Penggunaan Blockchain pada Sistem Keamanan Penerbitan Ijazah Digital

Kirana Shely Sefiana 18220036
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : kiranas2602@gmail.com

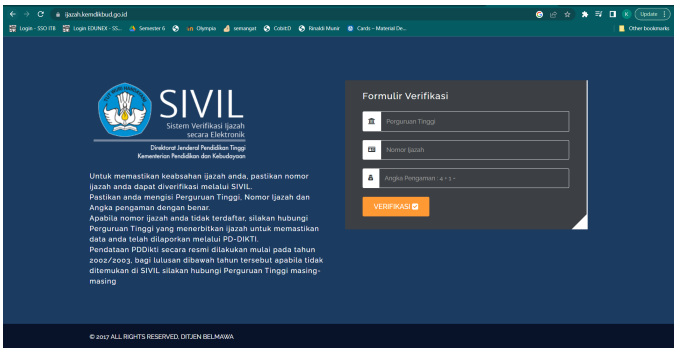
***Abstrak*— Dalam dunia pendidikan, ijazah merupakan bukti resmi yang menunjukkan bahwa seseorang telah menyelesaikan suatu program pendidikan pada instansi tertentu. Namun, tidak jarang adanya beberapa oknum tidak bertanggung jawab yang memalsukan ijazah demi bisa melamar untuk suatu posisi. Padahal pemalsuan ijazah sangat dilarang dalam pasal UUD. Untuk mengatasi permasalahan ijazah ini, diperlukan suatu teknologi yang dapat memastikan kebenaran sertifikat digital suatu ijazah. Selain itu, teknologi ini juga harus bisa memastikan bahwa setiap data yang terdaftar pada sistem kemdikbud adalah benar dan tidak dapat dipalsukan dengan mudah. Dengan menggunakan salah satu teknologi dari cabang ilmu kriptografi, yaitu *blockchain*, permasalahan tersebut dapat diselesaikan dengan baik. Dengan penggunaan teknologi ini, proses verifikasi dapat dilaksanakan dengan aman karena *blockchain* menggunakan *data hashing* yang dapat memastikan apakah suatu ijazah digital merupakan asli atau palsu serta sekaligus mengamankan data agar tidak mudah dicuri. Selain itu, data pemilik dan institusi yang mengeluarkan ijazah juga dapat dipastikan aman dan tidak akan mudah dipalsukan karena *blockchain* memiliki sistem *block* yang terkait satu sama lain sehingga akan sulit untuk memalsukan ijazah.**

Keywords*— *Blockchain; Hash; Verifikasi Ijazah Digital; Security; Kriptografi

I. PENDAHULUAN

Dalam dunia pendidikan, ijazah merupakan bukti resmi yang menunjukkan bahwa seseorang telah menyelesaikan suatu program pendidikan pada instansi tertentu. Tentunya ijazah ini merupakan bukti penting bagi sarjana sebagai surat untuk melamar pekerjaan, menunjukan kompetensi diri, atau sebagai modal untuk melanjutkan ke jenjang pendidikan yang lebih tinggi. Namun, tidak jarang adanya beberapa oknum tidak bertanggung jawab yang memalsukan ijazah demi bisa melamar untuk suatu posisi. Padahal pemalsuan ijazah sangat dilarang dalam pasal UUD dan memiliki sanksi berat jika ada yang melakukannya. Sesuai dengan Undang-Undang Nomor 1 Tahun 2022 tentang Kitab Undang-Undang Hukum Pidana bahwa setiap orang yang memalsukan ijazah atau sertifikat kompetensi dapat dipidana penjara paling lama 6 tahun atau denda sebanyak 500 juta rupiah.

Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi atau kemdikbud, selaku pemerintahan yang bertanggung jawab dalam mengurus pendidikan di Indonesia, telah membuat platform yang berguna untuk memverifikasi ijazah. Namun, metode verifikasi yang dilakukan menggunakan input data nama perguruan tinggi, nomor ijazah, dan angka pengamanan saja. Kemudian, dalam platform tersebut disebutkan bahwa data ijazah yang dapat diverifikasi hanya data yang telah dilaporkan oleh perguruan tinggi terkait kepada instansi kemdikbud yaitu PD-DIKTI. Hal ini tentunya bisa menjadi hambatan karena perlu adanya integrasi data terlebih dahulu antara perguruan tinggi dengan instansi dalam kemdikbud. Selain itu, integrasi data ini juga memerlukan keamanan yang ketat agar ijazah tidak mudah untuk dipalsukan.



