7 (2) July 2021 149-163 ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
Register: *Jurnal Ilmiah Teknologi Sistem Informasi*

Contents lists available at www.journal.unipdu.ac.id

Journal Page is available to www.journal.unipdu.ac.id/index.php/register

Research article

Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain

Nero Chaniago [a,*], *Parman Sukarno* [b], *Aulia Arif Wardana* [c]

[a,b,c] *Department of Informatics, Telkom University, Bandung, Indonesia*
email: [a,*] nerochaniago@student.telkomuniversity.ac.id, [b] psukarno@telkomuniversity.ac.id, [c] auliawardan@telkomuniversity.ac.id
** Correspondence*

ARTICLE INFO

Article history:
Received 1 June 2020
Revised 30 June 2020
Accepted 19 July 2020
Available online 3 May 2021

Keywords:
authentication
diplomas
public blockchain
Smart Contract ERC-721
transcript

Please cite this article in IEEE style as:
N. Chaniago, P. Sukarno, and A. A. Wardana, " Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 7, no. 2, pp. 149-163, 2021.

ABSTRACT

Ethereum is one of the oldest examples of blockchain technology provides a system that converts centralized storage to distributed and records transactions by way of decentralized and not by a centralized system and can be verified by each node, therefore it is suitable for storing fingerprints from official diploma documents and transcripts that are published. Smart contract is needed for making contract transactions to Ethereum with programming code, so contracts such as diplomas and transcripts uploaded on the Ethereum blockchain can distribute and produce diploma validation and the authenticity of transcripts with transaction hash, consensus, and comply with ERC-721 token standardization. The results showed that a sample of 5 electronic documents in pdf format with a transaction speed of 1 second on each file that were published and secured with Ethereum blockchain technology can be easily verified for authenticity, the system proposed and developed by us takes in consideration invalid and failure cases by giving the necessary feedback to the user.

1. Introduction

Diplomas and transcripts are certificates issued formally by educational institutions to students who have finished their study. Whether it's on elementary school level, junior high school, senior high school, and university level. Nowadays, many diplomas and transcripts are issued by educational institutions per year, but the problem with fake diplomas and transcripts is still a major problem. As stated by Kanan et.al. that fake diplomas and transcripts are serious problems, so efforts must be made to prevent forgery of this certificate at any time [1].

Technological advances that increasingly high efforts to protect data security need to be increased [2], for that technology such as the blockchain that recently has been discussed can be proposed on the security of electronic documents of diplomas and transcripts. Blockchain proposes data security by decentralized storage, having interrelated cryptographic hash functions and consensus [3, 4, 5, 6, 7]. The type of technology used in our study is public blockchain Ethereum, because the public blockchain provides the concept that all nodes can participate to mine and implement real decentralized technology [4].

The Head of HKLI Directorate General of Belmawa Nuril Furkan, discussed in 2019 the increasing news about the increasing of fake diplomas and transcripts, this fake diploma reporting took place during the 2019 general election, for this reason, the role of universities is expected to comply with the rule of law that has been stipulated in the Kementrian Riset dan Teknologi Republik Indonesia (Menristekdikti) No. 59 of 2018 [8]. Some companies in Indonesia, require prospective employees when they register for the job must send a copy of the diploma in the form of pdf files, this is vulnerable to

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

the falsification of electronic documents and must be prevented and see its authenticity with file upload based verification system.

Like a diploma in Indonesia in the form of the paper with affixing holograms and logo stamps does not reduce the cases of diplomas and fake transcripts, the true documents in the form of paper are vulnerable to forgery. Director-General of Belmawa in 2017 launched a website-based system for online diploma verification facilities. The name of the system is "Sistem Verifikasi Ijazah Secara Elektronik" (SIVIL). But another problem is a diploma verification system electronically stored on the centralized system. One of of centralized storage is that the database is vulnerable to hacked, because the information is stored on a centralized system [3].

Research conducted by Kanan et.al. focusing on the authentication system for the authenticity of diplomas using blockchain, the application was implemented at Al-Zaytoonah University Jordan, but system of verifying the authenticity of diplomas using student National ID [1]. Further research was conducted by Cheng et.al. focusing on diploma verification system in Taiwan, to solve the problem of fake diplomas in the country they propose a prototype system for verifying blockchain-based diplomas, but the verification mechanism on their system is by inputting a certificate search code on the system [2].

A research conducted by Kumar et.al. focusing on authentication of education certificate documents from the authorities, to carry out the process they use the blockchain technology mechanism, provides cryptographic and distributed concepts, the proposed system is to add a QR code and an inquiry string code to the paper-based certificate, then how to authenticate document using a phone scanner or website with certificate serial number [7].

A research conducted by N. Kumavat et.al. focusing on the problem of fake academic certificates and in the process of validating the authenticity of certificates often have to incur costs and a complex, they propose by storing certificates on the blockchain, but the verification system that they propose is to use a transaction id [9].

A research have reviewed digital signature method and SHA-1 algorithm for digital document security on legalizing undergraduate diplomas, with securing and validating digital document objects designed to be applied to diploma validation mechanisms, according to them legalization is based on having good security [10]. This research applies a website based system, but their system does not use blockchain technology. In addition, the process of verifying the authenticity of diplomas is by inputting digital signatures that printed on paper certificates and input on the website.

Research can verify the authenticity of a digital document, but the system does not use blockchain technology and in paper verification mechanism using digital signatures that printed on paper certificates and input on the website, research [1, 2, 7, 9] on the verification process using the student National ID, certificate search code, certificate serial number, and transaction id. Other than that Sistem Verifikasi Ijazah Secara Elektronik (SIVIL) in Indonesia does not use blockchain technology.

Therefore, In this paper our purpose of this system is to verify the authenticity of diplomas and transcripts with uploaded Portable Document Format (PDF) type files, the method proposed by this system is by Ethereum blockchain as a place to store fingerprints data from diplomas and transcripts, smart contract for data validation based on consensus and for making contract transactions to Ethereum with programming code, and SHA-256 algorithm to get fingerprint from diploma files and transcripts. Our system consists of DApp for making diploma and verification systems and file upload-based transcripts, DApp is a decentralized application can run on the Ethereum blockchain system and that uses peer-to-peer networks [3, 11].

2. Related Work

SmartCert blockchain imperative for educational certificates [1] presents, building an authentication system for the authenticity of diplomas using a blockchain, this application was carried out at Al-Zaytoonah University Jordan, the advantages of this research are building a system using a blockchain and applied directly to universities, and system of verifying the authenticity of diplomas using student National ID.

