International Journal of Innovative
Computing, Information and Control
Volume **18**, Number **5**, October **2022**

 ISSN 1349-4198
pp. **1601–1615**

SECURITY ANALYSIS OF PRIVATE BLOCKCHAIN IMPLEMENTATION FOR DIGITAL DIPLOMA

Arya Wicaksana* and James Christian Wira

Department of Informatics
Universitas Multimedia Nusantara
Jl. Scientia Boulevard, Gading Serpong, Tangerang 15810, Indonesia
james.wira@student.umn.ac.id
*Corresponding author: arya.wicaksana@umn.ac.id

Received April 2022; revised July 2022

Abstract. *Bachelor's diplomas are the most frequently forged documents, followed by high-school diplomas. The document is vital for admission, hiring, and citizenship, and the digital version allows easy access and uses, although it suffers from forgery and falsification. The establishment of blockchain technology enables the creation of diplomas as digital assets and the distribution of them confidentially and securely through a peer-to-peer network. This study aims to develop an application that utilizes a private blockchain for creating digital assets based on diplomas and storing, distributing, and managing them. Blockchain Lisk is chosen in this study with the Delegated Proof of Stake consensus protocol for implementing the application as a proof-of-concept. Actual diplomas from Universitas Multimedia Nusantara (UMN) are used in this study to design, implement, test, and evaluate the application. Evaluation of the security aspect of the application is measured using computer security base metrics: the common configuration scoring system (CCSS). This study shows that private blockchain technology stores distribute and manage diplomas securely and at no cost by eliminating fees and incentives. The actual security level of the application at UMN scored using CCSS obtained a BaseScore of 3.3, categorized as low vulnerability severity.*
Keywords: CCSS, Digital diplomas, DPoS, Lisk, Private blockchain, Security

1. **Introduction.** Bachelor's diplomas are the most frequently forged documents, followed by high-school diplomas. The illicit activities related to this forgery range from candidates who have never taken education, dropped out, have not graduated, grade point average (GPA) forgery, transcript forgery, and degree forgery [1]. The physical version of diplomas can be faked for the benefit of malicious parties [2]. The harms caused by these illicit activities are costly to interested parties in the diploma [3]. Physical diplomas can also be lost or destroyed because of human negligence, theft, and even natural disasters. The process and cost of verifying the authenticity of diplomas are lengthy and costly [4]. Thus, works on digital diplomas with additional security measures, i.e., blockchain, are ways to tackle the problem [4-9].

Digital diplomas are exposed to threats similar to any other digital documents. The blockchain distributed ledger technology is suitable for storing and distributing diplomas transparently and securely [10-12]. Blockchain technology, i.e., non-fungible tokens (NFT), creates a digital version of the diploma uniquely and securely. In addition to that, an additional consensus protocol ensures that only certified original diplomas exist on the blockchain. This whole concept makes diplomas forgery very difficult to afford. Another

DOI: 10.24507/ijicic.18.05.1601

obvious advantage of using blockchain is its immutable ledger, thus ensuring the integrity of the diplomas in the blockchain network for all parties [13].

Universities worldwide worked on this problem by utilizing blockchain for digital diplomas as studied in [4], which most are still conceptual or pilot projects. Most blockchain technologies used for digital diplomas are Bitcoin and Ethereum. These underlying technologies are limited to certain aspects, Bitcoin is Blockchain 1.0 with its sole purpose of being a cryptocurrency (electronic payment), and Ethereum 1.0 suffers from high transaction fees [14]. Public blockchain also relies on validators to run the application in demand for incentives. Private blockchain with the support of smart contracts and affordable transaction fees is needed for the problem. One related work used Hyperledger Sawtooth to develop a decentralized application for storing digital certificates (diplomas) [8]. The results indicate that Hyperledger Sawtooth is a transparent, secure, decentralized application able to store digital diplomas, and the application relies on validators.

There are two contributions of this study. The first is the implementation of the private blockchain Lisk as a digital diploma repository to create digital assets (the digital diplomas) and store, distribute, and manage them. Lisk allows developers to build applications on the sidechain, giving flexibility and privacy to the blockchain environment and eliminating the cost of validators' incentives. The second contribution is the security analysis of the application, which is measured using the common configuration scoring system (CCSS) based on the common vulnerability scoring system (CVSS) [15]. The idea of incorporating new technology, i.e., private blockchain for the digital diploma application, has to fit into today's security standards. This study also provides users with the interface to use the application using Web 3.0 and the application is developed and tested by using actual diplomas from Universitas Multimedia Nusantara.

The rest of this paper is organized as follows. Section 2 briefly describes the preliminaries related to the study. Section 3 describes the research methods. Section 4 explains the results and discussion. Finally, Section 5 concludes this paper with some suggestions for future work.

2. **Preliminaries.**

2.1. **CCSS metrics.**

The common configuration scoring system (CCSS) is a set of measures of the severity of software security configuration issues published by the Computer Security Division of Information Technology Laboratory at the National Institute of Standards and Technology (NIST). The security metric of CCSS used in this study is the BaseScore, formulated based on Base Impact (I) and Base Exploitability (E).

