fixed-sized data[66]. Hashes are implemented in electronic systems used for user data and use mathematical functions to transform data into various formats[67]. The best-known examples of hash functions are MD2, MD5, and SHA[68].

The study found that Message-Digest Algorithm 5 (MD5) was designed by Ronald Invest in 1991 and uses a hash size of 128 bits and a message block size of 512 bits[69]. The

MD5 algorithm enters a message of any length and produces a 128-bit message digest from the input as output. The authentication algorithm somehow normalizes all the data in the secret message used for authentication. Md5 consists of 64 tasks divided into 16 four-round operations. The MD5 algorithm was developed very quickly on 32-bit computers. The algorithm was invented by Professor Ronald L. Rivest[70].

In order to prevent the circulation of fake degree certificates, a method is proposed where the integrity of the contents within the certificate can be verified with the use of QR Code and a Smart website.



No. Certificate :

CERTIFICATE OF ACHIEVEMENT

THIS CERTIFICATE IS PRESENTED TO

Karunia Suci Lestari, S.Kom.

Sebagai PESERTA dalam workshop pelatihan Public Speaking selama 2 jam x 10 hari = 20 jam yang diselenggarakan pada 11 - 18 Desember 2021 melalui aplikasi Zoom.

Verify Certificate :

18/12/2021

DATE

SIGNATURE

Figure 9. examples of e-Certificates received from certain training/webinars

Figure 9 is an example of an e-certificate that wants to be verified, the certificate number is made into a QR Code to facilitate verifying the e-Certificate weblink of the Event Organizer Institution for verification and validation of e-Certificates made into QR Code as well. An example of a web view of a verification agency is in Figure 10, to start verifying and validating starting with Browse e-Certificate files that have been downloaded or that are already in your document storage.

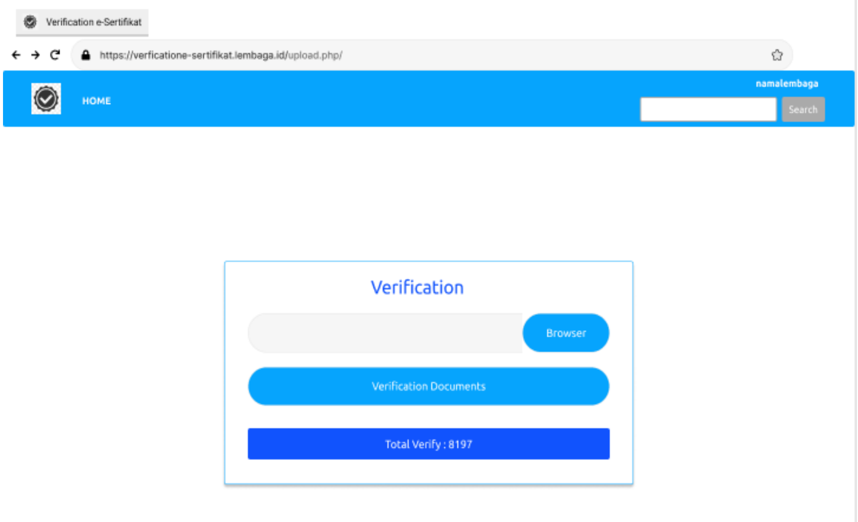
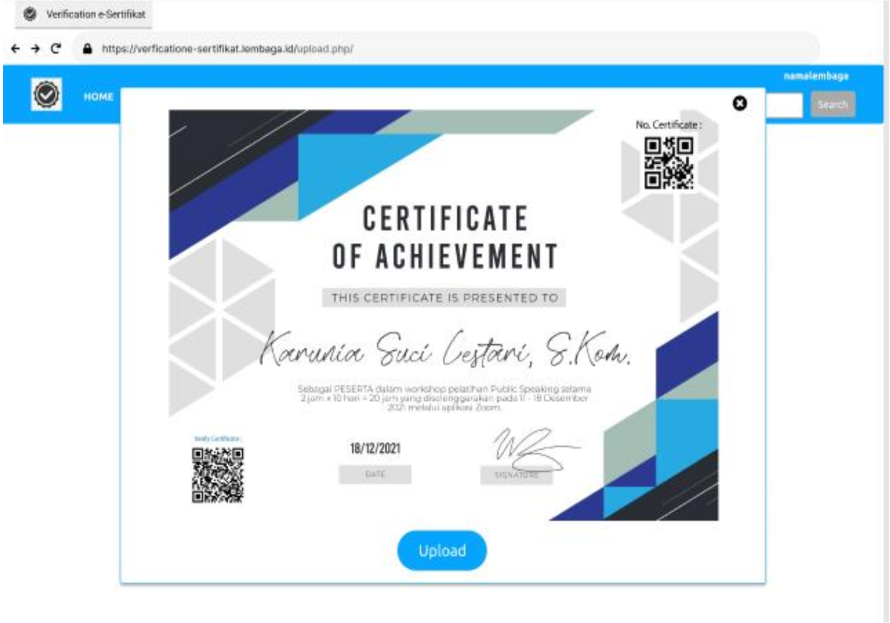