Blockchain and smart contract for digital certificate [2] presents, making a diploma verification system in Taiwan, to solve the problem of fake diplomas in the country they propose a prototype system for verifying blockchain-based diplomas, and the verification mechanism on their system is by inputting

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

a certificate search code on the system.

Educational certificate verification system using blockchain [7] presents, the process of verifying the authenticity of diplomas is one of the things that is routinely done by job providers, job providers require a lot of time to provide results from interviews, in this case a certificate of authenticity authentication process is needed, generally companies do authentication for a long time, to overcome this problem they create a blockchain-based diploma verification system, because the blockchain provides cryptographic and distributed functions, their verification system uses a phone scanner or website with a certificate serial number.

Certificate verification system using blockchain [9] presents, academic certificates issued from tertiary institutions still use hard copies to be given to students, problems that exist when the validation process of the authenticity of certificates often takes a long time, and there is potential for fake certificates, many cases of fake diplomas, problems they solve is reducing fake certificates with blockchain technology, blockchain can store certificate data, and the verification system that they propose is by transaction id.

Digital document security on legalize higher education diplomas with digital signature and SHA-1 algorithm [10] presents, security of digital diploma documents with digital signature method and SHA-1 algorithm, the digital signature that has been created is then placed on the certificate, and to test the validation of the diploma documents using the digital signature that is on the certificate.

Developing Ethereum blockchain-based document verification smart contract for moodle learning 1 management system [12] presents, in the digital verification system in the world of education in Turkey using a blockchain and smart contract-based system that is connected to the moodle learning system model, this system uses the public blockchain on the ropsten network.

Physical document validation with perceptual hash [13] presents, the process of electronic validation on the need for physical documents that are carried out electronically, a problem which shows that physical documents will have different hash values every digitized, the results get to show that validation with a hash can detect that the electronic file has been changed, as well as to detect the original file, but the system built does not use blockchain technology.

Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application [14] presents, the application of encryption and digital signatures for different cases such as health records, they proposed the 2048-bit RSA algorithm, AES 256-bit and SHA 256 in encryption and obtaining digital signatures. The application design developed is to provide integrity, confidentiality, and authentication services, their research uses the black box and white box testing in input testing.

Blockchain and smart contract for digital document verification [15] presents, student graduation occurs annually from different universities, all students who have graduated will have degrees and diplomas, diplomas can be used to apply for jobs or continue education due to the lack of mechanisms for the number of diploma forgery cases starting to occur, the proposed system for overcoming the problem is with blockchain technology, all personal IDs will be entered on the blockchain, e-cert will be created and obtain serial numbers and e-certificates entered into the blockchain, a QR code will be generated and given to the user, a verification mechanism for the authenticity of the diploma with a serial number or QR code.

2.1. Blockchain

Blockchain is a decentralized and distributed database that is widely used to record every different transaction in each block are encrypted with the hash of cryptography [1, 2, 3, 16] that uses blockchain is Ethereum [1, 2, 3], Ethereum is one that runs on the mechanism of blockchain technology and Ethereum presents ideas to avoid dependency on entities to store user data [3].

Blockchain has advantages in terms of securitization [5]. All blocks contained in the blockchain are connected with different or unique hashes and nonce. The node spreads decentralized, then the blocks in the node cannot be changed and can be verified by many parties [2, 17]. Blockchain uses many nodes scattered in the network, so that the number of nodes scattered will complicate the attacker in the breach of the system. One of the uniqueness of blockchain technology is the existence of mining which is called a miner if succeeds in solving a mathematical problem it will get a coin [17].

2.2. Smart contract

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

A smart contract is a self-executable, computerized transaction protocol which is useful for facilitating and verifying each contract [18]. Smart contract has a code function that consists of a complete series of Turing operations and makes a contract with code, the code that is run by the network on the blockchain once the contract is called, so each contract is stored in a decentralized database and cannot be changed [19, 20].

ERC-721 is an open standard token with the principle that tokens are not exchangeable or unique [21]. ERC-20 is currently the most popular Ethereum standard used to make tokens specifically [21]. ERC-20 can be managed in making tokens process that are operated in various blockchain implementations [4].

Smart contracts are executed independently when validation on a transaction is carried out, to use smart contracts on objects on the blockchain, transactions must be executed to notify that there is a new contract to be entered on the blockchain and the new contract is given a unique address with a 160-bit length, and the code is uploaded on the blockchain, after the contract is completed, the smart contract consists of the contract address, the contract balance, the nonce, and the transaction id [18]. Make smart contract using solidity, the solidity is based on contract-oriented programming, which aims to be able to run on Ethereum Virtual Machine (EVM). Just like other programming languages, solidity has data types, variables, and is almost similar to object-oriented programming such as inheritance. The contract function simple including:

- Admin can store diploma electronic document to blockchain.
- Admin can store transcript electronic document to blockchain.
- Stakeholder can verify the authenticity of diploma from blockchain.
- Stakeholder can verify the authenticity of transcripts from blockchain.

The implementation of ERC-721 tokens, following data types have been created the contract mechanism above:

- There is an object to store documents electronically. Each document will be signed using the SHA-256 hashing algorithm and accommodated in an object before being distributed on the blockchain.
- A map to make a 32 bytes record of documents. The mapping stage of each array is 32 bytes.

```
struct Sivil_chain {
        uint waktu_miner;
        uint nomor_block;
    }
    mapping (bytes32 => Sivil_chain) private
documents;
```

Fig. 1. Data types based on the contract using solidity language

Fig. 1 is an example of a struct data type in the solidity programming language that will be used to store several methods and attributes to support writing smart contract programs.

3. Method

In this paper, we propose a system for securing and verifying diploma and transcripts electronic documents using blockchain. The reason for using the blockchain is because it is decentralized and guarantees high data integrity [6, 22, 23]. The type blockchain that we use is the Ethereum blockchain which can make a data storage system decentralized and distributed so it does not make it centralized [11, 24, 25, 26].

The system that we created is based on relevant studies, in the system that we developed we produce diploma document data and transcripts in the form of electronic files of type pdf, where our system will generate hash values from the uniqueness of each document, so the data categories we store are cryptographic hash values and are further enhanced for storage using a blockchain, cannot be falsified, and the attacker cannot change the blockchain decentralized system because every node on the blockchain is spread and must be verified by a consensus algorithm namely Proof-of-Work, so this will be very difficult to hack.

Cryptographic hash values generated from our system consist of 66 digits which each time generated will produce a unique value. For reasons our system uses pdf files to verify the authenticity of diploma documents and transcripts, stakeholders do not need to worry about errors entering hash numbers, because our system accepts pdf files and will generate hashes from these files automatically and see if the value is stored in the blockchain.