Gambar 1. Platform verifikasi ijazah secara elektronik (sumber : https://ijazah.kemdikbud.go.id/)

Untuk mengatasi permasalahan ijazah ini, diperlukan suatu teknologi yang dapat memastikan kebenaran sertifikat digital suatu ijazah. Selain itu, teknologi ini juga harus bisa memastikan bahwa setiap data yang terdaftar pada sistem kemdikbud adalah benar dan tidak dapat dipalsukan dengan mudah. Dengan menggunakan teknologi yang dapat melakukan dua hal ini, sistem keamanan ijazah akan terhindar dari pemalsuan dan integritas data ijazah akan terjaga.

Kemudian akan sangat baik jika dengan teknologi yang sesuai, dibuatkan sistem keamanan untuk penerbitan ijazah dalam suatu platform yang terintegrasi.

Dengan menggunakan salah satu teknologi dari cabang ilmu kriptografi, yaitu *blockchain*, permasalahan tersebut dapat diselesaikan dengan baik. Dengan penggunaan teknologi ini, proses verifikasi dapat dilaksanakan dengan aman karena *blockchain* menggunakan *data hashing* yang dapat memastikan apakah suatu ijazah digital merupakan asli atau palsu serta sekaligus mengamankan data agar tidak mudah dicuri. Selain itu, data pemilik dan institusi yang mengeluarkan ijazah juga dapat dipastikan aman dan tidak akan mudah dipalsukan karena *blockchain* memiliki sistem *block* yang terkait satu sama lain sehingga akan sulit untuk memalsukan ijazah. Dapat dilihat dari sifat-sifat teknologi *blockchain* ini, bahwa teknologi ini sangat cocok bila diterapkan dalam sistem keamanan pada penerbitan sertifikat ijazah digital.

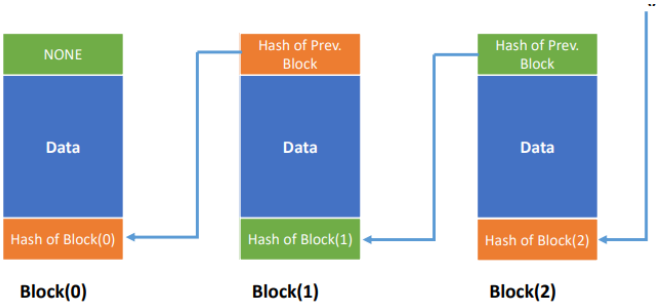
II. DASAR TEORI

A. *Blockchain*

Blockchain menggunakan struktur data yang dikenal sebagai "*block*" untuk menyimpan informasi transaksi. Setiap *block* terdiri dari header yang berisi metadata dan tautan ke *block* sebelumnya, serta data transaksi yang disimpan dalam bentuk *hash*. Setiap *block* terhubung satu sama lain membentuk rantai (*chain*), sehingga menciptakan integritas data. *Blockchain* juga bisa disebut sebagai keamanan yang bentuknya seperti sebuah *ledger* atau buku pencatat suatu transaksi yang tersimpan secara digital. *Blockchain* ini memiliki keamanan yang sangat tinggi sehingga mustahil untuk diserang atau diubah.

Dalam sejarah perkembangannya, *blockchain* pertama kali diperkenalkan pada tahun 2008 oleh seseorang atau sekelompok orang yang menggunakan nama samaran "Satoshi Nakamoto" dalam whitepaper berjudul "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Whitepaper ini menjelaskan konsep dasar *blockchain* yang digunakan dalam implementasi Bitcoin, yaitu sebagai teknologi yang memungkinkan transaksi digital tanpa perlu melibatkan pihak ketiga (terdesentralisasi).