Figure 10. Web Verification and Validation of e-Certificates



Verification e-Sertifikat
https://verficatione-sertifikat.lembaga.id/upload.php/
HOME
namalembaga
Search
No. Certificate :

CERTIFICATE
OF ACHIEVEMENT

THIS CERTIFICATE IS PRESENTED TO

Karunia Suci Lestari, S.Kom.

Sebagai PESERTA dalam workshop pelatihan Public Speaking selama 2 jam x 10 hari = 20 jam yang diselenggarakan pada 11 - 18 Desember 2021 melalui aplikasi Zoom.

Verify Certificate :

18/12/2021

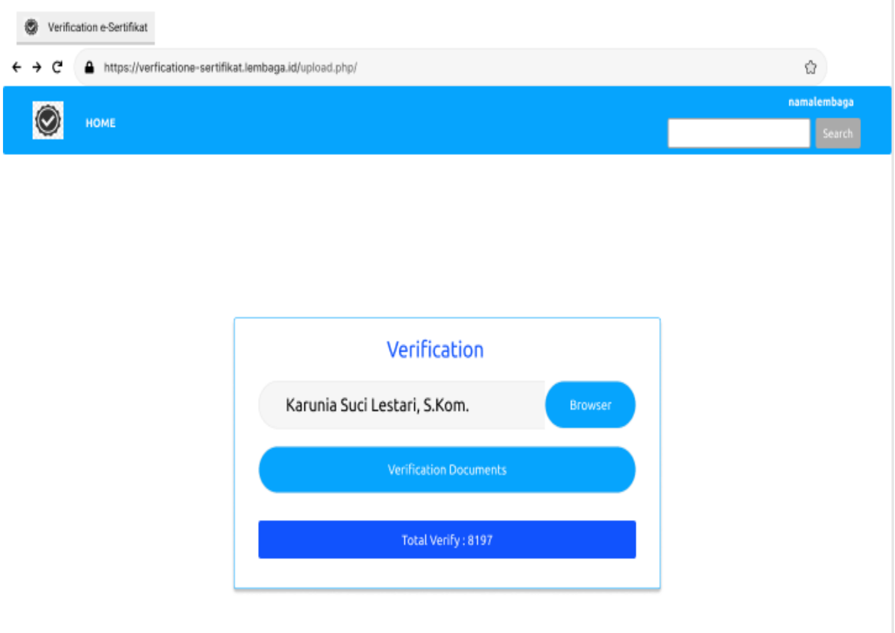
DATE

SIGNATURE

Upload

Figure 11. Upload e-Certificate Document file upload view

A document file upload dialog box will appear such as Figure 11. Once successfully uploaded the Browse column view will change according to the name of the file you want to verify and validate such as Figure 12. Then click the Verification Document. Users have the option of uploading files using PDF format. The results of the upload will display information about blockchain authentication.