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

One popular hacking method is MITM by an attacker to steal the integrity of the data that exists on the system [27, 28, 29]. Man-In-The-Middle (MITM) is an attack on the most popular systems in computer security networks MITM presents confidentiality and integrity [27], for this we need high system security in data protection, blockchain technology is used to ensure data integrity [3]. The hash value stored in an array of struct generated from the SHA-256 algorithm, as well as addresses stored in the struct, to secure diploma documents and admin transcripts make the document and produce the document into a pdf type, after that the document is inputted to the system, then when the admin sends the pdf to the blockchain, the system automatically gets the hash value and the smart contract address is saved.

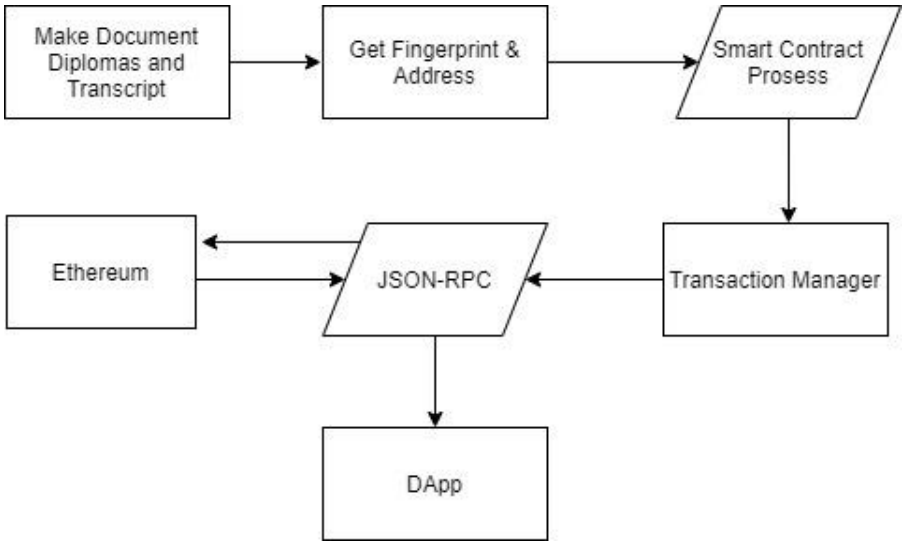

Fig. 2. Secure diplomas and transcript system

3.1. System overview

The general description of the system can be seen in Fig. 2, our DApp system is connected to the Ethereum blockchain, and has a code smart contract for file secure diplomas and transcript and verification.

a. Secure Diplomas and Transcripts:
   - Make Document Diplomas and Transcript
     Admin creates an electronic diploma document and transcript, by entering information from each student and making it a pdf type document, in the chancellor and dean section is added with a digital signature namely QR code.
   - Get Fingerprint & Address
     The system takes the hash from the diploma document and transcript with the SHA-256 algorithm. Secure Hash Algorithm (SHA) is a development of the hash MD function, this algorithm was introduced by the American National Institute as a FIPS standard in 1993 [6, 30]. Various types of the SHA algorithm include SHA-0, SHA-224, SHA-256, SHA-384, SHA-512. After the hash value is obtained, then the hash value is entered into an array of struct. The address used is generated from the smart contract when the compilation of the smart contract program occurs in the system and the address is entered into the array of struct. Here we use 3 smart contracts, first the smart contract called "file registration" is used to send the hash of the new file just created to the Ethereum blockchain, the second is the smart contract called “verify file” which is used for the verification process of the electronic document contract diploma and transcript which is in the consensus block on the Ethereum blockchain, and the third “migration file” that is used to create a new address at the address on the Ethereum blockchain.
   - Smart Contract Process
     At this stage, making smart contracts using a programming language solidity on Remix IDE, contracts that have been made with solidity language programming are then carried out transactions using the smart contract program including hash, address, value ether, gas value, limit gas. Smart contracts are important in the DApp system because this contract is used for basic programming operations in Dapp in our system the contract is used as:

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

Ijazah

Universitas Telkom

Nomor: AKD-123-111

Berdasarkan keputusan rektor menyatakan bahwa:

Nama: Nero Chaniago
Tempat Tanggal Lahir: Rangkasbitung-Lebak, 19 Juni 1998
Nomor Induk Mahasiswa: 1301164305
Program Studi: S1 Informatika
Tanggal Lulus: 2020-05-29

telah menyelesaikan dan memenuhi seluruh persyaratan pendidikan

S.Kom

beserta segala hak dan kewajiban yang melekat pada sebutan tersebut

Rektor,

Dekan,

(a)

Fakultas Informatika
S1 Informatika

Universitas Telkom

Transkrip Akademik

Nomor : AKD-123-111
Nama : Nero Chaniago
Nomor Induk Mahasiswa : 1301164305
Tempat, Tanggal Lahir : Rangkasbitung-Lebak, 19 Juni 1998
Tanggal Lulus : 2020-03-25
Jenjang Pendidikan : S1
No. Keputusan Rektor : Dasdsadasdasd

No	Kode	Mata Kuliah	Semester	SKS	Nilai

Pencapaian Akademik

SKS (Satuan Kredit Semester)	Total	0 sks
IPK (Indeks Prestasi Kumulatif)	Grade	3.25 (dari 4.00)

Tugas Akhir

Backchain Dan Smart Contract Untuk Keamanan Dokumen Elektronik: Studi Kasus Ijazah Dan Transkrip

Rektor,

Dekan,

(b)

Fig. 3. Example of Figure: (a) Diplomas.pdf; (b) Transcript.pdf

http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

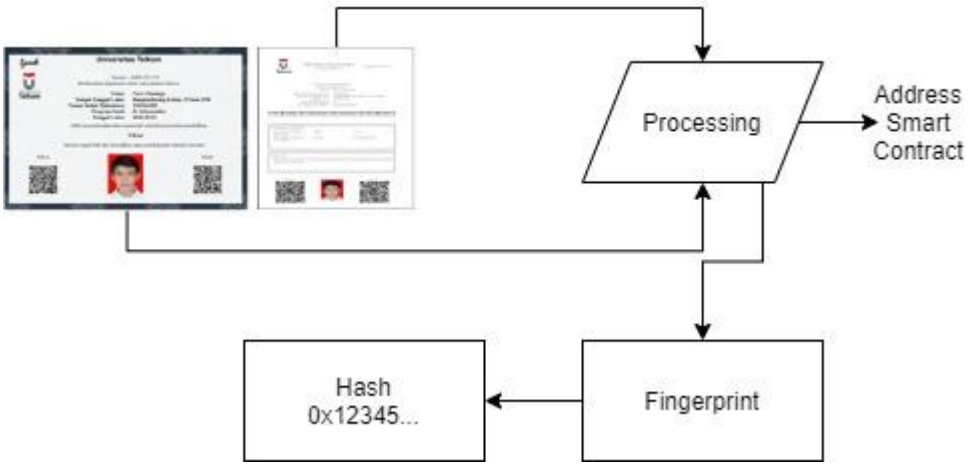

Fig. 4. Get fingerprint and address

Fig. 3 are examples of diplomas and transcripts generated by our system, and Fig. 4 is a system diagram for obtaining the fingerprint of the certificate hash value and the transcript.

a) Hash notes of electronic documents diplomas and transcripts.
b) Look for hashes and validation of electronic document diplomas and transcripts on consensus on the Ethereum blockchain.