Definition 2.1. *The base equation does not include two base metrics: Exploitability Method and Privilege Level. The f(Impact) = 0 if Impact (I) = 0, 1.176 otherwise. The calculation of BaseScore is done by calculating the Exploitability (E), Impact (I), and f(Impact) [15].*

$$BaseScore = round\_to\_1\_decimal(((0.6 * I) + (0.4 * E) - 1.5) * f(I)) \tag{1}$$

Impacts are divided into confidentiality (ConfImpact), integrity (IntegImpact), and availability (AvailImpact) impacts. ConfImpact (CI) measures the potential impact of confidentiality if the exploit is successful. The score on the CI is divided into none, partial, and complete. A score of none means there is no impact on system confidentiality, and a partial score means some information is out or has access that it should not have. The complete score means that information is open and visible to individuals or groups who do not have rights. Integrity Impact (II) measures the potential impact on the system's integrity if the exploitation is successful. IntegImpact (II) score is divided into none,

partial, and complete. A score of none means no integrity impact on the system, and a partial score means the modification of configuration or information can occur. The complete score means the system's integrity is compromised, and an attacker can make complete changes to the system. AvailImpact (AI) measures the potential availability impact if the exploitation is successful. The AI score is divided into none, partial and complete. A score of none means there is no impact on system availability. A partial score means reduced system performance, but the system can still run. A complete score means the system is not available [15].

Definition 2.2. *The following is the formula to calculate Impact (I). CI means ConfImpact. II means IntegImpact. AI means AvailImpact [15].*

$$I = 10.41 * (1 - (1 - CI) * (1 - II) * (1 - AI)) \tag{2}$$

Exploitability has AccessVector (AV), Authentication (Au), and AccessComplexity (AC) properties. The AV metric measures the level of access required to be able to perform configuration exploits. The parameters are local, adjacent network, and network. Local means exploitation can be done by physically gaining system access. Adjacent network means exploitation can be carried out by gaining access to the local network via Bluetooth, wireless network, or local Ethernet. Network means that exploitation can be done with access outside the local network. The Au measures how much authentication is required to be able to perform an exploit. These metric measurements are multiple, single, and none. Multiple means a security loophole requires two or more authentications. Single means the vulnerability requires one authentication. None means that the vulnerability does not require authentication. The AC measures the difficulty of access required to perform an exploit, and this metric is divided into high, medium, and low. High means that access to exploits is quite tricky, i.e., gaining privileges, and medium means that access is not too easy but still requires searching for more information. Low means quickly obtaining access [15].

Definition 2.3. *The following is the formula to calculate Exploitability (E). AV means AccessVector. Au means Authentication. AC means AccessComplexity [15].*

$$E = 20 * AV * Au * AC \tag{3}$$

Calculations of BaseScore, Impact, and Exploitability are completed using scores described in Table 1. The scoring is defined in the CCSS document published by NIST [15]. The valuation of the BaseScore interprets the severity of exploitation on the application, and the details are given in Table 2 [16].

2.2. **Lisk blockchain.** Lisk is a blockchain application platform that can be used to develop blockchain applications using the software development kit (SDK) that is already available. The SDK on the Lisk framework is written using the JavaScript programming language. Lisk has its token used in its ecosystem called Lisk (LSK). Lisk does not use ledgers [17].

The consensus algorithm used is Delegated Proof of Stake (DPoS). DPoS is a consensus algorithm used to maintain valid agreements across the network, validate transactions, and act as a form of digital democracy. As a form of democracy, there are elections in DPoS. Elections are made to determine the delegate. Delegates (representatives) are account types registered using a delegate registration transaction. This selection distinguishes DPoS from ordinary PoS (proof of state). The more coins a stakeholder has, the more that stakeholder is likely to create new blocks in the blockchain [18], while in DPoS, delegates function to create the next block, validate the block, and insert the block into the blockchain. Block entry into the chain is done by default every 10 seconds. This

Table 1. Base equation of CCSS scoring

Metric		Parameter	Score
Impacts	ConfImpact (CI)	none	0
		partial	0.275
		complete	0.66
	IntegImpact (II)	none	0
		partial	0.275
		complete	0.66
	AvailImpact (AI)	none	0
		partial	0.275
		complete	0.66
Exploitability	AccessVector (AV)	requires local access	0.395
		adjacent network accessible	0.646
		network accessible	1
	Authentication (Au)	requires multiple instances of authentication	0.45
		requires single instance of authentication	0.56
		requires no authentication	0.704
	AccessComplexity (AC)	high	0.35
		medium	0.61
		low	0.71

Table 2. The national vulnerabilities database (NVD) severity ratings

Severity	Base score range
none	0.0
low	0.1-3.9
medium	4.0-6.9
high	7.0-8.9
critical	9.0-10.0

activity continued until the last delegate. When the last delegate has finished creating a block, a loop is successfully executed, and the next round is executed from the original delegate. Delegates who successfully create blocks will receive incentives [17].

Each token holder (stakeholder) can choose a representative. Stakeholders can vote using a vote transaction. Representatives have the role of generating blocks and validating transactions. As long as the blockchain network is still running, voting can be done by stakeholders. The change of a stakeholder into delegates depends on the number of votes it receives in the network. Lisk requires 101 active delegates to secure the consensus, not to include delegates who are actively processing transactions. Lisk has basic (default) transactions that each has their purpose. Lisk uses a configuration file to define and manage the blockchain, and Lisk provides a sample configuration file. The configuration manages three parts: apps, components, and modules [17].

