Bit-Tech (Binary Digital - Technology)
Vol.6, No.3, April 2024
Available online at: http://jurnal.kdi.or.id/index.php/bt

Implementation of Diploma and Transcript Verification System on the Ethereum Blockchain Network

Intan Anjali Putri[1)], Aditiya Hermawan[2)*], Ardiane Rossi Kurniawan Maranto[3)]

[1)2)3)]*Universitas Buddhi Dharma*
Jl. Imam Bonjol No.41 Karawaci, Tangerang, Indonesia
[1)]intan.anjaliputri@ubd.ac.id
[2)]aditiya.hermawan@ubd.ac.id
[3)]ardiane.rossi@ubd.ac.id

Article history:

Received 22 April 2024;
Revised 23 April 2024;
Accepted 25 April 2024;
Available online 30 April 2024

Keywords: {use 5 keywords}

Blockchain
Ethereum
Transcript Value
Smart Contracts
Verification of Diplomas

Abstract

Blockchain, a decentralized database safeguarded by cryptographic security, has gained prominence for its resistance to manipulation. Its application extends notably to ensuring the security of financial transactions, including the acquisition of digital currencies. This study endeavors to develop a system aimed at validating diplomas and academic transcripts, enhancing their authenticity and bolstering the security of document storage. Leveraging the Ethereum Blockchain and Smart Contracts, the methodology focuses on the utilization of specialized codes executed within the Ethereum network. The outcome of this research manifests as a system blueprint designed for the verification of diplomas and transcripts, integrated within a web-based Ethereum Network platform. By harnessing the Ethereum Blockchain's inherent security features and employing Smart Contracts, the proposed system endeavors to streamline the verification process, ensuring the integrity and reliability of academic credentials while fortifying document storage against potential breaches. Through this innovative approach, the study contributes to advancing the authentication and security standards within the realm of academic documentation management. The integration of Blockchain technology in academic credential verification offers a tamper-proof and transparent solution, ensuring trust and reliability in the verification process. This technological advancement holds the potential to revolutionize academic credential authentication, providing a robust and immutable framework for verifying educational qualifications.

I. INTRODUCTION

Degrees and grade transcripts are essential documents issued by educational institutions, serving as formal proof of an individual's educational completion. A degree not only signifies the accomplishment of a course of study but is also a prerequisite when applying for employment after finishing education at a school or college. Unfortunately, the escalating forgery of these documents poses a serious threat, deemed an unlawful act [1].The incidence of forgery is on the rise, especially during the 2019 General Election, as informed by Nuril Furkan, Head of the HKLI Division at Ditjen Belmawa [2]

Currently, the verification of the authenticity of degrees and grade transcripts is challenging, particularly with the presence of the Electronic Degree Verification System (SIVIL), which has not fully addressed data security issues [3]. Previous research has attempted to integrate Blockchain technology to tackle this issue, such as the authentication of degrees at Al-Zaytoonah University, Jordan, by T. Kanan [4] or the addition of QR codes to degree certificates by [5]. Nevertheless, the implementation of Blockchain technology in Indonesia's SIVIL is still limited.

This study proposes an innovative solution by leveraging Blockchain technology, particularly Ethereum Blockchain, to create a verification and storage system for degrees and grade transcripts. Through the implementation of Solidity-based smart contracts, this research aims to enhance the security, transparency, and distribution of academic data. The primary goal is to provide a more advanced solution to the high rate of document forgery, improve the integrity of academic data, and simplify the process of verifying the authenticity of degrees and grade transcripts. In the context of the education sector, the issuance of degrees and grade transcripts by educational institutions is a crucial requirement reflecting the academic achievements of students

ISSN 2622-2728 (online) 2622-271X (print)
doi: 10.32877/bt.v6i3.1288

or scholars. However, these documents are susceptible to forgery, creating uncertainty regarding the integrity and authenticity of academic data.

The current challenges involve the difficulty of verifying the authenticity of degree and grade transcript documents, amidst the increasing rate of forgery. Although there have been efforts, such as the Electronic Degree Verification System (SIVIL) [3], data security remains a challenge, leaving room for fraud. Several studies have attempted to address this issue by implementing Blockchain technology. T. Kanan [4] introduced degree authentication using Blockchain at Al-Zaytoonah University, Jordan. The research [5]added QR codes to degree certificates and scanned serial numbers through a website. However, the implementation of Blockchain in Indonesia's SIVIL is still limited.