Contracts made can perform functional operations on our system, smart contract algorithm in Algorithm 1.

Algorithm 1. Smart contract algorithm

```
contract SmartContract {
        function Catatan (hash) public {
            catatan = Record(waktu, blocknumber)
            save[catatan] = catatan
        }
        function CariCatatan (hash) public view {
            return save[catatan]
        }
}
```

- Transaction Manager

  At this stage, the webserver sees whether the ether value and gas value are sufficient to carry out transactions to the Ethereum blockchain or not, if the price is sufficient, contracts consisting of addresses will be signed using the ECDSA signature and then processing will continue to the Ethereum blockchain, whereas if the price is insufficient then the data transaction will be canceled.

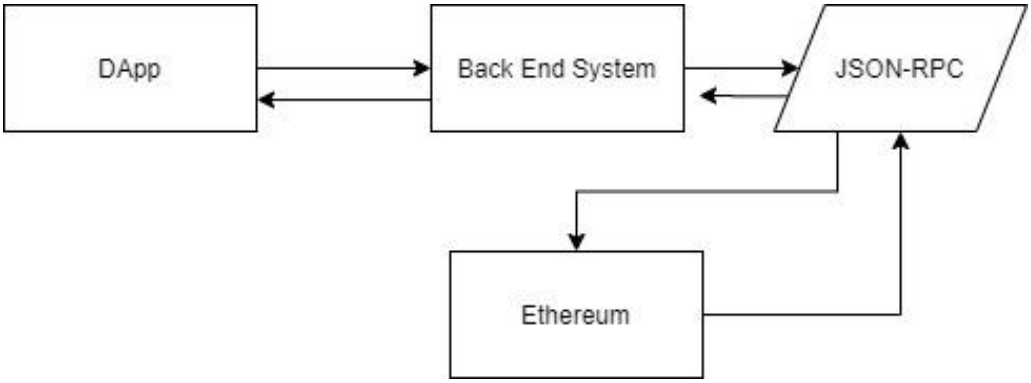

Fig. 5. Web3js JSON-RPC process

- Web3js JSON-RPC

  At this stage, Web3js JSON-RPC has a role in connecting our system with the Ethereum blockchain to DApp, our system supported by web3js on DApp that works with smart contracts to create consensus validation on the Ethereum blockchain node and integrates with Ethereum blockchain, JSON-RPC web3js bridges the DApp system we created with the Ethereum blockchain network, transactions that meet the criteria are then uploaded on the blockchain, and the smart contract code will compile on the Ethereum blockchain to make consensus agreed

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

by nodes on the Ethereum network, so as to do validation without requiring a third party. Some systems that use Web3js JSON-RPC in data distribution [30, 31, 32, 33, 34]. Fig 5. is an overview of the DApp system connected to the JSON-RPC API and then, connected to ethereum via API on the back end.

After all steps of the method are implemented the system will notify the display that the diploma and transcript electronic documents have been successfully uploaded to the blockchain, the notification includes the address contract, hash value, and transaction ID.

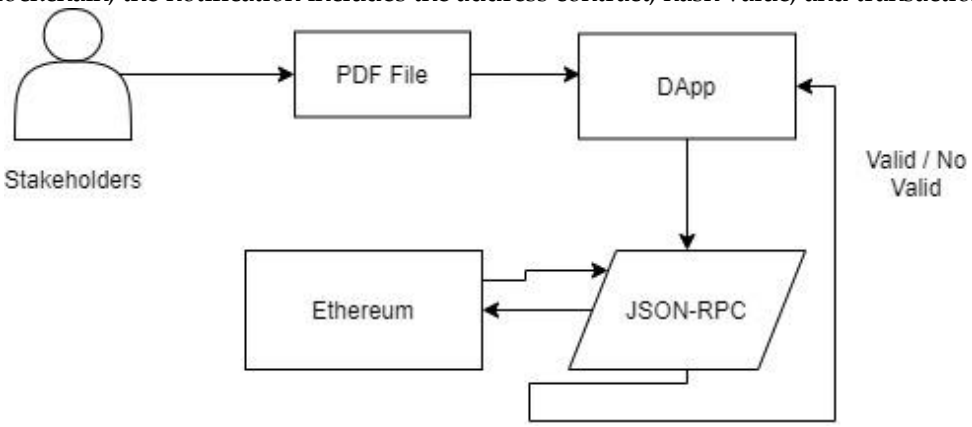

Fig. 6. Verification diplomas and transcript process.

Fig. 6 is a system description of verification, starting from the stakeholders uploading a pdf format document on our DApp, then our DApp communicates to the ethereum back end via the API, so that if there is a match in the hash value then the pdf is valid.

b. Verification Diplomas and Transcript Process:

This verification system starts from stakeholders uploading diploma files and transcripts pdf on the system, then the system sees the fingerprint of the document so that the hash value is obtained, the smart contract sends the hash to the Web3js JSON-RPC connected to the blockchain. If the hash is on the blockchain the system states valid and display valid information, block number, and timestamp so that it is stated that the file is authentic and trustworthy, otherwise if the hash is not present on the blockchain the system returns invalid information and the document is not valid. Fig. 7 is an overview of our system interface for uploading diploma files and transcripts for verification.

Fig. 7. Uploading diploma and transcript

3.2. Process overview

Ethereum blockchain with its distributed and decentralized nature, in this study the workings of our system are as follows:

1. The university records student information, then the system makes it a pdf file and records the fingerprint of the file (does not record student data information only the fingerprint of the file).
2. The system verifies all documents.
3. University turns over pdf files to students whose fingerprints have been recorded, students do not need to get a diploma because paper diplomas can still be falsified and this makes paper waste, the pdf file contains diplomas and transcripts that have been signed by the chancellor and dean digitally using QR code.
4. When diplomas and transcripts will be used to verify their authenticity whether applying for jobs or continuing education to a higher level, students can simply attach a pdf electronic document to the company or university to be addressed.