Verification e-Sertifikat
https://verficatione-sertifikat.lembaga.id/upload.php/
HOME
namalembaga
Search

Verification

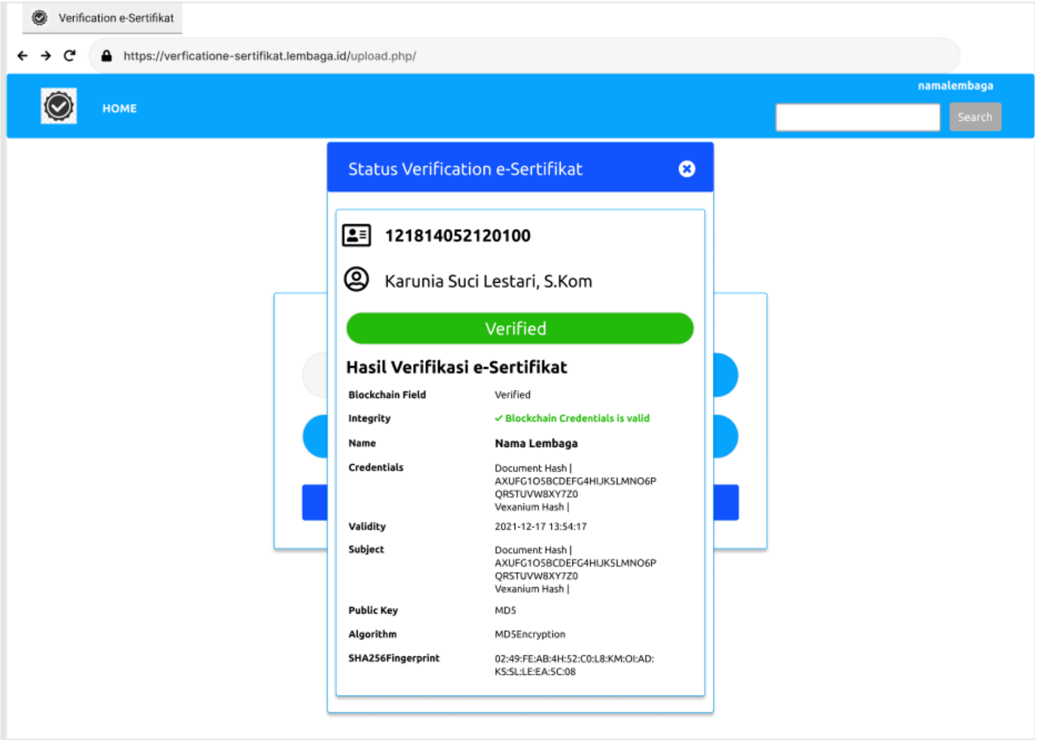
Karunia Suci Lestari, S.Kom.

Browser
Verification Documents

Total Verify : 8197

Figure 12. Prototype Website Verification e-Certificate

If the e-Certificate is declared indeed issued by the Institution, it will appear the verification results with identical greens such as Figure 13. with complete information of the verification results of the document or the e-Certificate is declared Verified. Some of the information that appears includes Credentials, TimeStamp document verification, Public Key and Algorithm used, and hash code of the document.


Verification e-Sertifikat
https://verficatione-sertifikat.lembaga.id/upload.php/
HOME
namalembaga
Search
Status Verification e-Sertifikat