Secara umum *blockchain* dimulai saat adanya transaksi. Transaksi ini dapat berupa transfer aset digital, catatan data, atau eksekusi perjanjian pintar. Setiap transaksi memiliki informasi tertentu, misalnya dalam untuk penerbitan ijazah digital terdapat data mahasiswa, institusi, nilai kelulusan, dan data terkait lainnya. Setelah transaksi dibuat, informasi transaksi tersebut diverifikasi oleh jaringan node dalam blockchain. Setiap node memeriksa keabsahan transaksi menggunakan aturan dan protokol yang telah ditetapkan. Protokol yang dilakukan misalnya proses verifikasi yang melibatkan pemeriksaan tanda tangan digital, validasi data nama, atau aturan tertentu lainnya. Setelah berhasil melalui protokol verifikasi tersebut, transaksi tersebut akan dimasukkan menjadi "*block*". Setiap melakukan penyimpanan blok, data referensi mengenai blok sebelumnya juga akan disimpan dalam blok tersebut dalam bentuk *hash*. Hal inilah yang membuat antar blok dalam *blockchain* akan saling terkait.



Gambar 2. Rangkaian *blockchain* yang terkait oleh *hash*
(sumber : Materi kuliah II4031 *Blockchain* - Rinaldi Munir)

Perlu diperhatikan bahwa sebelum blok ditambahkan ke *blockchain*, jaringan node perlu mencapai kesepakatan tentang kevalidan blok tersebut. Ini dilakukan melalui proses yang disebut "algoritma konsensus". Algoritma konsensus menetapkan aturan untuk memilih node yang akan membuat blok berikutnya dan memvalidasi blok sebelumnya. Beberapa contoh algoritma konsensus adalah *Proof of Work* (PoW), *Proof of Stake* (PoS), dan *Delegated Proof of Stake* (DPoS). Setelah blok baru diterima dan divalidasi oleh mayoritas node dalam jaringan, blok tersebut ditambahkan ke blockchain. Setiap node dalam jaringan memperbarui salinannya dari blockchain dengan menambahkan blok terbaru. Proses ini memastikan bahwa semua node dalam jaringan memiliki salinan yang sama dan konsisten dari blockchain.

```
{
      previousHash: "0",
      index: 1,
      data: "Bambang - STI - 18217001 - 3.56",
      timestamp: "2023-05-20 13:35:50.279527",
      currentHash:
"acb3fdba475aa73baeae5eae6abf3a63706063d0e02b30617
9db7202c8b62e64"
   }
```

Tabel 1. Contoh penyimpanan blok dalam bentuk data json
(sumber : pribadi)

Terdapat tiga prinsip dasar dalam operasi *blockchain*,

1. Desentralisasi

Blockchain beroperasi secara terdesentralisasi, artinya tidak ada satu otoritas tunggal yang mengontrol atau mengelola data. Data disimpan dan dikelola oleh jaringan peer-to-peer yang terdiri dari banyak komputer yang disebut "node". Dengan begitu proses operasi pencatatan transaksi akan lebih transparan dan terpercaya.

2. Transparansi

Seluruh transaksi yang terjadi dalam blockchain dapat dilihat oleh semua pihak yang terhubung ke jaringan. Setiap perubahan data harus disetujui oleh mayoritas node dalam jaringan, sehingga menciptakan keandalan dan transparansi.

Selain itu, konsep *blockchain* ini dikembangan secara terbuka atau *open-source* dan dokumentasi nya pun disebarluaskan oleh *developernya.*

3. *Immutable*

Seluruh data blok dalam *blockchain* harus melewati konsensus terlebih dahulu sehingga data yang masuk tidak mudah diubah atau dimanipulasi oleh siapapun. Selain itu, data dalam *blockchain* dilindungi dengan menggunakan teknik kriptografi yang kuat. Setiap transaksi dienkripsi dan terhubung dengan transaksi sebelumnya dalam bentuk rantai (*chain*), sehingga sulit untuk dimanipulasi atau dicurangi.

B. *Hashing*

Hash merupakan fungsi kriptografis yang mengambil input data atau pesan dengan panjang tertentu dan menghasilkan keluaran (*message digest)* dengan panjang tetap. Setiap input pesan yang dimasukkan akan menghasilkan keluaran yang berbeda atau unik. Bila ada sedikit saja perbedaan antar input, hasil *hash* yang dikeluarkan tidak akan sama.

Fungsi *hash* ini berbeda dengan fungsi kriptografi lainnya yang dapat melakukan enkrip dan dekrip. *Hash* ini bersifat *one-way* atau dengan kata lain hasil *hash* tidak dapat dikembalikan lagi menjadi input atau pesan awal. Walaupun begitu, dengan adanya sifat ini, fungsi *hash* ini sangat berguna untuk keamanan data karena isi data atau input tidak akan bisa ditemukan dengan mudah.