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

5. The company or university will verifies on the system whether the file is valid or fake.

3.3. How the process work

Fig. 8 is an overview of our working system illustrated. Flow diagram starts with the administrator creates an electronic diploma document and transcript by entering the student's identity such as name, place of birth, university, rector, grades and others. After that DApp creates QR code from the chancellor and dean, then the document is generated into pdf. The document that has become a pdf is done prepocessing by taking a fingerprint hash with the SHA-256 algorithm and the hash is transacted using smart contract steps, transaction manager, and JSON-RPC. If the transaction is approved by consensus on the blockchain node then the hash value is stored on the Ethereum blockchain, but if it is not appropriate then the transaction is canceled. After that the original document that has been taken hash been given to students via email in the form of a pdf file. If students have obtained diploma documents and transcripts, these documents can be verified and can be given to interested parties. To verify the authenticity of diploma and transcript electronic documents, stakeholders can upload the pdf file to the website-based DApp system that we created, if the file is uploaded the SHA-256 algorithm will check the hash value, after that the hash is delivered by the smart contract, JSON-RPC to search on contract address on the Ethereum blockchain, if the hash value is present and correct then DApp will provide notification information that the file is valid along with the digital signature and block number, but if the hash value is not present on the Ethereum blockchain then the file is declared invalid.

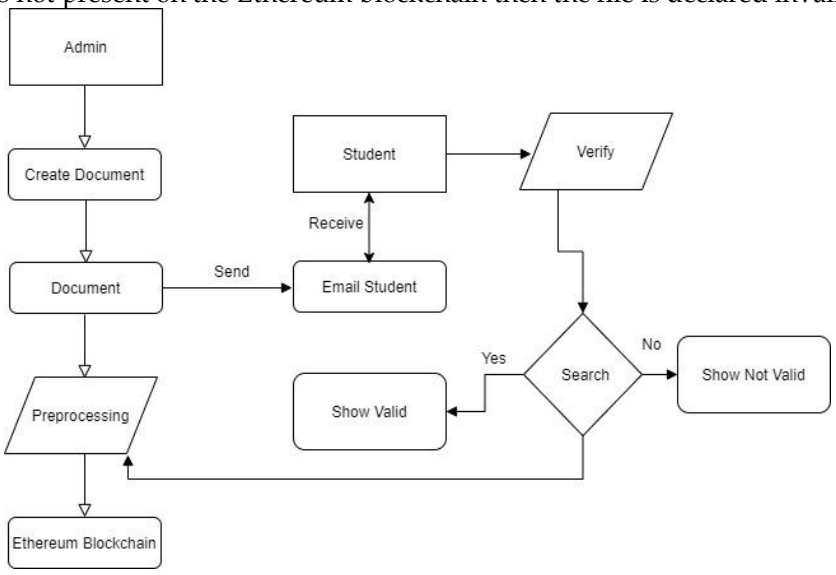

Fig. 8. Working process system

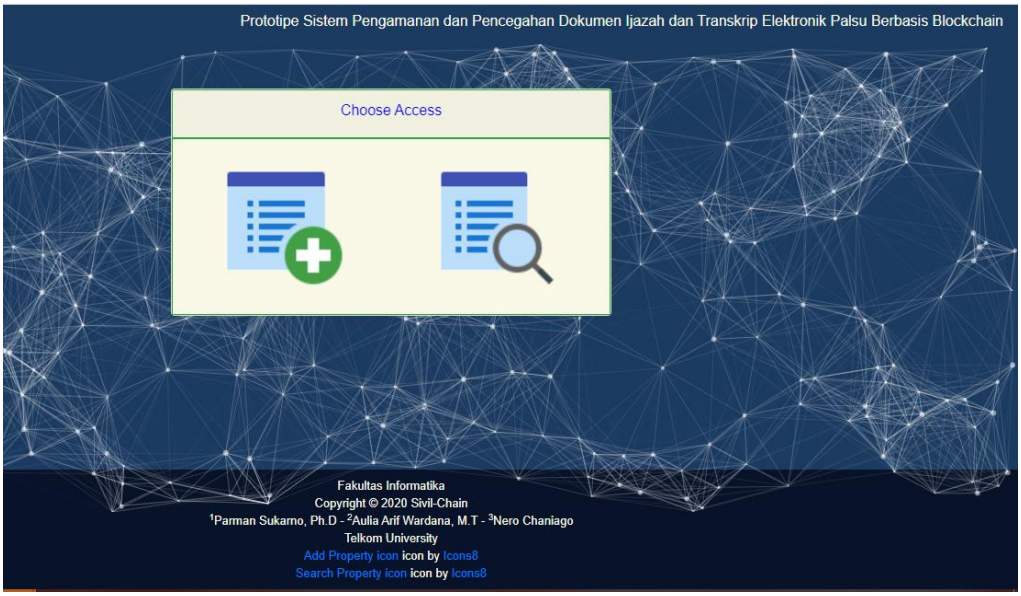

Fig. 9. Home page web

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

4. Results and Discussion

The system that we made can be seen in Fig. 9, the case here is only the admin who can make diploma documents and transcripts, and for stakeholders can only verify the authenticity of diplomas and transcripts.

In making diplomas and transcripts, the admin inputting information from students and making the document type pdf, after the document was successfully created the system will generate to get the hash value of the document. The hash will be stored in the struct of the smart contract and uploaded to the blockchain. If the document was uploaded successfully on the public blockchain, system will return that the document has been successfully uploaded.

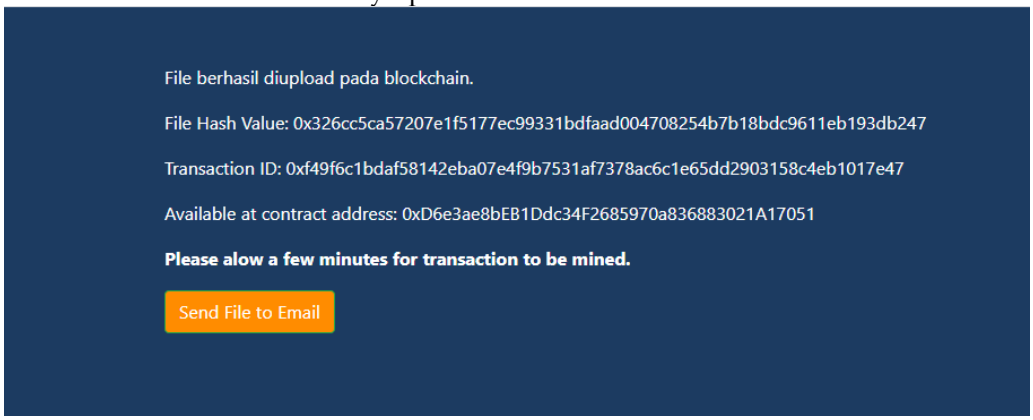

Fig. 10. Notification upload file page to Ethereum blockchain

In Fig. 10 the system provides information if the diploma document and transcript are successfully uploaded to Ethereum blockchain and make it decentralized, the information is in the form of hash, transaction id, and contact address. The hash of the document is recorded with the transaction id to the node scattered on the blockchain, this makes it not easily hacked and falsified, because if the hash value is not found on the document blockchain it is false.