121814052120100

Karunia Suci Lestari, S.Kom

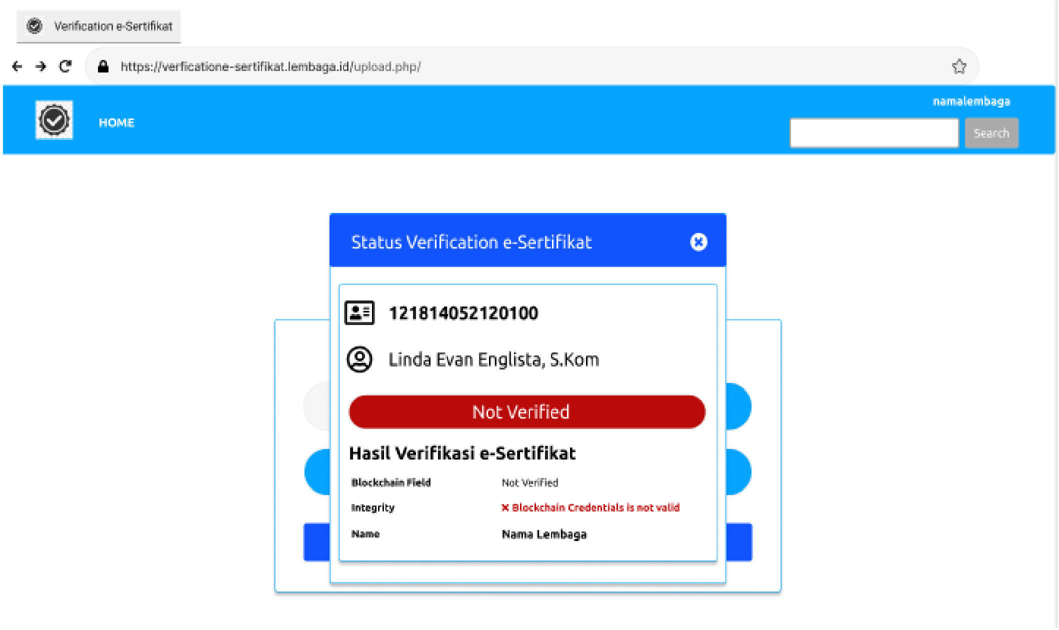
Verified

Hasil Verifikasi e-Sertifikat

Blockchain Field	Verified
Integrity	✓ Blockchain Credentials is valid
Name	Nama Lembaga
Credentials	Document Hash | AXUFG1O5BCDEFG4HIJK5LMNO6P QRSTUVW8XY7Z0 Vexanium Hash |
Validity	2021-12-17 13:54:17
Subject	Document Hash | AXUFG1O5BCDEFG4HIJK5LMNO6P QRSTUVW8XY7Z0 Vexanium Hash |
Public Key	MD5
Algorithm	MD5Encryption
SHA256Fingerprint	02:49:FE:AB:4H:52:C0:L8:KM:OI:AD: KS:SL:LE:EA:5C:08

Figure 13. E-Certificate notifications successfully verified

However, if the e-Certificate is declared or not issued by the Institution, it will appear verification results with identical reds such as Figure 14. with complete verification information from the document or e-Certificate and declared Not Verified.


Verification e-Sertifikat
https://verficatione-sertifikat.lembaga.id/upload.php/
HOME
namalembaga
Search
Status Verification e-Sertifikat

121814052120100

Linda Evan Englista, S.Kom

Not Verified

Hasil Verifikasi e-Sertifikat

Blockchain Field	Not Verified
Integrity	✕ Blockchain Credentials is not valid
Name	Nama Lembaga

Figure 14. E-Certificate notification was not successfully verified or e-Certificate data not found

4. CONCLUSION

The research proposes creating a blockchain-based document verification and validation automation architecture to avoid the falsification of digital assets as a framework for accelerating the digital transformation to secure and maintain data confidentiality in a document. So that validation of a document maintains authenticity. The application of cryptography using the Blockchain method helps to keep our documents secure with a shared storage system and if there are changes or updates only agree if there is mutual agreement and agreement from all parties.

In addition, this architectural model uses Proof of Stake consensus and MD5 encryption in order to shorten the time in distributing a transaction request so that the time in e-certificate verification and validation can be faster. Then the use of QR Code in addition to hiding the encryption of certificate numbers also shortens the time in verification and validation of the e-Certificate. If the e-Certificate is correctly issued by the institution distributing the e-Certificate then a Verified notification appears stating if the e-Certificate is valid, if it is not valid then a Not Verified notification will appear. The notification displayed is quite clear by displaying some information that appears such as Credentials, the institution that distributes e-certificates, TimeStamp document verification, Public Key and explains the algorithm used and the hash code of the document. for future research, it is hoped that pseudocode will be made so that it can be implemented.