Terdapat tiga sifat fungsi *hash,*

1. *Collision resistance*

Sifat ketahanan tabrakan dalam fungsi *hash* artinya bahwa sangat sulit atau hampir tidak mungkin untuk menemukan dua input yang berbeda yang menghasilkan hash value yang sama. Dalam konteks ini, tubrukan mengacu pada situasi ketika dua input data yang berbeda menghasilkan hasil *hash* yang sama persis sehingga artinya *message digest* dari fungsi hash sudah tidak unik lagi. Fungsi hash yang tahan tubrukan atau *collision,* menjaga integritas data dengan memastikan bahwa perubahan kecil pada input akan menghasilkan perubahan besar pada hash value yang dihasilkan. Jika fungsi *hash* memiliki ketahanan tabrakan yang baik, maka akan sangat sulit bagi penyerang untuk memanipulasi data dengan mencari dua input yang menghasilkan hash value yang sama.

2. *Preimage resistance*

Sifat *preimage resistance* artinya sangat sulit atau hampir tidak mungkin untuk mendapatkan input data asli (pesan asli) hanya dari hasil *hash* yang diketahui. Dalam kata lain, jika hanya diberikan *message digest*, akan sangat sulit untuk melakukan "reversal" dan mengembalikan input data asli. Fungsi hash yang memiliki ketahanan *preimage* yang baik memastikan bahwa hasil *hash* tidak akan memberikan informasi mengenai data input.

3. *Second preimage resistance*

Sifat *second preimage resistance* artinya akan sangat sulit untuk menemukan dua input data yang berbeda yang menghasilkan hasil *hash* yang sama (*collision*), saat salah satu dari input tersebut sudah diketahui. Dalam hal ini, penyerang memiliki akses ke input data asli dan mencoba menemukan input data kedua yang akan menghasilkan hash value yang sama dengan input asli. Ketahanan dari sifat ini memastikan bahwa sulit bagi penyerang untuk menemukan input kedua yang memenuhi kondisi ini.

Seiring perkembangan, jenis-jenis algoritma fungsi *hash* menjadi banyak bermunculan. Beberapa diantaranya adalah algoritma MD5, RIPEMD, SHA-1, SHA-256, dan WHIRLPOOL. Terdapat juga beberapa algoritma *hash* yang terdapat tubrukan atau *collision*. Maka dari itu, biasanya dalam penggunaan kehidupan nyata algoritma SHA-256 merupakan salah satu algoritma yang sering digunakan.

Algoritma	Ukuran *message digest* (bit)	Ukuran blok pesan	Kolisi
MD2	128	128	Ya
MD4	128	512	Hampir
MD5	128	512	Ya
RIPEMD	128	512	Ya
RIPEMD-128/256	128/256	512	Tidak
RIPEMD-160/320	160/320	512	Tidak
SHA-0	160	512	Ya
SHA-1	160	512	Ada cacat
SHA-256/224	256/224	512	Tidak
SHA-512/384	512/384	1024	Tidak
WHIRLPOOL	512	512	Tidak

Gambar 3. Beberapa fungsi *hash* (sumber : Materi kuliah II4031 Fungsi *hash* - Rinaldi Munir)

III. Desain dan Rancangan

Untuk melakukan implementasi *blockchain* pada sistem keamanan penerbitan ijazah digital, akan digunakan metode pemberian tanda QR *code* pada ijazah saat proses transaksi data berlangsung. Pada proses nya, pertama-tama akan diminta terlebih dahulu data mengenai mahasiswa, program studi, nomor induk mahasiswa, dan nilai akhir kelulusan. Setelah itu akan masuk ke proses transaksi. Pada operasi transaksi akan melakukan *hashing* terhadap data yang telah di-input. Kemudian hasil *hash* akan disimpan dalam blok bersamaan dengan penyimpanan data dan hasil hash pada blok sebelumnya. Hasil *hash* tersebut juga akan dijadikan data value untuk menghasilkan QR *code* yang nantinya akan dimasukkan dalam ijazah digital sebagai alat verifikasi.