Fig. 11. Notification verification valid file page

In Fig. 11, system detects the original diploma document and transcript, so we get a hash, block number, and timestamp. If the fake file is verified it will show invalid as shown in Fig. 12.

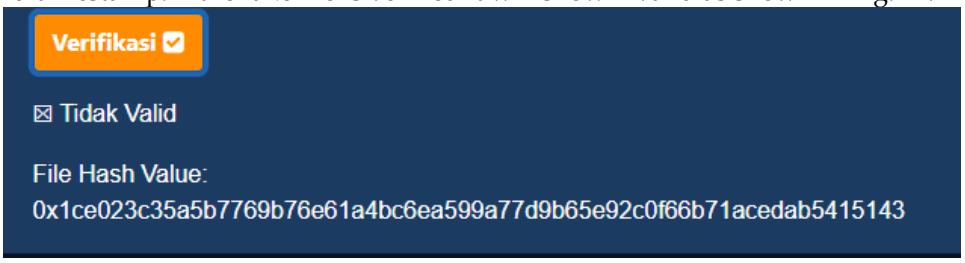

Fig. 12. Notification verification not valid file page

The hash value of the document shown in Fig. 12 is not on the blockchain so our system states that the file is not valid and fake. To see the truth that the hash of the document has been uploaded to the blockchain, we can look at Ethereum by looking at transactions from our system's blockchain address as shown in Fig. 13.

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

In Fig. 13, stating that the hash transaction, status, block number, etc. Indicate that our diploma and transcript files were successfully uploaded on the blockchain, especially on Ethereum declaring success status, if a transaction has been entered on the Ethereum blockchain then the transaction cannot be hacked or deleted, so diploma and transcript data will be safe from falsification of documents. Table 1 are the results of the integrity testing of electronic document diploma and transcripts:

In Table 1, based on the results of integrity testing of electronic documents diplomas and transcripts by getting fingerprint values using the SHA-256 hashing algorithm and by using blockchain technology for data storage has very good authentication, seen from the hash file, valid hash, and block number, block number contains that the data stored is in a block in Ethereum which is decentralized and secured with cryptographic hashes but related to each other, the block number always contains the hash of the previous block. If the hash file and valid hash have different values, then the file is not in the block number in Ethereum because the file is invalid, so it will minimize the falsification of electronic documents diplomas and transcripts, and the system has strong security because it uses a decentralized Ethereum blockchain storage technology and secured by cryptography that are interrelated with one another.

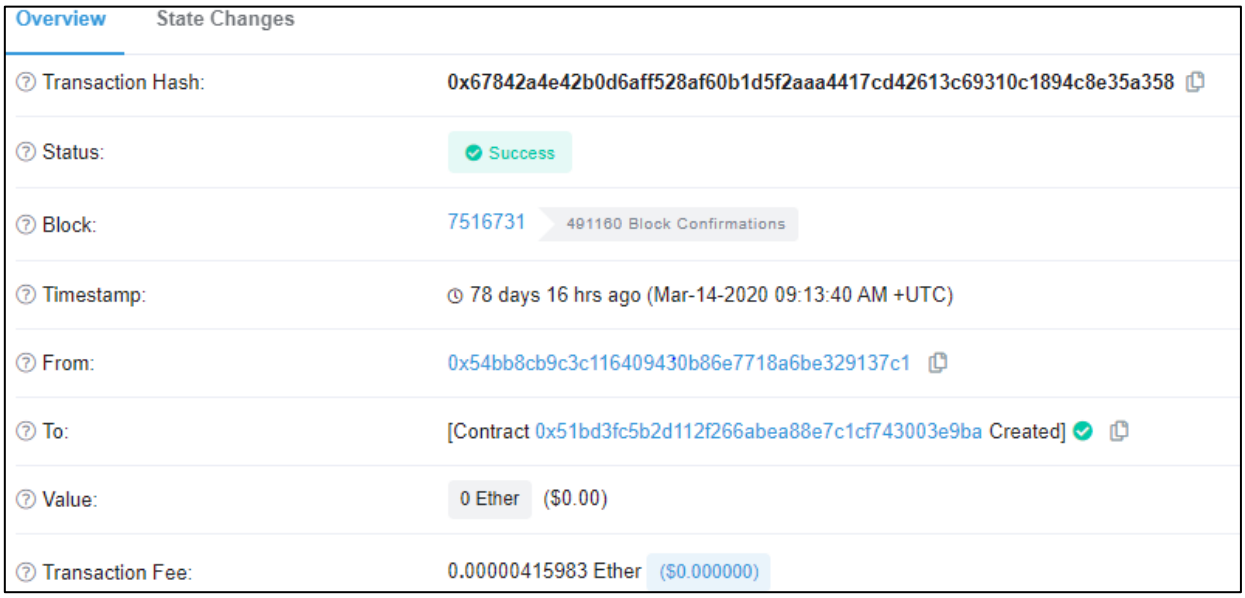

Fig. 13. Example transaction on Ethereum page

Table 1. The results of the integrity

Name File	File Hash	Valid Hash	Block Number
File 1	0xe384dbb8efa471c8cfd08f3a618a508cdd9b6c55596ec69a7fa627be87fee9f6	0xe384dbb8efa471c8cfd08f3a618a508cdd9b6c55596ec69a7fa627be87fee9f6	20276
File 2	0x4d25ddeb31135b247659d4f1a1330c005e4ed9bd3d2c37601c5ff9605fe006dc	0x4d25ddeb31135b247659d4f1a1330c005e4ed9bd3d2c37601c5ff9605fe006dc	20385
File 3	0x25c8da8baa77cdfb302e8973516c7b729a66655fe26738161de2afa764aef09d	0x25c8da8baa77cdfb302e8973516c7b729a66655fe26738161de2afa764aef09d	20393
File 4	0x13656aa5f330603df63c1a2767498b3f10411cf62e3b7a891efb3a27da691278	0x13656aa5f330603df63c1a2767498b3f10411cf62e3b7a891efb3a27da691278	20445
File 5	0xb720f0401e3bf067f60179eeb5a42a3227d65e5fd56bd5643bdd447c710ab706	0xb720f0401e3bf067f60179eeb5a42a3227d65e5fd56bd5643bdd447c710ab706	20467

http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

4.1. Performance

In this section we will see the performance of the 5 files when a transaction is made to the Ethereum blockchain which includes transaction speed, gwei, gas limit, gas cost, total price and transaction hash on Ethereum.