5. REFERENCES

[1] *Harefa, N., Gultom, S., & Purba, L. S. L. (2019). Implementasi Webinar Terhadap Sikap Sadar Keamanan Kimia Mahasiswa. Jurnal Dinamika Pendidikan, 12(1), 17-28.*

[2] *Izza, S., Ningrum, B. S., & Hariyati, R. T. S. (2019). Pemanfaatan Webinar Dalam Bidang Keperawatan. Jurnal Penelitian Perawat Profesional, 1(1), 13-20.*

[3] *Rohimat, S., Susilo, D., & Iswarni, I. (2021). Webinar Mengemas Hasil Penelitian Menjadi Artikel Jurnal Ilmiah Untuk Guru Kimia. Abdikarya. Jurnal Pengabdian Dan Pemberdayaan Masyarakat, 3(1), 64-74.*

[4] *Prabowo, E. C., & Afrianto, I. (2017). Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital. Komputa: Jurnal Ilmiah Komputer Dan Informatika, 6(2), 83-90.*

[5] *Rahardja, U., Harahap, E. P., & Christianto, D. D. (2021). Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah. Technomedia J, 4(2), 211-222.*

[6] *Harahap, E. P., Aini, Q., & Anam, R. K. (2020). Pemanfaatan Teknologi Blockchain Pada Platform Crowdfunding. Technomedia Journal, 4(2 Februari), 199-210.*

[7] *Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-Of-Stake Consensus Mechanisms For Future Blockchain Networks: Fundamentals, Applications And Opportunities. IEEE Access, 7, 85727-85745.*

[8] *Vasin, P. (2014). Blackcoin's Proof-Of-Stake Protocol V2. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 71. access on 19 November 2021*

[9] Nugraha, A. C. (2020). *Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan: Studi Kasus Jurusan Teknik Komputer dan Informatika POLBAN.* Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi, 4(1), 15-20.

[10] [Rahardja, U., Harahap, E. P., & Christianto, D. D. (2021). *Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah*. Technomedia J, 4(2), 211-222.

[11] Winarno, A. (2019, April). *Desain E-Transkrip dengan Teknologi Blockchain*. Prosiding Seminar Nasional Pakar (pp. 1-37).

[12] Prawiyogi, A. G., Rahman, R., Sastromiharjo, A., Sulistiawati, S., & Aini, Q. (2021). *Ontologi Blockchain Pada Karya Tulis Puisi Di Pendidikan Sekolah Dasar: Metode Merkle Root.* CSRID (Computer Science Research and Its Development Journal), 13(1), 23-33.

[13] Harahap, E. P., Aini, Q., & Anam, R. K. (2020). *Pemanfaatan Teknologi Blockchain Pada Platform Crowdfunding*. Technomedia Journal, 4(2 Februari), 199-210.

[14] Argani, A., & Taraka, W. (2020). *Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi*. ADI Bisnis Digit. Interdisiplin J, 1(1), 10-21.

[15] Setiowati, D. (2021). *A Blockchain System For Digital Sertificate Verification On E-Learning*. Klik-Kumpulan Jurnal Ilmu Komputer, 8(3), 265-278.

[16] Maulani, G., Gunawan, G., Leli, L., Nabila, E. A., & Sari, W. Y. (2021). *Digital Certificate Authority with Blockchain Cybersecurity in Education*. International Journal of Cyber and IT Service Management, 1(1), 136-150.

[17] Rahardja, U., Aini, Q., Budiarty, F., Yusup, M., & Alwiyah, A. (2021). *Socio-economic impact of Blockchain utilization on Digital certificates*. Aptisi Trans. Manag, 5(2), 106-111.

[18] Yusup, M., Aini, Q., Apriani, D., & Nursaputri, P. (2019, December). *Pemanfaatan Teknologi Blockchain Pada Program Sertifikasi Dosen*. SENSITIf: Seminar Nasional Sistem Informasi dan Teknologi Informasi (pp. 365-371).