Selain melakukan penerbitan QR *code* untuk ijazah digital, hasil implementasi ini juga akan mempunyai fungsi verifikasi. Proses verifikasi ini akan meminta terlebih dahulu data mahasiswa yang akan diperiksa keaslian QR *code* pada ijazahnya. Setelah data dimasukkan, file QR *code* yang tertera pada ijazah perlu dimasukkan. Jika QR *code* yang dimasukan adalah benar, maka akan ada pesan bahwa ijazah berhasil diverifikasi. Namun, jika QR *code* yang dimasukkan adalah palsu atau data mahasiswa yang akan diverifikasi merupakan data yang salah, maka akan muncul pesan bahwa ijazah tidak terverifikasi. Proses verifikasi ini akan membaca data yang di-input, lalu akan mengecek apakah data tersebut ada dalam data blok-blok. Kemudian, jika data ada, informasi blok akan diambil dan akan dilakukan pengecekan apakah informasi nilai *hash* pada blok sama dengan nilai *hash* yang ada pada

QR *code*. Dengan rancangan inilah implementasi *blockchain* akan dilakukan untuk proses penerbitan ijazah dan verifikasi keasliannya.

IV. Implementasi dan Pengujian

A. Implementasi

Proses implementasi *blockchain ini* akan dilakukan dengan membuat program sederhana menggunakan *reactJS*. Penggunaan *reactJS* ini bertujuan agar dapat membuat tampilan sederhana secara terpisah dan membuat fungsi operasi dengan library tambahan untuk proses *hash*. Proses *hash* ini akan menggunakan algoritma SHA-256 yang menghasilkan nilai *hash* sepanjang 256 bit. Kemudian dibutuhkan juga library untuk pemrosesan QR *code*. Maka dari itu, digunakan juga library *QRcode* dan *QRscanner*. Berikut ini adalah kode program dari implementasi *blockchain*.

Program implementasi *blockchain*

```
import { StatusBar } from
'expo-status-bar';
import { StyleSheet, Text, View } from
'react-native';
import { useState, useRef } from 'react';
import { QRCode } from
'react-qrcode-logo';
import QrScanner from 'qr-scanner';
import { sha256 } from 'js-sha256';
import ijazah from '../data/ijazah'


const homeScreen = () => {
    const [file, setFile] =
useState(null);
    const [data, setData] =
useState(null);
    const [hash, setHash] =
useState(null);
    const fileRef = useRef();

    const [dataInput, setDataInput] =
useState(null);

    const handleClick = () => {
        fileRef.current.click();
    };


    const handleChange = async (e) => {
        const file = e.target.files[0];
        setFile(file);
        const result = await
QrScanner.scanImage(file);
        console.log(result);
        if (sha256(ijazah.data) == result
&& dataInput == ijazah.data){
            alert("Ijazah Anda
terverifikasi!!")
        }else{
            alert("Ijazah Anda tidak
terverifikasi :((")
        }

    }

    const handleGenerate = async (e) => {
        const data = e.target.value;
        setData(data);
        setHash(sha256(data));
        console.log("hasil hash : ",
sha256(data));
        alert("QR anda berhasil
digenerate!");
    }

    const handleInput = async (e) => {
        const input = e.target.value;
        setDataInput(input);
        setHashInput(sha256(dataInput));
    }

  return (
    <View style={styles.container}>
      <Text>Generate QR Ijazah</Text>
      <input placeholder="Nama - Jurusan
- NIM - IPK Kelulusan"
onChange={handleGenerate} size="35"/>
      <StatusBar style="auto" />
      <QRCode value={hash || 0} />
      <Text>Verifikasi QR Ijazah</Text>
      <input placeholder="Nama - Jurusan
- NIM - IPK Kelulusan"
onChange={handleInput} size="35"/>
      <input type="file" accept=".png,
.jpg, .jpeg" onChange={handleChange}/>
    </View>
  );
}
export default homeScreen
const styles = StyleSheet.create({
  container: {
    flex: 1,
    backgroundColor: '#fff',
    alignItems: 'center',
    justifyContent: 'center',
  },
});
```

Dapat dilihat pada kode program di atas, bahwa fungsi *handleGenerate* akan melakukan penerbitan QR *code* dan penyimpanan data. Lalu pada fungsi *handleVerif* akan melakukan proses verifikasi dengan membaca data dan QR *code* yang diinput lalu mengecek kesamaan nilai *hash*. Setelah