3. **Methods.**

3.1. **Requirement analysis.** Based on the analysis carried out, the following are the main requirements of the application.

1) Storage must be secure and transparent.
2) Diplomas can be accessed by the public as long as they have the ID of the diploma.
3) Blockchain technology is used to store UMN diplomas.
4) Application development requires an interface so that users can interact with the blockchain.
5) The data contained in the diploma is the name, unique student number, place and date of birth, study program, faculty, degree obtained, UMN internal diploma number, National Diploma Numbering (PIN), date of diploma, date, and place where the diploma was given, and student photo.
6) Diplomas are made after students fulfill the SKKM (Student Activity Credit Unit) points and complete compulsory courses, internships, theses, and student administrations.

3.2. **System architecture.** The system architecture is made to be semi-decentralized. The nature and requirement of the application do not require a fully decentralized architecture for creating, storing, distributing, and managing digital diplomas. The semi-decentralized architecture allows certain aspects of the process to be controlled and run by the university, which ensures integrity and saves costs by eliminating the need for giving out incentives to validators. Meanwhile, the ledger is distributed across the blockchain network and accessible via the Web 3.0 interface. The configuration is designed to restrict connections of blockchain nodes only from designated parties: the Bureau of Academic Information (BIA) at UMN, which can be adjusted to certain parties in the institution or organization. The API access can only be done through the web applications to ensure limited access and tighten security policy.

This study uses the default genesis block provided by Lisk regarding the genesis block. Lisk runs with the Javascript programming language. Thus, interface applications can be made into a website directly. This web page will connect the user with the Lisk server. The connection between the two is made using the API that Lisk has provided, and the server will return data to the user, which will eventually be processed to display the data. Figure 1 displays the complete architectural design of the digital diplomas application.

3.3. **Database design.** The database only stores login information (email and password), user roles, diploma ID, and diploma status. This information is used by the web application to accelerate processes, i.e., displaying digital diplomas and verifying digital diplomas. The diploma details are committed to the blockchain. The database design is created with an entity-relationship diagram, as shown in Figure 2.

3.4. **Application flow.** There are three types of users: public, university, and alumni. Public users are restricted from viewing diplomas unless they provide the application with the diploma identification number. This number is given by the university and stored in the blockchain and the database. Public users could input the identification number in the web application to search for the diploma. The application searches the identification number in the database and continues retrieving the data from the blockchain if there is one that matches the identification number. Public users could view the retrieved information with the digital diploma on the web application. This guarantees the authenticity and originality of the digital diploma for the public (companies, institutions, and governments).

The university acts as the administrator of the application and the blockchain network. Lisk blockchain mandates 101 delegates for the consensus protocol to take place, and the delegates could be wholly run by the university as proposed in this study to eliminate