[19] Rakhmansyah, M., Rahardja, U., Santoso, N. P. L., Khoirunisa, A., & Faturahman, A. (2021). *Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT*. ADI Bisnis Digital Interdisiplin Jurnal, 2(1), 39-47.

[20] Haryatmi, E. (2021). *Implementasi Teknologi Blockchain Proof of Work Pada Penelusuran Supply Chain Produk Komputer*. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5(3), 446-455.

[21] Rizky, A., Kurniawan, S., Gumelar, R. D., Andriyan, V., & Prakoso, M. B. (2021). *Use of Blockchain Technology in Implementing Information System Security On Education*. BEST Journal (Biology Education, Sains and Technology), 4(1), 62-70.

[22] Augusta, M. O., Syeira, C. P. O., & Hadiapurwa, A. (2021). *Penggunaan Teknologi Blockchain Dalam Bidang Pendidikan*. Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi, 5(2), 437-442.

[23] Husna, M. U., & Dellia, P. (2021). I*mplementasi Blockchain Untuk Optimalisasi Sistem Keamanan Dokumen Transportasi Pada SIM dan STNK*. Jurnal Ilmiah Teknik Mesin, Elektro dan Komputer, 1(1), 1-9.

[24] Lukita, C. (2020). *Penerapan Sistem Pendataan Hak Cipta Content Menggunakan Blockchain*. ADI Bisnis Digital Interdisiplin Jurnal, 1(2 Desember), 40-45.

[25] Hu, S. D. K., Palit, H. N., & Handojo, A. (2019). *Implementasi Blockchain: Studi Kasus e-Voting*. Jurnal Infra, 7(1), 183-189.

[26] Wijaya, I., Haryatmi, E., & Kurniawan, A. B. (2020). *Implementasi Teknologi Blockchain pada Sistem Presensi Staff VM LePKom Berbasis Web*. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5(1), 162-169.

[27] Rahardja, U., Aini, Q., Yusup, M., & Edliyanti, A. (2020). *Penerapan Teknologi Blockchain Sebagai Media Pengamanan Proses Transaksi E-Commerce*. CESS (Journal of Computer Engineering, System and Science), 5(1), 28-32.

[28] Singh, S., Hosen, A. S., & Yoon, B. (2021). *Blockchain Security Attacks, Challenges, And Solutions For The Future Distributed Iot Network*. IEEE Access, 9, 13938-13959.

[29] Agyekum, K. O. B. O., Xia, Q., Sifah, E. B., Cobblah, C. N. A., Xia, H., & Gao, J. (2021). *A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain*. IEEE Systems Journal. doi : 10.1109/JSYST.2021.3076759

[30] Debe, M., Salah, K., Jayaraman, R., Yaqoob, I., & Arshad, J. (2021). *Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices*. IEEE Access, 9, 132875-132887.

[31] Iqbal, M., & Matulevičius, R. (2021). *Exploring Sybil and Double-Spending Risks in Blockchain Systems*. IEEE Access, 9, 76153-76177.

[32] Prabowo, E. C., & Afrianto, I. (2017). *Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital*. Komputa: Jurnal Ilmiah Komputer Dan Informatika, 6(2), 83-90.

[33] Alajrami, E., Ashqar, B. A., Abu-Nasser, B. S., Khalil, A. J., Musleh, M. M., Barhoom, A. M., & Abu-Naser, S. S. (2020). *Handwritten signature verification using deep learning. International Journal of Academic Multidisciplinary Research (IJAMR)*, 3(12).

[34] S. R. M. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "*Security approaches for integrated enterprise systems performance: a review*," Int. J. Sci. Technol. Res., vol. 8, no. 12, pp. 2485–2489, 2019.

[35] Alajrami, Eman; Ashqar, Belal A.M. ; Abu-Nasser, Bassem S.; Khalil, Ahmed J.; Musleh M.; Barhoom, Alaa M. & Abu-Naser, Samy S. (2020) *Handwritten Signature Verification using Deep Learning* International Journal of Academic Multidisciplinary Research (IJAMR)3 (12):39-44.