Corresponding author

The innovation in this research involves the utilization of Blockchain technology, particularly Ethereum Blockchain, to create a verification and storage system for degrees and grade transcripts. By employing Solidity-based smart contracts, this research aims to enhance data validation and transactions on the Ethereum network, increase transparency, and secure stored data. With this approach, the study seeks to address the issue of degree and grade transcript forgery through a more innovative and distributed solution.

This research has the main objective of creating an innovative system for verifying and storing degrees and grade transcripts using Blockchain technology, focusing on the implementation of Ethereum Blockchain and Solidity-based smart contracts. The aim is to address the high rate of degree and grade transcript forgery, provide a distributed security solution, and improve the integrity of academic data. By presenting a more sophisticated solution, this research is expected to fill knowledge gaps related to degree verification, answer previously unanswered questions, and positively contribute to increasing confidence in the validity of academic documents.

II. Related Works/Literature Review

A. Blockchain

Blockchain can be referred to as distributed accounting technology which is a concept in which the parties that join a distributed network have the right to access the accounting [6]. Blockchain is a rule that aims to know a structure and division of data or can also be called a data structure that allows to create a digital book of data and share data in a network [6]. This concept is used in bitcoin which is at the same time the answer to the problem of the absence of third parties to build trust between parties. Blockchain technology can be compared to a distributed database where information is recorded and stored and shared with every party involved in the network.
Types of blockchain that exist today include public blockchain, permissive blockchain, and private blockchain [7]. The three types of blockchain use a cryptography that allows any party to manage the data or the big books in a secure way without involving a third party.

B. Advantages and How Blockchain Works

The superiority of blockchain technology [8], [9] lies in several aspects. Firstly, it organizes information chronologically, ensuring that any modifications do not overlap with previous data. Secondly, it instills trust through a verification process conducted by multiple computers. Each data entry necessitates validation from one of the computers within a block, fostering reliability. Thirdly, it eliminates intermediaries in transactions, resulting in reduced administrative costs, particularly evident in interbank transactions where third-party involvement is unnecessary. The functioning of blockchain [9] involves distributing a general ledger across a network of computers for verification. Each computer maintains a ledger recording all network transactions, with verified data stored in blocks. These blocks are then permanently linked in a chain, connecting preceding and succeeding transactions. There is no centralized server overseeing transactions; instead, each block requires verification and must meet specific criteria. Additionally, each block contains cryptographic hashes, facilitating data retrieval from previous blocks and serving as a compact string to detect potential data sabotage.

C. Smart Contract and Ethereum

Smart Contract according [10] is a special logic or code used and executed in the Ethereum virtual environment. Smart Contracts are rules of transactions that are digitized and encoded between accounts, helping in transferring digital assets among accounts. Smart contracts can store data, stored data can be used to record information, facts, balances, and other information necessary to apply logic in real-world contracts.

According to [11]Etherum is an open-source platform and distributed on the basis of blockchain technology, generally ethereum is a transaction machine. Ethereum has all the features of the public blockchain like public/private key encryption, cryptography hash function, Merkle tree, and hard/soft fork, etc. The primary purpose of ethereum according to [10] is to accept transactions from the account and update its status as well as maintain its status until other transaction to be re-updated. The entire process of acceptance, execution, and transaction writing can be divided into two phases in ethereum. There's a separation between when transactions are received by Ethereum and when the transaction is executed and written into the ledger.

D. Solidity

Solidity is a programming language that targets the Ethereum Virtual Machine (EVM). The ethereum blockchain helps expand its functionality by writing and executing code known as smart contracts. Solidity is a programming language that is very similar to JavaScript. Similarities between JavaScript and C can be found in Solidity.

E. Metamask and Ether.js

Ethers.js is a MIT licensed Ethereum library that is compact, fully functional and has been extensively tested and has received DevEx grants from the ethereum foundation for expansion and maintenance [12]. Metamask is the oldest and most widely used decentralized application in the ethereum network. Metmask is an extension of the chrome application, and serves to store Ether [13]. The website application will run using the Metamask browser, which is where metamask serves as a bridge between the web app and the Ethereum blockchain [14].

III. METHODS

The research methods are also used in the creation and development of web sites for verification of degrees and transcripts of values, i.e. using the Software Development Life Cycle (SDLC) method.

A. *Data Collection*

1) *Questionnaire*
   This is done by making a list of questions to other people about the system that has been created. The aim is to find out the results of the diploma and transcript verification system that has been created. The questionnaire is used to gather feedback from users regarding the conducted research. The questionnaire is distributed to the HRD department, responsible for employee recruitment, and the Academic Affairs Office (BAA) as administrators.