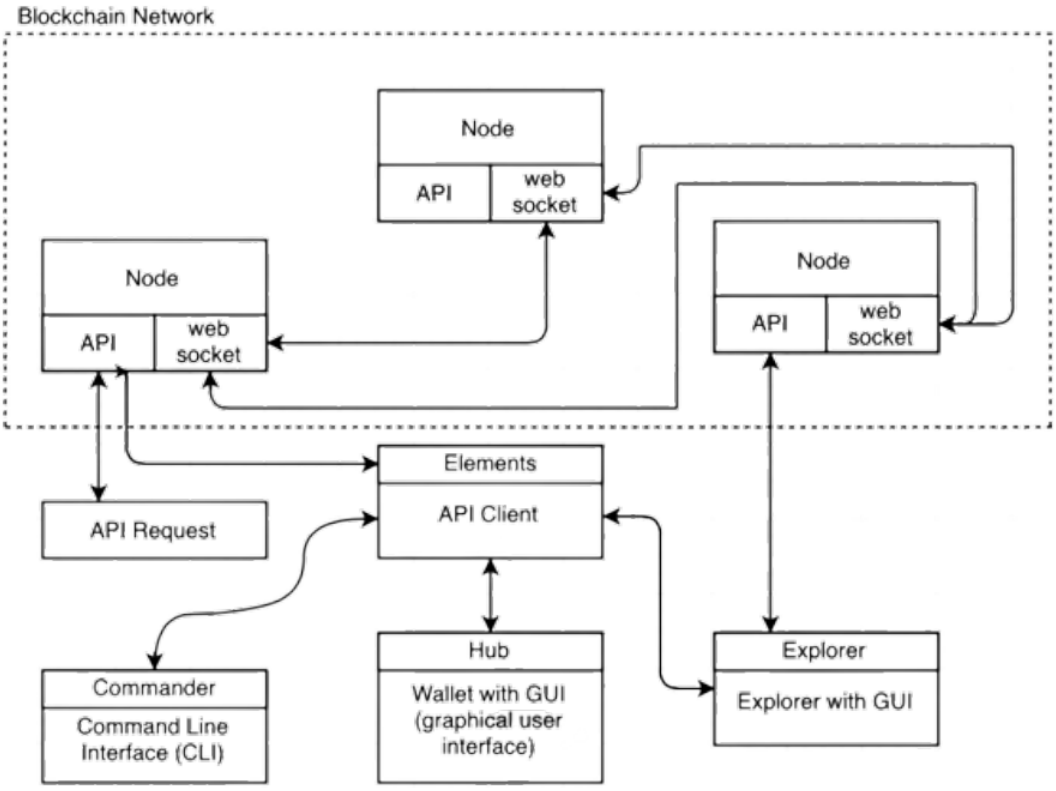

FIGURE 1. System architecture

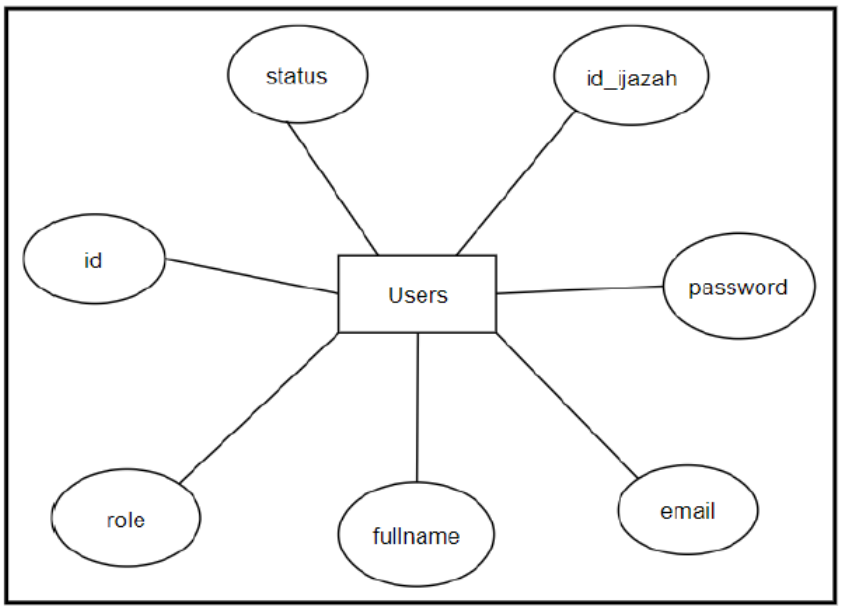

FIGURE 2. Entity relationship diagram (ERD)

incentives. In another scheme, this could be expanded to allow external parties to contribute to the consensus by becoming the 101 delegates. The role of the administrator in the digital diplomas process is to create digital diplomas and store them in the blockchain.

The alumni are users who had pre-registered accounts on the web application to use this application. These users can access their diploma directly without inputting the diploma identification number. Instead, they get the information of their diploma and

identification number from the application. Both the university and alumni are required to log in to the application. Meanwhile, the public users do not have to log in or register to the application to verify the digital diplomas they intended to.

3.5. **Implementation.** The process begins with installing the PostgreSQL inside the Docker. This is the database that is used and linked to the Lisk blockchain. Next, a file to accommodate transactions for the digital diplomas is created. In this file, there are settings to set the transaction type and the transaction cost. TYPE is used to set the transaction type, and FEE is used to set the transaction cost. The number 20 in TYPE is a custom-made type for diploma transactions, and the fee for making transactions for diplomas is 0.

The Lisk API is made inaccessible to outsiders by setting the IP address used to access the API to be the same as the computer's local IP. This forbids external access that is not coming from the university network. This policy adds trust and security to the application due to alumni accessing the Lisk API from the university's local area network. This process requires their students' identification and password, which are given by the university, ensuring the process's integrity.

Adding delegates to Lisk cannot be done arbitrarily and only by the department that handles diplomas at the university. In this study, the university is Universitas Multimedia Nusantara (UMN), and the related department is the Bureau of Academic Information (BIA). This setting is set by default in the Lisk's configuration file by not setting a public static IP but with a local IP. This setting is done in the server configuration file of Lisk.

The configuration block is also set in the same configuration file. The block configurations that can be set manually are BLOCK_TIME, MAX_TRANSACTIONS_PER_BLOCK, and REWARDS (MILESTONES, OFFSET, and DISTANCE). The block configuration uses the default configuration and is described in Figure 3.

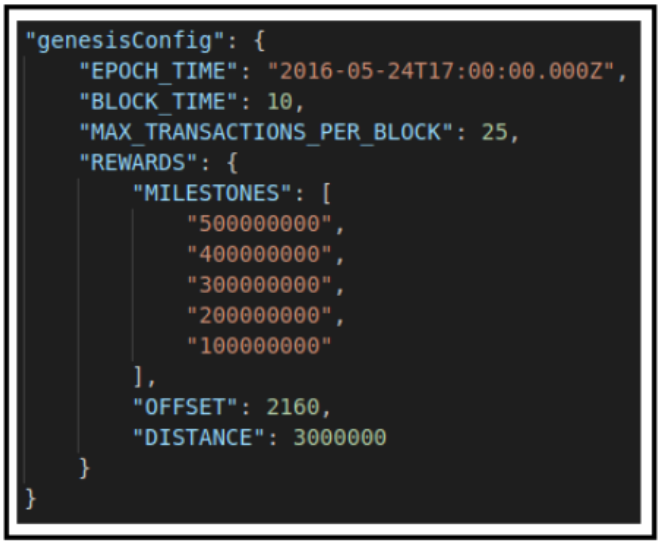

FIGURE 3. Block configuration

BLOCK_TIME is the time it takes to create a block. MAX_TRANSACTIONS_PER_BLOCK is the maximum number of transactions in a block. MILESTONES are rewards that are received by the delegate who created the block. OFFSET determines when a delegate receives a reward. OFFSET is calculated from the height of the chain. DISTANCE is the distance between milestones. DISTANCE is also calculated from the height of the

chain. The creation of the genesis block uses the example from the Lisk SDK and does not make any changes.