[36] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). *Proof-Of-Stake Consensus Mechanisms For Future Blockchain Networks: Fundamentals, Applications And Opportunities*. IEEE Access, 7, 85727-85745.

[37] Vasin, P. (2014). *Blackcoin's Proof-Of-Stake Protocol V2*. URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf, 71. access on November, 19th 2021

[38] M. V. X. Ferreira and S. M. Weinberg, "*Proof-of-Stake Mining Games with Perfect Randomness*," *EC 2021 - Proc. 22nd ACM Conf. Econ. Comput.*, pp. 433–453, 2021, doi: 10.1145/3465456.3467636.

[39] J. Spasovski and P. Eklund, "*Proof of stake blockchain: Performance and scalability for groupware communications*," *9th Int. Conf. Manag. Digit. Ecosyst. MEDES 2017*, vol. 2017-January, pp. 251–258, 2017, doi: 10.1145/3167020.3167058.

[40] T. Kerber, A. Kiayias, M. Kohlweiss, and V. Zikas, "*Ouroboros crypsinous: Privacy-preserving proof-of-stake*," *Proc. - IEEE Symp. Secur. Priv.*, vol. 2019-May, pp. 157–174, 2019, doi: 10.1109/SP.2019.00063.

[41] A. Mohammed Ali and A. Kadhim Farhan, "*A Novel Improvement With an Effective Expansion to Enhance the MD5 Hash Function for Verification of a Secure E-Document*," in IEEE Access, vol. 8, pp. 80290-80304, 2020, doi: 10.1109/ACCESS.2020.2989050.

[42] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., & Cao, Y. (2021). *A Survey on Blockchain Technology: Evolution, Architecture and Security*. IEEE Access, 9, 61048-61073.

[43] Singhal, A., & Pavithr, R. S. (2015). *Degree Certificate Authentication Using QR Code And Smartphone*. International Journal of Computer Applications, 120(16).

[44] Husain, A., Bakhtiari, M., & Zainal, A. (2014). *Printed Document Integrity Verification Using Barcode*. Jurnal Teknologi, 70(1). https://doi.org/10.11113/jt.v70.2857

[45] Pal K., Kumar C.R.S. (2021). *QR Code Based Smart Document Implementation Using Blockchain and Digital Signature. In: Sharma N., Chakrabarti A., Balas V., Martinovic J. (eds) Data Management, Analytics and Innovation.* Advances in Intelligent Systems and Computing, vol 1174. Springer, Singapore. https://doi.org/10.1007/978-981-15-5616-6_32

[46] Afrianto, I. R. A. W. A. N., Heryandi, A. N. D. R. I., Finandhita, A. L. I. F., & Atin, S. U. F. A. (2020). *E-Document Authentication With Digital Signature Model For Smart City In Indonesia*. Journal of Engineering Science and Technology, 15, 28-35.

[47] Warasart, M., & Kuacharoen, P. (2012, May). *Based document authentication using digital signature and QR code*. In the 4TH International Conference on Computer Engineering and Technology (ICCET 2012).

[48] D. Pasaribu *and S. Faustina, "Barcoding Digital Signature Authenticity," vol. 5, no. 8, pp. 255–274, 2021.*

[49] M*. T. Scholar, C. Kumar, and A. G. Kumar, "Digital Signature Verification using Support Vector Machine," pp. 4–9, 2020.*

[50] R. Asmara and D. Saputra, "*Perancangan Aplikasi Otomatisasi Penerbitan Dan Pendistribusian E-Sertifikat Webinar*," *J-Click*, vol. 6, no. 2, pp. 201–207, 2019.

[51] *A.I Ardiansyah, M.Syani, and I. Pendahuluan, "Sistem informasi pengolahan sertifikasi berbasis web," J. Masy Inform.Indones., 2017.*

[52] Taş, R., & Tanrıöver, Ö. Ö. (2021). *A Manipulation Prevention Model for Blockchain-Based E-Voting Systems*. Security and Communication Networks, 2021

[53] Febriyanto, E., Triyono, T., Rahayu, N., & Nurbaiti, R. (2020). *QRcode Verifikasi Sertifikat Sebagai Bukti Keabsahan Dokumen dalam Bidang Pendidikan*. Technomedia Journal, 5(1 Agustus), 96-105.