2) *Literature Review*
   This is done by reading and studying books, articles, the internet, journals and materials from various other sources related to research.

B. Software Development Life Cycle (SDLC)

The System Development Life Cycle (SDLC) is an attempt to design a system that will always move like a wheel, passing through several steps or stages among other stages of investigate, analyze, design, implementation and maintenance [15]

1) *Planning Stages*
   The earliest stage that can be used to develop a new information system or system change is identifying the potential, problems and opportunities that exist in research on certificate and transcript verification systems. In this case, various information will be collected to assist in this research.
2) *Phase of analysis*
   In analyzing the system under development, a thorough identification of potential system weaknesses will be conducted. Additionally, the methods to be employed within the system will be studied in detail to ensure their effectiveness and accuracy of implementation. The focus will also be on the performance of the system, identifying factors that can affect responsiveness, speed, and reliability. Furthermore, additional information will be sought regarding issues related to the research.
3) *Design Stages*
   The system design will be created in the form of wireframe designs to be presented as the website design to be implemented. This stage involves determining the overall structure of the web pages, including the layout of main elements such as the header, navigation menu, main content, and footer. Each section of the website will be detailed in the wireframe, including the placement of buttons, forms, images, and text. This wireframe layout will provide a clear visual representation of how users will interact with the website, ensuring an intuitive and efficient user experience.
4) *Implementation Stages*
   The implementation of the website design and the development of the blockchain system will be carried out with the assistance of Solidity programming language for creating Smart Contracts, as well as HTML, CSS, JavaScript, and PHP programming languages. The system will utilize experimental networks using extensions or Metamask plugins. This stage involves coding and developing applications that integrate the designed website layout with blockchain system functionalities.
5) *Maintenance Stages*
   Evaluate the results of the research conducted. It is used to determine the level of user satisfaction in using applications that are created and used as system development materials.

C. Blockchain Method

The research will create a certificate verification website and transcribe values using the blockchain method using the ethereum network as the storage of the data. Ethereum is useful for running Smart Contracts that can implement blockchain technology. The code that will be generated during the storage will be displayed in the degree document and value transcripts through the QR code, so that users who want to verify the authenticity of the document can do it easily.

Blockchain can be referred to as distributed accounting technology which is a concept in which the parties that join a distributed network have the right to access the accounting [6]. Blockchain is a rule that aims to know a structure and division of data or can also be called a data structure that allows to create a digital book of data and share data in a network [6]This concept is used in bitcoin which is at the same time the answer to the problem of the absence of third parties to build trust between parties. Blockchain technology can be compared to a distributed database where information is recorded and stored and shared with every party involved in the network.
Types of blockchain that exist today include public blockchain, permissive blockchain, and private blockchain [7]. The three types of blockchain use a cryptography that allows any party to manage the data or the big books in a secure way without involving a third party.

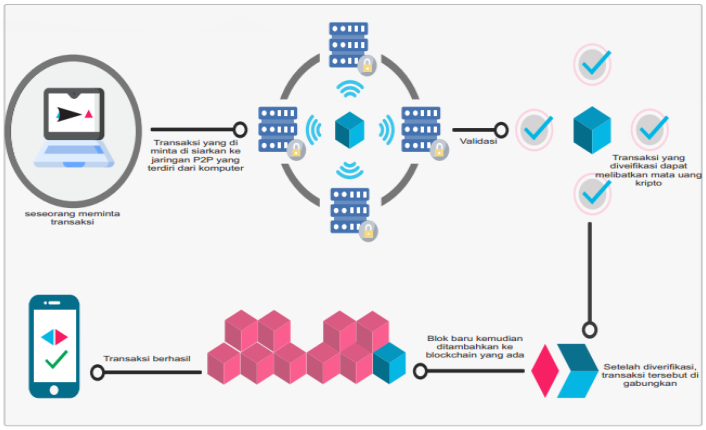

Fig 1 How Blockchain Works [9]

IV. RESULTS

Based on what has been submitted, it is necessary to have a system design that will be made according to the needs of the system.

A. Plan and Analysis

In the initial Planning Stages, the primary objective is to lay a solid groundwork for the research on the certificate verification system and transcript of values. This phase involves a meticulous approach towards identifying potential issues, problems, and opportunities that may significantly influence the development and effectiveness of the system.