3.6. **Application testing.** Testing is carried out by experimenting with the generated diplomas. The number of inputs is carried out in units (1 diploma) and large quantities simultaneously (10 and 100). The implementation test is declared successful if the diploma is successfully added to the blockchain and the alumni account is created. The first test is to input diploma data on the Diploma Input page. Figure 4 shows the implementation result of the web application for the input page to add new diplomas.

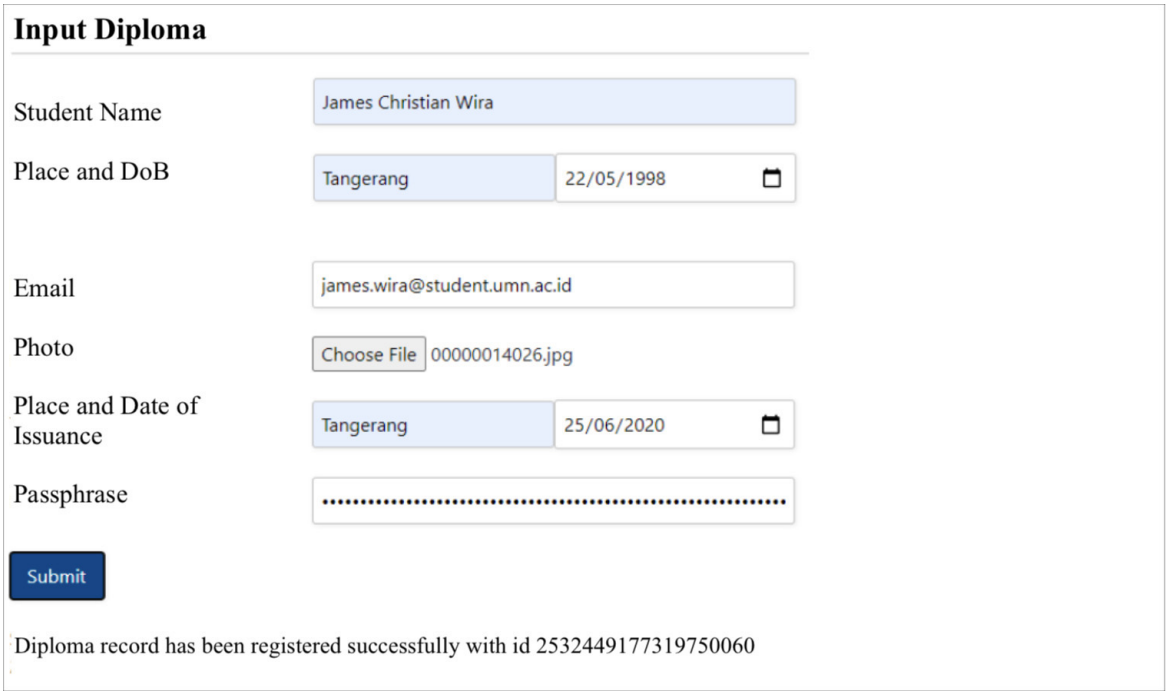

FIGURE 4. Input page for adding new diploma

The Submit button is used to send the diploma. Diplomas are sent in the form of Lisk transactions. If the diploma is successfully entered, there will be a sentence stating that the diploma has been successfully entered into the blockchain and the alumni account has been created in the MySQL database. Figure 5 shows the log on the blockchain when the diploma transaction is sent.

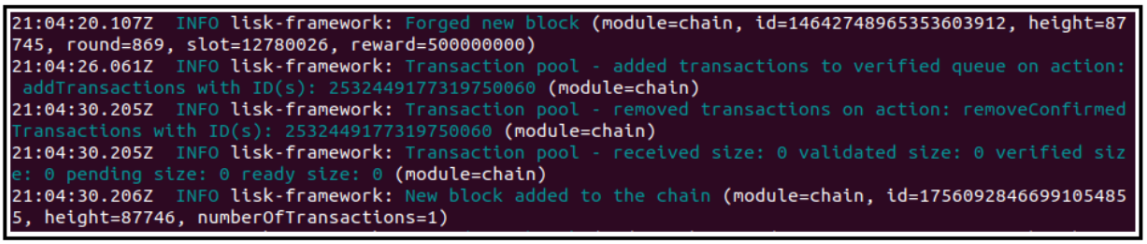

FIGURE 5. Log when transaction is sent

In Figure 5, it can be seen that the last block is created at the 20th second. Diploma transactions are accepted and entered into the transaction pool on the 26th second. At the 30th second, a new block is created with a number of transactions of 1. The block is then added to the chain. That is, the diploma transaction is successfully entered into the

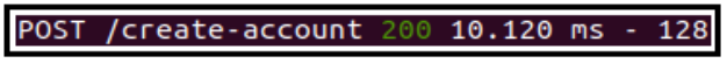

FIGURE 6. Backend logs when transactions are submitted

id	role	fullname	email	password	id_ijazah	status
1	admin	Admin BIA	admin.bia@umn.ac.id	5d2c85dab165392d0650861c40a0712d		0
22	student	James Christian Wira	james.wira@student.umn.ac.id	4027416c087a667a514513d7ef35df3a	2532449177319750060	1

FIGURE 7. Records in the database after the transaction is sent

blockchain. Then check the backend to find out if the alumni account has been created. Figure 6 shows the result of the log on the backend when the transaction is submitted.