From the results of the evaluation in Table 2, it is found that the transaction process from the trial of the 5 documents is 1 second for each document, this can be considered because it only takes 1 second for each transaction, the total price amount is interrelated with the gas cost and file size, if the size of the file is large, the gas cost becomes large, so that the total price paid increases with the amount of gas cost. The result of the gas limit of each document is in the range 1613249 to 1654428, for that if the gas cost is increased in the range 1613249-1654428 will affect the performance of the file transaction speed which will result in faster transaction speeds and a greater total price. Then the transaction that is successfully accepted to be forwarded by the smart contract to the Ethereum blockchain, will be signed with an ECDSA signature and uploaded to the node on the blockchain with consensus validation, so that the file has a hash value and a digital signature value on Ethereum.

Table 2. The results of performance

Name File	Size	Tx Speed (Second)	Gwei	Gas Limit	Gas Cost	Total Price	Tx Hash
1	405 KB	1	1	1625532	831966	0.000014ETH	0xf49f6c1bdaf58142eba07e4f987531af7378ac6c1e65dd2903158c4eb1017e47
2	3.278 KB	1	5	1625628	832014	0.000062ETH	0x8ec69a63e1f73b81d5f94b50ff635148e8f2f4f80f6214866d7040afa7cf80d0
3	5.661 KB	1	5	1654428	836988	0.000067ETH	0x80cd1cb2d0b814679447ea5a977c3e4292b392805ac0fbbbe2e223c2b848e557
4	338 KB	1	1	1621128	831415	0.000010ETH	0xeeb047e380cf5caa2121812b0ed22e06f3c94b0e742f0b182bd6a05d000236a8
5	313 KB	1	1	1613249	831137	0.000004ETH	0xffbb27f3cb45d11d25c73cb7e860a9d84ad4eda4a3c71f699aeb8e7ff416ee10

We did a test on the file without changing the contents of the file, by compressing the file to be as small as possible with the help of online compression tools to see the integrity of files on the blockchain, the results obtained can be seen in Table 3.

Table 3. The results of compress file

Name File	Original Size (KB)	Size Modification (KB)	Hash Before Compression	Hash After Compression
1	405	173	0xe384dbb8efa471c8cfd08f3a618a508cdd9b6c55596ec69a7fa627be87fee9f6	0x57081f9edc716a7c565073d41b418cc6971fce7a7f3a3a9eb4ded1498eb0d58a
2	3.278	168	0x4d25ddeb31135b247659d4f1a1330c005e4ed9bd3d2c37601c5ff9605fe006dc	0xa3a18d14053fd890e19340ef57859e600673a3054d202c1874b93b11896b92fa
3	5.661	174	0x25c8da8baa77cdfb302e8973516c7b729a66655fe26738161de2afa764aef09d	0xc4d36e5038bd5da1a7d1b61d6185e6c564eab2ebb204ac2d4a0a85f618b8552e
4	338	153	0x13656aa5f330603df63c1a2767498b3f10411cf62e3b7a891efb3a27da691278	0xb96028163bc65d27be39a053bafda53f4f12a2cbd718c16d826f954e6e9b12e3
5	313	146	0xb720f0401e3bf067f60179eeb5a42a3227d65e5fd56bd5643bdd447c710ab706	0x858341d6ee437dbeef31f48f1fbd402c513345eb08ae957e7ce9bb5fd17cf9b5

The results obtained from Table 3 are if the file is compressed without changing the content and meta data, then the hash will be different from there was before in the Ethereum blockchain, but if the file is only copied and pasted it will not change the hash because the integrity of the file is still maintained and original . So that this can maintain the authenticity of the diploma file and transcript

 http://doi.org/10.26594/register.v7i2.1959

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

because after making the diploma document and transcript file version and uploaded to the Ethereum blockchain, the file is already a final and original file.

4.2. Discussion

The verification process of diploma documents and paper-based transcripts is not discussed in detail in this paper, but there is potential to deal with this problem, in this paper discusses the file-based verification process to overcome the occurrence of false documents and overcome the validation process of documents that previously used fees and use a lot of time.

A way to facilitate the process of verifying files that have been changed without changing the content is to look at the hash of the file on the blockchain, because every time a file is corrupted and meta data changes it will change the hash value of the file, so if the file has been taken and hashed uploaded to Ethereum through smart contract programming, the hash cannot be modified, so if the file is corrupted then the hash of the file will not be registered in Ethereum.

Diploma documents and paper-based transcripts are still being made but for the verification and legalization process using file uploads on a blockchain-based system, so stakeholders who want to verify the authenticity of the diploma simply provide a copy of the electronic file that has been given. For this reason, future studies can discuss paper-based documents digitalized using Optical Character Recognition (OCR) or Barcode techniques. Then the system to apply the off-chain mechanism to the files created, and the on-chain mechanism for transaction records.

4.3. Comparative study

In this section is a summary of the diploma verification system using blockchain technology based on related work, the verification system that we propose to verify the authenticity of diplomas and transcripts is to use file uploads on public blockchain Ethereum. Here we summarize in Table 4 regarding the comparative study.

Table 4. The comparative study

Researcher	Verification System Proposed
Kanan et al. [1]	Making systems with blockchain technology and verification using student National ID.
Cheng et al. [2]	Making systems with blockchain technology and verification using certificate search code.
Kumavat et al. [9]	Making systems with blockchain technology and verification using transaction id.
Kumar et al. [7]	Making systems with blockchain technology and verification using phone scanner or website with a certificate serial number.
Kumari et al. [15]	Making systems with blockchain technoogy and verification using serial number or QR code.

5. Conclusion

The system can detect the authenticity of electronic documents diplomas and transcripts with file-based Ethereum blockchain technology, so that the file-based verification process can prevent fake diplomas and transcripts and make verification easier, with the file replacing printed versions of diplomas and transcripts so that it will be more economical in spending paper, the results of testing the transaction time from file to Ethereum is 1 second from each file and file integrity indicates if the file is damaged, modified, or the hashed will be different from the original on the Ethereum blockchain, so that the file is detected for authenticity on Ethereum blockchain is a file that has not been modified and falsified, and hashes from the original file stored on a Ethereum. Using a system based on blockchain technology can reduce the falsification of electronic documents, because the process of publishing and verification is done transparently within the system, the system can guarantee the information provided is correct with the right accuracy.