1) Issue Identification

In the planning stages, various challenges and potential issues have been identified for the development and implementation of the certificate verification system and transcript of values. The detailed documentation of these challenges includes technical, logistical, and procedural aspects. These challenges encompass ensuring the seamless integration of the system, addressing potential logistical bottlenecks, and defining clear procedural guidelines for efficient execution. Categorizing these challenges provides a roadmap for developing effective mitigation strategies to overcome hurdles.

2) Opportunity Exploration

While identifying challenges, the planning stages have also focused on exploring opportunities for enhancing and improving the current certificate verification system and transcript of values. Opportunities include streamlining the verification process, incorporating innovative technologies like blockchain for increased security, and optimizing logistical workflows. This exploration aims to leverage potential areas for improvement to make the system more robust, efficient, and user-friendly.

3) Information Gathering

The planning stages involve extensive information gathering from diverse sources to establish a solid foundation for the research on the certificate verification system and transcript of values. This comprehensive data collection includes insights from relevant literature, questionnaires distributed to potential users, and an in-depth study of existing systems. The goal is to gather varied perspectives, technical requirements, and user expectations to inform the subsequent phases of analysis and design effectively.

B. Design

In the Design phase, the comprehensive set of functional and non-functional requirements, derived from the thorough analysis and refinement process, forms the basis for creating a systematic and user-centric blueprint for the certificate verification system. The key aspects addressed in this phase include:

1) Blockchain Integration

Within the Design phase, a meticulous plan is devised to strengthen the security of the certificate verification system, focusing on the integration of blockchain technology. Specifically, this plan corresponds to the development of a comprehensive flowchart outlining the systematic process of entering data into the blockchain can be see in 2. The intricacies of this flowchart include strategic measures to securely store and safeguard data, ensuring the integrity and immutability of verified records. By aligning the design strategy with a detailed flowchart, the system's architecture for entering data into the blockchain becomes transparent, allowing for a clear visualization of the steps involved in enhancing security standards and incorporating decentralized ledger systems. This systematic approach positions the certificate verification system as not only robust in security but also as a transparent and technologically advanced solution in the realm of academic credential verification.

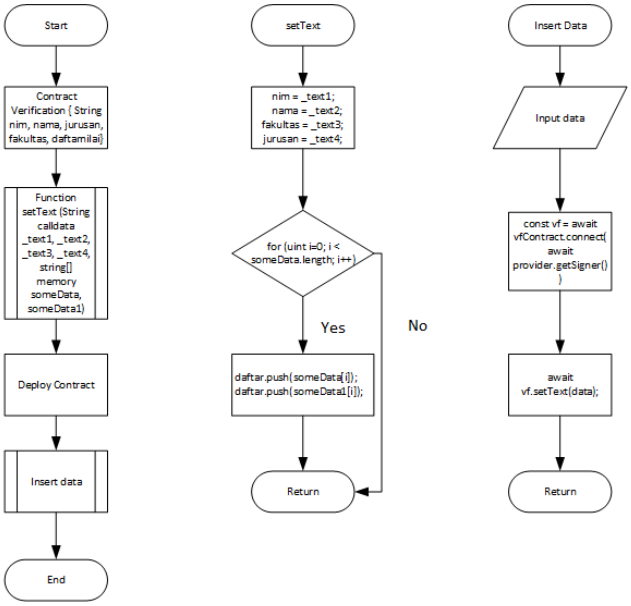

Fig 2 Flowchart of the System for Entering Data into the Blockchain

2) Database Design

Efficient data management is pivotal for the system's success. The database design phase involves structuring a well-organized database schema that accommodates diverse data types, facilitates quick searches, and supports the seamless import of student grades and other relevant information.

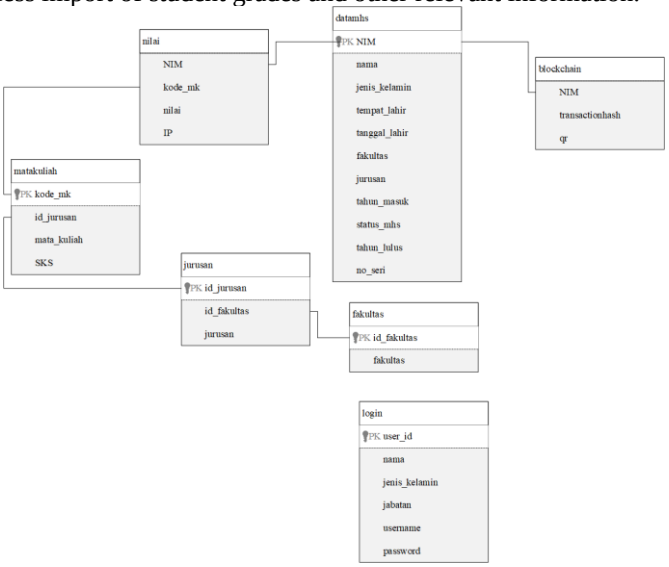

Fig 3 Entity Relationship Diagram

3) Wireframing

The system design is visually represented through wireframes, providing a skeletal structure of the website. These wireframes serve as a visual guide for the placement of various elements, ensuring alignment with user expectations and the overall system requirements.