The backend returns a response code of 200, meaning an alumni account is already created in the database. Figure 7 shows the content of the database after new accounts are generated.

The second and third tests enter 10 and 100 diplomas, respectively. The data used is random data whose contents follow the data on the diploma. The creation and entry of diplomas into the blockchain and database are assisted with a button. Not all generated digital diplomas (transactions) are immediately inserted into a block, and each block holds only 25 transactions following the blockchain configuration. Thus, the remaining transactions in the transaction pool are added to the next block after 10 seconds. The tests are carried out successfully, proving the functionalities of the application.

3.7. **Security analysis.** The CCSS scoring of the application aimed to measure the security level of the designed and implemented digital diplomas application based on private blockchain Lisk. In this study, the security evaluation is carried out under the actual condition of the application implementation for Universitas Multimedia Nusantara.

4. **Results and Discussion.** The interface used is ReactJs as a framework for the web application. Using ReactJs requires only NodeJs, and NodeJs itself is installed along with Lisk's installation. Based on the design, 8 web pages are developed: Initial Display as shown in Figure 8, After Login (2 views), Input Diplomas, All Diplomas, Search Diplomas, and Diplomas.

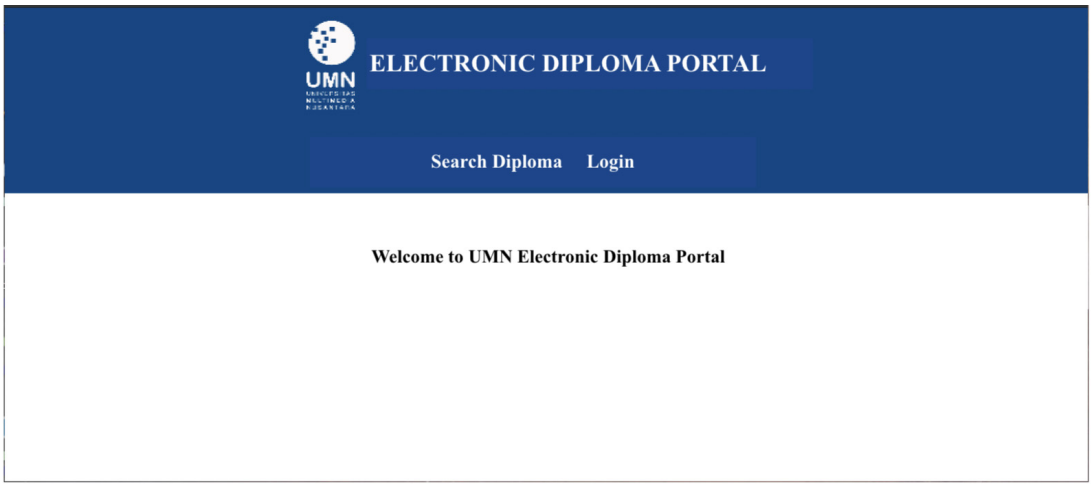

FIGURE 8. Initial view of the web application

When the web application is opened, the application displays the initial screen and checks the email contained in the browser cookie. If there is no email, the page displays the Search Diploma and Login menu, whereas if there is an email, the page displays a menu according to the role of the email. The roles in question are admin and student (alumni). The next screen is the search page. This page is used to search for diplomas contained on the blockchain.

The search page only accepts input in the form of ID from the diploma. The ID is used to search for diplomas on the blockchain. The search for diplomas is carried out after searching for a diploma before submitting it. The previously entered ID will search for diplomas using the API shown in Figure 9.

A successful search process displays the diploma and related data, as presented in Figure 10. At the bottom, there is also a button to download the diploma in PDF form. Diplomas in PDF are created using HTML, with the data overwritten using placeholders.

```
api.transactions.get({ id: this.state.idIjazah })
    .then( response => {
        if(response.meta.count === 0){
            this.setState({values: false})
        } else {
            this.setState({values: response.data[0].asset});
        }
    })
```

FIGURE 9. Coding the API to search for diplomas

FIGURE 10. The diploma page

FIGURE 11. Sample of the downloaded diploma file

The creation of this PDF file type is assisted by "react-pdf". Figure 11 displays a sample of a downloaded file that presents the actual diploma of alumni from UMN.

The university user role has a different role from alumni, so the menu owned by university users is different. The All Diplomas menu displays the All Diplomas page, which aims to display all diplomas that the university (UMN) has awarded. Diploma data retrieval begins by retrieving all diploma identification numbers (IDs) from the database using the "getCert.js" router. All IDs received are then searched to the blockchain with an API (same as looking for diplomas). When displaying diplomas, not all data is displayed. Only data related to alumni and UMN is displayed, i.e., name, NIM, study program, faculty, UMN diploma number, national diploma number, status, and actions.

There are additional features, namely filters. The filters provided are filters based on faculty and based on study programs. There are 2 buttons in the action section: Activate/Deactivate and View. The Activate/Deactivate button changes the diploma status from Active to Inactive and vice versa. The status change process is carried out using the "certificateAction.js" router. The View button is used to view diploma details.