Author Contributions

Nero Chaniago: Methodology, conceptualization and software. Parman Sukarno: Formal analysis, validation and review & editing. Aulia Arif Wardana: Supervision, software and review & editing.

Acknowledgment

We would like thank to Allah SWT for his grace so that this research can be completed on time, program "Insentif Riset Sistem Inovasi Nasional (INSINAS) Kemenristek BRIN" and Telkom University for support & funding this research, and also Forensic and Security (Foresty) Laboratory for their support.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

Declaration of Competing Interest

We declare that we have no conflict of interests.

References

[1] T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019.

[2] J.-C. Cheng, N.-Y. Lee, C. Chi and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018.

[3] R. Gupta, Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain, Birmingham, UK: Packt, 2018.

[4] A. K. Shrivastava, C. Vashistth, A. Rajak and A. K. Tripathi, "A Decentralized Way to Store and Authenticate Educational Documents on Private Blockchain," in *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2019.

[5] J. Fat, H. Candra and W. William, "Sekuritisasi Data Sensor pada Aplikasi Internet of Things (IoT) dengan Menggunakan Blockchain Ethereum di Jaringan Testnet," *TESLA,* vol. 21, no. 1, pp. 79-86, 2019.

[6] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access,* vol. 7, pp. 147782-147795, 2019.

[7] K. D. Kumar, P. Senthil and M. K. D.S, "Educational Certificate Verification System Using Blockchain," *International Journal of Scientific & Technology Research,* vol. 9, no. 3, 2020.

[8] I. Yunelia, "Laporan Peredaran Ijazah 'Aspal' di Tahun Politik Meningkat," Medcom, 26 August 2019. [Online]. Available: https://www.medcom.id/pendidikan/news-pendidikan/1bVydZ2N-laporan-peredaran-ijazah-aspal-di-tahun-politik-meningkat.

[9] N. Kumavat, S. Mengade, D. Desai and J. Varolia, "Certificate verification system using blockchain," *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET),* vol. 7, no. IV, p. 53–57, 2019.

[10] B. Triand, S. Effendi, R. Puspasari, I. F. Rahmad and E. Ekadiansyah, "Digital Document Security on Legalize Higher Education Diplomas with Digital Signature and SHA-1 Algorithm," in *2019 7th International Conference on Cyber and IT Service Management (CITSM)*, Jakarta, Indonesia, 2019.

[11] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access,* vol. 6, pp. 53019-53033, 2018.

[12] E. Karataş, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System," *Bilişim Teknolojileri Dergisi,* vol. 11, no. 4, pp. 399-406, 2018.

[13] P. A. W. Putro, "Physical document validation with perceptual hash," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, Bandung, Indonesia, 2017.

[14] M. A. Sadikin and R. W. Wardhani, "Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application," in *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, Lombok, Indonesia, 2016.

[15] S. S. Kumari and D. Saveetha, "Blockchain and Smart Contract for Digital Document Verification," *International Journal of Engineering & Technology,* vol. 7, no. 4.6, pp. 394-397, 2018.

[16] M. Crosby, N. Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman, "BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review,* vol. 2, pp. 6-19, 2016.

[17] A. D. Yulianto, P. Sukarno, A. A. Warrdana and M. A. Makky, "Mitigation of Cryptojacking Attacks Using Taint Analysis," in *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia, 2019.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 149-163

[18] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Campobasso, Italy, 2018.

[19] A. Bogner, M. Chanson and A. Meeuw, "A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain," in *6th International Conference on the Internet of Things (IoT'16)*, Stuttgart, Germany, 2016.

[20] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 1594-1605, 2019.

[21] N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris and G. C. Polyzos, "OAuth 2.0 authorization using blockchain-based tokens," in *Proc. Workshop Decentralized IoT Syst. Secur. (DISS) Conjunct Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2020.

[22] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," *IEEE Internet of Things Journal,* vol. 7, no. 2, pp. 818-829, 2020.

[23] R. Shrestha and S. Y. Nam, "Regional Blockchain for Vehicular Networks to Prevent 51% Attacks," *IEEE Access,* vol. 7, pp. 95033-95045, 2019.

[24] S. Sayeed, H. Marco-Gisbert and T. Caira, "Smart Contract: Attacks and Protections," *IEEE Access,* vol. 8, pp. 24416-24427, 2020.

[25] S. R. Niya, F. Schüpfer, T. Bocek and B. Stiller, "A Peer-to-peer Purchase and Rental Smart Contract-based Application (PuRSCA)," *it - Information Technology,* vol. 60, no. 5-6, pp. 307-320, 2018.

[26] Q. Xu, Z. He, Z. Li, M. Xiao, R. S. M. Goh and Y. Li, "Chapter 8 - An effective blockchain-based, decentralized application for smart building system management," in *Real-Time Data Analytics for Large Scale Sensor Data*, vol. 6, H. Das, N. Dey and V. E. Balas, Eds., Academic Press, 2020, pp. 157-181.

[27] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 3, pp. 2027-2051, 2016.

[28] G. Oliva, S. Cioabă and C. N. Hadjicostis, "Distributed Calculation of Edge-Disjoint Spanning Trees for Robustifying Distributed Algorithms Against Man-in-the-Middle Attacks," *IEEE Transactions on Control of Network Systems,* vol. 5, no. 4, pp. 1646-1656, 2018.

[29] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussai, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," *IEEE Internet of Things Journal,* vol. 7, no. 4, pp. 3310-3322, 2020.

[30] R. Roshdy, M. Fouad and M. Aboul-Dahab, "Design and Implementation a New Security Hash Algorithm Based on MD5 and SHA-256," *International Journal of Engineering Sciences & Emerging Technologies,* vol. 6, no. 1, pp. 29-36, 2013.

[31] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1676-171, 2019.

[32] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon and A. Seneviratne, "A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain," *IEEE Access,* vol. 7, pp. 33159-33172, 2019.

[33] S. Guo, Y. Dai, S. Guo, X. Qiu and F. Qi, "Blockchain Meets Edge Computing: Stackelberg Game and Double Auction Based Task Offloading for Mobile Blockchain," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 5, pp. 5549-5561, 2020.

[34] M. C. I. Putri, P. Sukarno and A. A. Wardana, "Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on web application," *Register: Jurnal Ilmiah Teknologi Sistem Informasi,* vol. 6, no. 2, pp. 74-85, 2020.