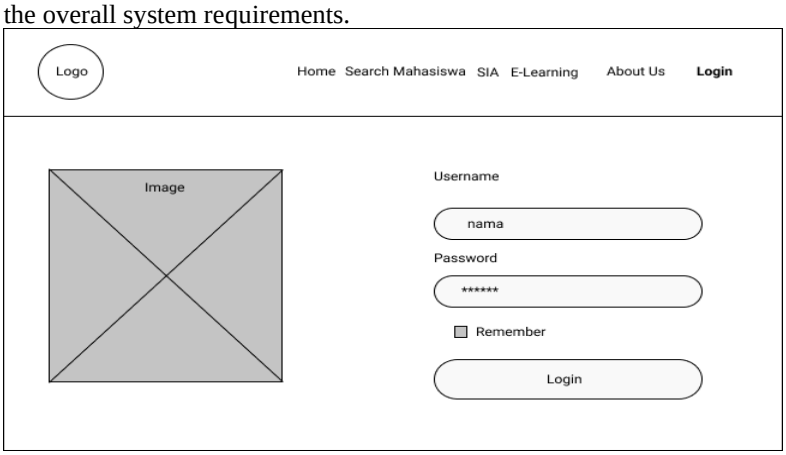

Fig 4 Admin Login Screen Design

C. Implementation

Data storage into the blockchain is on the “blockchain” menu where there is a “connect wallet” button that is useful for connecting a “metamask” wallet (containing ethereum balances) used to carry out storage in the blockchain. When the admin presses the "connect wallet" button, it will display the "metamask" application to enter the password first. For example, see in Fig 5

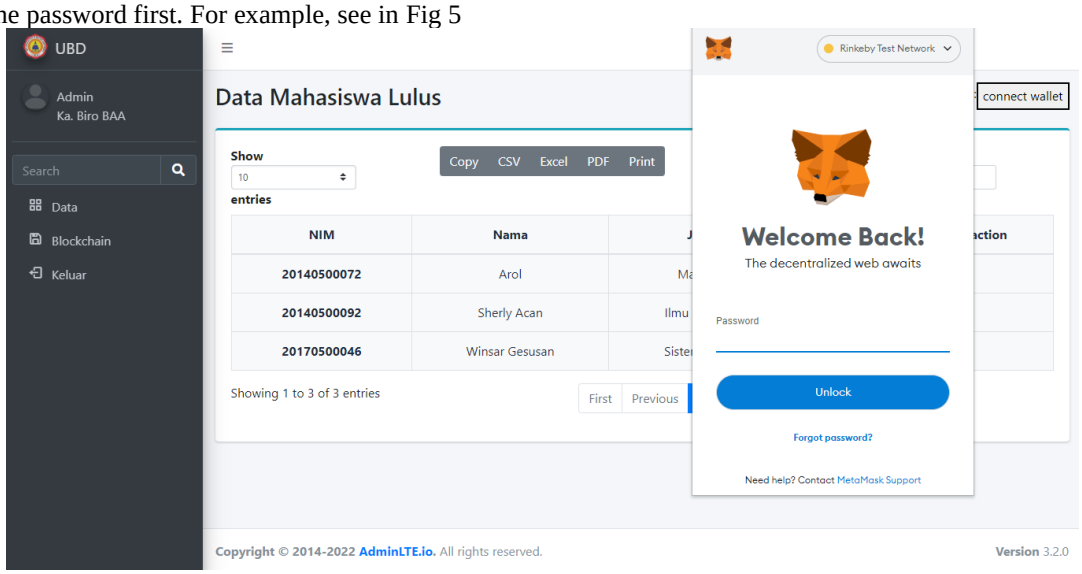

Fig 5 Metamask Login View

After entering the password, a digital wallet containing the ethereum balance will be opened. The wallet can be connected to the website by using the code as shown in Fig 6

```
async function connect(){
    await ethereum.request({ method: 'eth_requestAccounts' });
    provider = new ethers.providers.Web3Provider(window.ethereum);
    account = await provider.getSigner().getAddress()
    document.getElementById("welcome").innerText += account
    document.getElementById("wallet").classList.add("invisible");
    vfContract = new ethers.Contract("0x1202CFc27F99d0D62c0Dc5F90c60F758Fd844f1A",abi,provider)
}
```