The Diploma Input menu displays the Diploma Input page, aiming to enter diploma data into the blockchain. The data needed to be entered into the blockchain are name, NIM, place, date of birth, education level, faculty, study program, degree, UMN diploma number, national diploma number, date of national diploma, student email, student photos, place and the date the diploma was awarded, and the passphrase. The passphrase is used to sign a block. A transaction object is created after BIA has completed filling in the data. This transaction object is included in a block. Then, the block is spread across the network.

CCSS scoring. The security analysis is evaluated under the actual existing condition of the application implementation at Universitas Multimedia Nusantara (UMN). The data stored in the database is limited to user account details and diploma identification

numbers. The details of the diplomas are stored in the blockchain. The data stored in the database are amendable, requiring administrator privilege, while the data stored in the blockchain are immutable. The availability of the web application is subject to an attack on the web server, i.e., a denial-of-service attack (DoS). At the same time, the blockchain network consists of hundreds of delegates run by the university. Access to the application is divided into two paths: external and internal. External access is for public users, allowing access from the Internet. Internal access requires users, i.e., university administrators and alumni, to join the university's local area network (LAN) to access the application. Authentications are required to access sensitive information stored within the application, i.e., the database and blockchain. This is achieved by implementing indirect multilevel authentication: physical access to the LAN, university official email account, application login credentials, and administrator privilege. These combinations intensify the complexity of exploiting the application. Based on the evaluation of the actual condition, Table 3 summarizes the CCSS scoring.

Table 3. Evaluation results of Exploitability and Impact

Metrics	Evaluation	Score
ConfImpact	partial	0.275
IntegImpact	none	0
AvailImpact	partial	0.275
AccessVector	local	0.395
Authentication	multiple	0.45
AccessComplexity	high	0.35

The ConfidentialityImpact (ConfImpact) metric is "partial" due to the nature of the partially confidential diploma to a certain degree. Upon successful exploitation, the digital diplomas are accessible by the attacker, eliminating confidentiality. However, the information presented in the diplomas is general and could not be used solely to commit other illicit activities. Even the information written in the diplomas does not carry personal properties. On the configuration side, no root-level access is given to any of the users.

The IntegrityImpact (IntegImpact) metric is "none" due to the immutable permanent ledger of the blockchain technology. Even when the configuration file is exposed and exploited, the data on the blockchain cannot be altered. Adding false diplomas to the blockchain also requires administrator privilege and has to break through the consensus protocol. Given the actual circumstances, it is almost impossible to impersonate a valid user with an administrator level.

The AvailabilityImpact (AvailImpact) metric is "partial" due to the nature of the web server that could suffer from denial-of-service (DoS) and other attacks to disrupt the availability nature of the application. However, the blockchain network runs on multiple nodes (decentralized), making it highly challenging to shut down all nodes simultaneously. Configuration settings can be exploited, but the outcome is not necessarily disrupting availability as the blockchain network nodes are wholly controlled and coordinated by the university. Thus, making a fork of the corrupted blockchain and recovering the configuration file along with closing the vulnerability are immediately done by the administrator without compromising availability.

The AccessVector (AV) metric is "local" due to the fact that the degree of access needed to exploit the application requires direct access that is only available through the web application. Direct access to the blockchain network through the application programming interface (API) requires a connection to the local network on which the

blockchain network is running. It is impossible to exploit the application outside the local area network (LAN). The Authentication (Au) metric is "multiple" due to four instances, as described earlier, mandating the authentication process directly or indirectly to exploit the application. The AccessComplexity (AC) is "high" due to the facts of the application's multilevel authentications, architectural design, and blockchain technology.

The BaseScore valuation of the application is $3.29733495 \approx 3.3$ "low severity", with the Base Impact score being 6.34359375, the Base Exploitability score being 1.24425, and the f(Impact) is 1.176. This BaseScore means that if the application is attacked and successfully exploited, the security risk and loss is 33%. This scoring is subject to the actual condition of the application implementation at Universitas Multimedia Nusantara with the established policy and supporting system settings. Security devices, i.e., firewalls and intrusion prevention systems (IPS), exist on the university network. The flow's design and nature of the application flow mandate the users' physical presence that could be exploited to carry out destructive attacks. Public users' access is limited to the functionalities provided by the web application interface. In addition, the policy of creating and inserting a digital diploma into the application requires multilevel authentication, i.e., physical presence and access to the BIA administrator's computer at the university. The government issues this digital diploma identification number upon official request from the university, which carries specific characteristics, in addition to the wet signatures from the dean and rector.

5. Conclusions.

This study demonstrates the implementation of a private blockchain for digital diplomas with actual data at Universitas Multimedia Nusantara (UMN). This study's main contribution is exploring using a private blockchain to create, store, distribute, and manage digital diplomas and the security analysis of the design and implementation carried out. The blockchain network is protected from direct access via a centralized web and database server that acts as the gateway. This adds the security perimeter necessary to mitigate the blockchain network's exploitation risks. The application's security is studied and measured following industrial standard CCSS from NIST. The security metrics analysis focuses on the vulnerabilities of the application configuration related to confidentiality, integrity, and availability.