[54] Albar, D., & Perdana, B. F. F. (2021, June). *Designing Digital Certificate Issuance Information System*. IOP Conference Series: Materials Science and Engineering (Vol. 1158, No. 1, p. 012018). IOP Publishing.

[55] Febriyanto, E., Rahardja, U., Faturahman, A., & Lutfiani, N. (2019). *Sistem Verifikasi Sertifikat Menggunakan Qr Code pada Central Event Information*. Techno. Com, 18(1), 50-63.

[56] Munawarah, S. F., Asih, M. S., & Handoko, D. (2020). *Penerapan Sistem Autentikasi Qr Code Dan Hill Cipher Sebagai Pengambil Keputusan Validasi Sertifikat*. Seminar Nasional Teknologi Informasi & Komunikasi Ke-7 (Vol. 1, No. 1, pp. 151-159).

[57] Rahardja, U., Febriyanto, E., & Aldiya, M. A. (2018). *Penerapan Central Event Information Untuk Mencetak Sertifikat dan Verifikasi Dengan QR Code Menggunakan Global Extreme Programming*. Jurnal Informatika Upgris, 4(2).

[58] Suratma, A. G. P., & Azis, A. (2017). *Tanda Tangan Digital Menggunakan QR Code Dengan Metode Advanced Encryption Standard.* Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto), 18(1), 59-68.

[59] Lorien, A., & Wellem, T. (2021). *Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature*. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(4), 663-671.

[60] Ardhianto, E., & Wakhidah, N. (2016). *Pengembangan Metode Otentikasi Keaslian Ijasah Dengan Memanfaatkan Gambar Qr Code.* Jurnal Transformatika, 13(2), 35-41.

[61] Lestari, E. A. P. (2020). *Kajian Perlindungan E-Payment Berbasis Qr-Code dalam E-Commerce*. Jurnal Penelitian dan Pengembangan Sains dan Humaniora, 4(1), 28-36.

[62] Saputro, W. T., Widatama, K., & Ardiansyah, I. (2021). *Pengembangan Sistem Informasi Presensi Mahasiswa Memanfaatkan Teknologi QR-Code*. INTEK: Jurnal Informatika Dan Teknologi Informasi, 4(2), 91-100.

[63] Qashlim, A., & Hasruddin, H. (2015). *Implementasi Teknologi QR-Code Untuk Kartu Identitas*. Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar, 1(2), 1-6.

[64] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "*Untangling Blockchain: A Data Processing View of Blockchain Systems*," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[65] Jayesh G. Dongre, "*Education Degree Fraud Detection and Student Certificate Verification using Blockchain*," *Int. J. Eng. Res.*, vol. V9, no. 07, pp. 300–303, 2020, doi: 10.17577/ijertv9is070156.

[66] Rahardja, U., Hidayanto, A. N., Putra, P. O. H., & Hardini, M. (2021). *Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol*. Journal of Applied Research and Technology, 19(4), 308-321.

[67] R. Suganya, R. A. Jothi, and V. Palanisamy, "*Retina based authentication for E-voting system using MD5 algorithm*," vol. 4, no. 4, pp. 4–7, 2018.

[68] H. W. Dhany, F. Izhari, H. Fahmi, M. Tulus, and M. Sutarman, "*Encryption and Decryption using Password Based Encryption, MD5, and DES*," vol. 141, no. ICOPOSDev 2017, pp. 278–283, 2018, doi: 10.2991/icoposdev-17.2018.57.

[69] L. B. De Guzman, A. M. Sison, and R. P. Medina, "*MD5 secured cryptographic hash value*," *ACM Int. Conf. Proceeding Ser.*, pp. 54–59, 2018, doi: 10.1145/3278312.3278317.

[70] D Rachmawati et al 2018 J. Phys.: Conf. Ser. 978 012116