Fig 6 Connect Wallet Code

Storing data into the blockchain can use buttons on the action column. See Fig 8

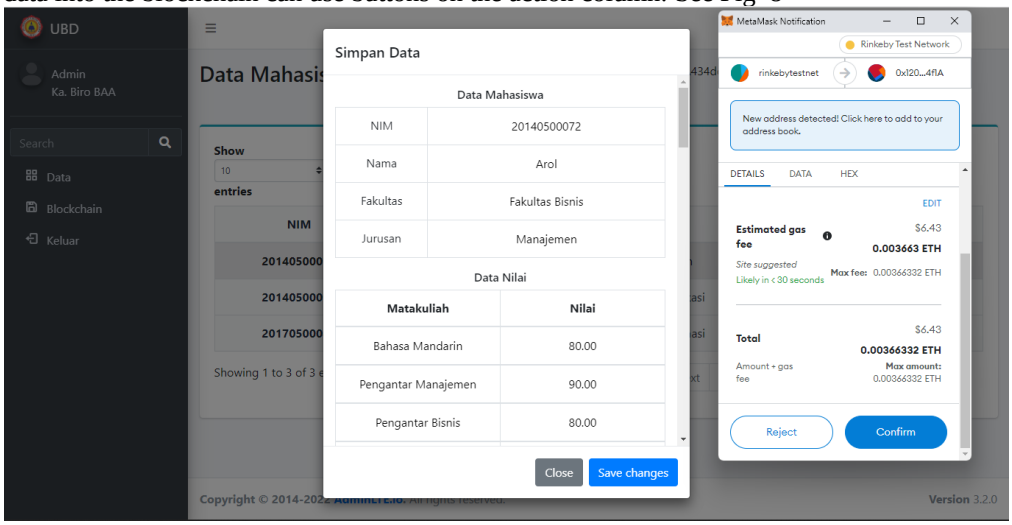

Fig 7 Blockchain Dialog Box

The administrator can press the "Save Changes" button to do the data storage, but must first make sure the data is correct and valid. If so, then the metamask dialog box will appear to make the transaction payment. The cost of each ethereum transaction can be determined by the density of the network, where the more transactions are made, the more the costs will go up. The fee is called the "Gas Fee", which is paid with the ethereum balance. Once the data is verified, you can immediately press the “confirm” button on the “metamask” to make the payment and process the transaction. If a transaction has been processed then a processed transaction notification will appear and can be viewed on the Etherscan website.

The creation of smart contracts to carry out storage into the blockchain can be seen in Fig 8 8

```
//SPDX-License-Identifier: MIT
pragma solidity 0.8.4;

import "hardhat/console.sol";
contract verification{
    string public nim;
    string public nama;
    string public jurusan;
    string public fakultas;
    string[] daftar;

    function setText(string calldata _text1, string calldata _text2, string calldata _text3, string calldata _text4, string[] memory someData,string[] memory someData1)external{
        nim = _text1;
        nama = _text2;
        fakultas = _text3;
        jurusan = _text4;
        for (uint i=0; i < someData.length; i++) {
           daftar.push(someData[i]);
           daftar.push(someData1[i]);
        }
    }
}
```

Fig 8 Smart Contract Code

Fig 9 Smart contracts that have already been saved and deployed need to be integrated into the front end of the website in order to perform data storage .

```
if(vfContract!=null){
const textvalue = nimEdit;
const textvalue1 = namaEdit;
const textvalue2 = fakultasEdit;
const textvalue3 = jurusanEdit;
var daftarMatkul = [], nilaiMatkul = [];
var matkuls = $('.matkul'+nim).map((_,el) => el.value).get()
var nilais = $('.nilai'+nim).map((_,el) => el.value).get()


var daftarMatkulNilai = []
var daftarMatkul = []
var daftarMatkulNil = []

for (let i = 0; i < matkuls.length; i++) {
  // daftarMatkulNilai[i] = [matkuls[i], nilais[i]]
  daftarMatkul[i] = matkuls[i];
  daftarMatkulNil[i] = nilais[i];

}
// console.log(daftarMatkul)
// console.log(daftarMatkulNil)

const transkripnilaimatkul = daftarMatkul;
const transkripnilainilai = daftarMatkulNil;

// // console.log(matkuls,nilais)
  const vf = await vfContract.connect(await provider.getSigner())
  await vf.setText(textvalue,textvalue1,textvalue2,textvalue3,transkripnilaimatkul,transkripnilainilai);
```

Fig 9 Save to Blockchain Code

The result of the data storage like Fig 10 into the blockchain can be viewed on the Etherscan Rinkeby website by performing a search using a hash transaction.