The test shows that the design and implementation of the digital diplomas application are successful under actual data and environment at UMN. The security analysis shows that the CCSS BaseScore of the application is 3.3, which means low vulnerability severity. This study also shows the different approaches to merging centralized servers with distributed ledger technology (blockchain) to eliminate fees and incentives. The developed application is functionally working and could process digital diplomas at UMN, and the content of the diplomas is also standardized in Indonesia. Thus, other universities could use this application with minor changes to the PDF template of the diploma. Suggestions for future works based on this study's findings are as follows.

1) Evaluate the application performance based on parameters, i.e., number of transactions in a block, block creation time, and the number of transactions in the pool. Performance is an essential factor for computer applications. Adding heavy security measures could lead to a low-performance system.
2) Security analysis on other metrics in the CCSS, i.e., temporal and environmental, provides a complete view of the system security score. An external auditor and contributor to this process could provide general scoring for the application.

Acknowledgment. The authors would like to thank Universitas Multimedia Nusantara for the support of this research work.

REFERENCES

[1] C. Johnson, Credentialism and the proliferation of fake degrees: The employer pretends to need a degree; the employee pretends to have one, *Hofstra Labor Employ. Law J.*, vol.23, no.2, pp.269-343, 2006.

[2] O. Ghazali, Q. Al-Maatouk and O. S. Saleh, Graduation certificate verification model: A preliminary study, *Int. J. Adv. Comput. Sci. Appl.*, vol.10, no.7, pp.575-582, 2019.

[3] N. Lutfiani, D. Apriani, E. A. Nabila and H. L. Juniar, Academic certificate fraud detection system framework using blockchain technology, *Blockchain Front. Technol.*, vol.1, no.2, pp.55-64, 2022.

[4] R. Q. Castro and M. A.-Y. Oliveira, Blockchain and higher education diplomas, *Eur. J. Investig. Heal. Psychol. Educ.*, vol.11, pp.154-167, 2021.

[5] U. Rahardja, S. Kosasi, E. P. Harahap and Q. Aini, Authenticity of a diploma using the blockchain approach, *Int. J. Adv. Trends Comput. Sci. Eng.*, vol.9, pp.250-256, 2020.

[6] E. Durant and A. Trachy, Digital diploma debuts at MIT, *MIT News*, 2017.

[7] Q. Tang, Towards using blockchain technology to prevent diploma fraud, *IEEE Access*, vol.9, 2021.

[8] F. Wegelid, *Storing Digital Certificates Using Blockchain*, Master Thesis, Lund University, 2019.

[9] S. Mahmoodzadeh, J. Shahrabi, M. Pariazar and M. S. Zaeri, Project selection by using fuzzy AHP and TOPSIS technique, *Int. J. Soc. Manag. Econ. Bus. Eng.*, 2007.

[10] B. B. A. Christyono, M. Widjaja and A. Wicaksana, Go-Ethereum for electronic voting system using clique as proof-of-authority, *TELKOMNIKA (Telecommunication Comput. Electron. Control)*, vol.19, no.5, p.1565, 2021.

[11] L. Mark, V. Ponnusamy, A. Wicaksana, B. B. Christyono and M. Widjaja, A secured online voting system by using blockchain as the medium, in *The Smart Cyber Ecosystem for Sustainable Development*, P. Kumar, V. Jain and V. Ponnusamy (eds.), Wiley, 2021.

[12] M. El Khatib, F. Beshwari, M. Beshwari and A. Beshwari, The impact of blockchain on project management, *ICIC Express Letters*, vol.15, no.5, pp.467-474, 2021.

[13] IBM, *What is Blockchain Technology?*, 2022, https://www.ibm.com/topics/what-is-blockchain, Accessed on Apr. 14, 2022.

[14] Irwan and A. Julianto (eds.), Ethereum presents London hard fork to fix high transaction fees on its network, *VOI*, 2021, https://voi.id/en/technology/67336/ethereum-presents-london-hard-fork-to-fix-high-transaction-fees-on-its-network, Accessed on Jul. 04, 2022.

[15] P. M. Mell and K. Scarfone, The common configuration scoring system (CCSS): Metrics for software security configuration vulnerabilities, *NIST Interagency/Internal Report (NISTIR)*, 2010.

[16] National Institute of Standards and Technology, *National Vulnerability Database*, https://nvd.nist.gov/vuln-metrics, Accessed on Jul. 07, 2022.

[17] Lisk Foundation, *Lisk*, 2021, https://lisk.com, Accessed on Apr. 14, 2022.

[18] W. Wang et al., A survey on consensus mechanisms and mining strategy management in blockchain networks, *IEEE Access*, pp.22328-22370, doi: 10.1109/ACCESS.2019.2896108, 2019.

Author Biography

Arya Wicaksana is a lecturer at the Department of Informatics at UMN. He received Master Degree in VLSI Engineering from Universitas Tunku Abdul Rahman. He successfully demonstrated the UTAR first-time success ASIC design methodology on a multi-processor system-on-chip project using 0.18μm processing technology in 2015. His main research interests are blockchain applications and computational intelligence. He recently worked on a decentralized autonomous social media. He is affiliated with ACM and IEEE as a professional member. He has served as an invited reviewer in IEEE ACCESS, IJNMT, and IFERP and an invited author in IntechOpen and other scientific publications.

James Christian Wira received the B.Sc. degree in Informatics from Universitas Multimedia Nusantara, Indonesia, in 2021. His research interests are blockchain applications and applied computing.