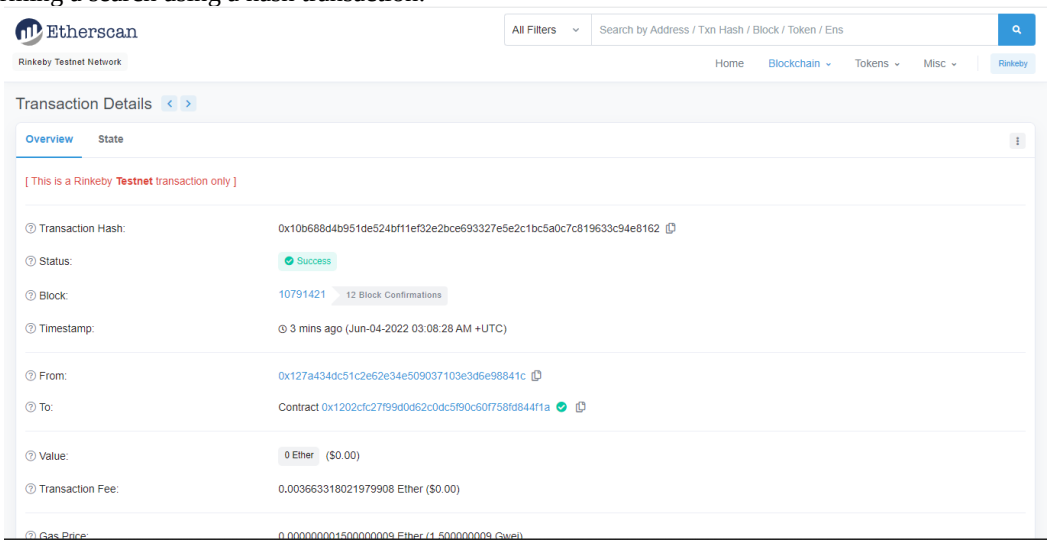

Fig 10 Etherscan View

Fig 11 will display a number of menus that are accessible to users and scanners to be used by users to check the degree data of graduate students of Buddhi Dharma University.

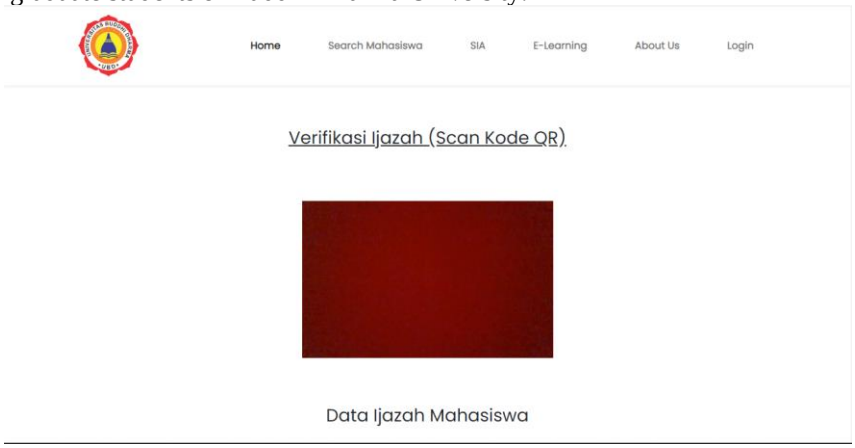

Fig 11 Verification Page View

When a user scans a QR code, the website displays the data according to the QR code being scanned. The data displayed is student data (NIM, name, faculty, major, year of admission, graduation year) and student overall grade transcript data.

V. DISCUSSION

The certificate verification and transcription system with blockchain technology has been fully implemented. Users can now easily verify the authenticity of data using the QR code embedded in each issued degree. However, the system still relies on experimental data, requiring refinement to enhance user-friendliness through the website.

The process of storing student data in the blockchain has been meticulously organized to ensure data security and authenticity. Only data of graduated students will be stored in the Ethereum blockchain. By storing data in the blockchain, the information is distributed and its security is guaranteed, given the potentially large amount of student data. The presence of data in the blockchain also makes data manipulation more difficult.

The website development for this system was carried out using the Solidity programming language for smart contract creation. Ethereum Remix was utilized as a tool in the development process of smart contracts. Additionally, data in this system is also stored in a local database as temporary storage using MySQL, an open-source application of the Relational Database Management System (RDMS). This approach allows for more flexible and efficient data management while maintaining the security of data authenticated by the blockchain[16].

VI. CONCLUSIONS

Based on the research conducted on the creation of a degree verification system and transcript of records using blockchain technology, several important conclusions can be drawn. The system that has been built is capable of certifying degrees and displaying student transcript data through the blockchain network effectively. The use of blockchain technology in data storage proves to be highly suitable for this purpose due to the high level of security it offers. Furthermore, the use of QR codes in the certification process has facilitated system usage, accelerated verification processes, and enhanced trust in the authenticity of the data. Thus, this system can provide significant benefits to companies or educational institutions in verifying degrees and student transcript data. However, it is important to note that the use of blockchain technology also comes with costs. Each data storage transaction in the Ethereum network incurs a fee determined by network congestion, known as a gas fee. Therefore, companies or educational institutions need to consider these costs when using the system. Additionally, a limitation to be noted is the inability to modify data once it is stored in the blockchain. Although data can be replaced with new data, this underscores the importance of ensuring data accuracy before storing it in the system. Overall, this research demonstrates that the use of blockchain technology in degree verification and transcript of records systems has the potential to enhance security and efficiency in the process. However, careful consideration needs to be given to costs and potential technical limitations that may arise from its use.

REFERENCES

[1] U. Rahardja, E. P. Harahap, and D. D. Christianto, “Pengaruh Teknologi Blockchain Terhadap Tingkat Keaslian Ijazah,” *Technomedia Journal*, vol. 4, no. 2, 2020.

[2] Al-Basith, “Waspadai Ijazah Palsu, Subbagian Hukum Ditjen Belmawa Selenggarakan Sosialisasi.,” lldikti13 Kemendikbud.

[3] Kemendikbud, “SIVIL:Sistem Verifikasi Ijazah secara Elektronik,” https://ijazah.kemdikbud.go.id/.

[4] Nero Chaniago, “Blockchain dan Smart Contract untuk Keamanan Dokumen Elektronik: Studi Kasus Ijazah dan Transkrip,” 2020.

[5] K. and A. S. and J. H. Khandelwal Harshita and Mittal, “Certificate Verification System Using Blockchain,” in *Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies*, S. and K. A. and G. X.-Z. and M. S. Gunjan Vinit Kumar and Senatore, Ed., Singapore: Springer Singapore, 2020, pp. 251–257. doi: 10.1007/978-981-15-3125-5_27.

[6] R. C. Noorsanti, H. Yulianton, and K. Hadiono, *Blockchain-Teknologi Mata Uang Kripto (Crypto Currency)*. 2018.

[7] “Blockchain_For_Dummies”.

[8] M. Oka Augusta, C. Putriana Oktaviandi Syeira, A. Hadiapurwa, and K. Kunci, “Penggunaan Teknologi Blockchain Dalam Bidang Pendidikan,” vol. 437, no. 2, 2021, [Online]. Available: https://digitalcredentials.mit.edu

[9] H Purwantoro and M Y Wibowo, *Teknologi Blockchain dan Cara Kerjanya*. APTIKOM, 2020.

[10] R Modi, *Solidity Programming Essentials 1st ed*. 2018.

[11] G. Zheng, L. Gao, L. Huang, and J. Guan, *Ethereum Smart Contract Development in Solidity*. Singapore: Springer Singapore, 2021. doi: 10.1007/978-981-15-6218-1.

[12] Andreas M Antonopoulos and Dr Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps 1st Edition*, 1st ed. O’Reilly Media, 2018.

[13] J. Haritsah, A. Budiyono, and A. Widjajarto, "Analisis Proses Sistem Untuk Implementasi Interplanetary File System (Ipfs) Pada Smart Contract Ethereum System Process Analysis For Implementation Of Interplanetary File System (Ipfs) In Smart Contract Ethereum."
[14] F. Aprialim, Adnan, and A. W. Paundu, "Penerapan Blockchain dengan Integrasi Smart Contract pada Sistem Crowdfunding," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 1, pp. 148–154, Feb. 2021, doi: 10.29207/resti.v5i1.2613.
[15] D. Abdullah, *Merancang Aplikasi Perpustakaan Menggunakan SDLC*. 2017.
[16] M. Huda, *Bootstrap 4: Belajar CRUD Menggunakan PHP dan MySQL*.