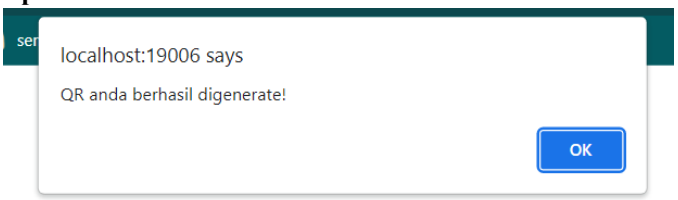
itu akan ada dua kondisi keluaran yaitu terverifikasi dan tidak terverifikasi.

Program ini dibuat oleh bahasa pemrograman *reactJS*. Oleh karena itu, jika hasil implementasi ini akan digunakan, platform yang dihasilkan bisa dalam bentuk web atau *mobile application*. Dengan begitu, proses verifikasi dan penerbitan ijazah akan semakin mudah untuk dilakukan.

B. Pengujian

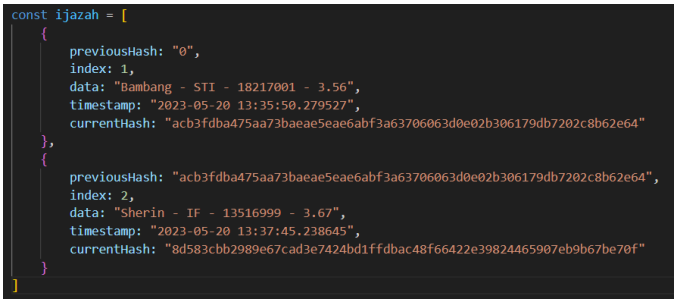
Setelah proses pembuatan program untuk implementasi *blockchain* selesai, akan dilaksanakan proses pengujian untuk memastikan apakah program yang dibuat sudah memenuhi fungsi yang dibutuhkan atau belum. Pengujian ini akan dilakukan dengan menggunakan beberapa skenario *test case*.

Pengujian fungsi penerbitan QR *code* ijazah dari data input.



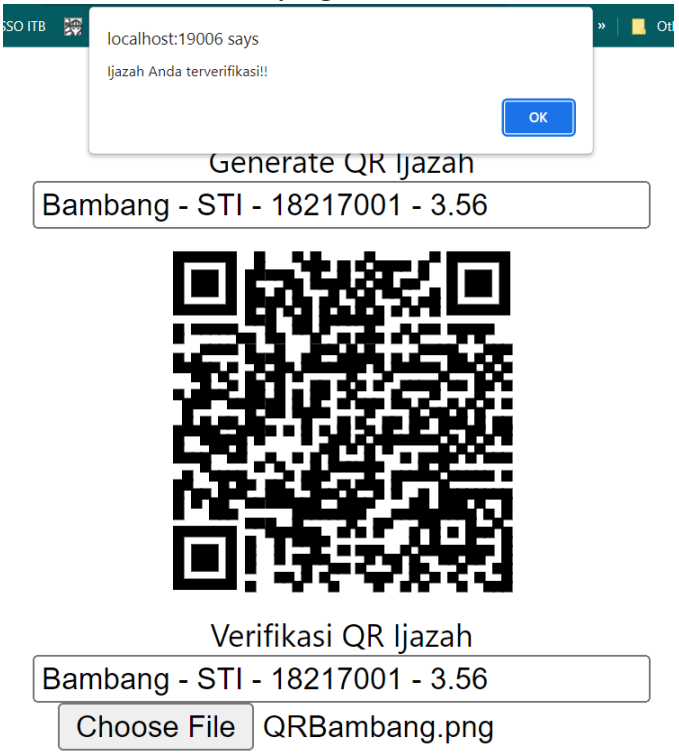
Gambar 4. Hasil pengujian penerbitan QR *code* ijazah

Dapat dilihat pada gambar di atas, bahwa setelah data yang diminta dimasukkan, proses transaksi akan dimulai dengan melakukan hash pada data dan memasukan blok baru pada penyimpanan data. Lalu akan muncul notifikasi ‘QR anda berhasil digenerate!’ dan QR *code* yang berisi hasil *hash* akan muncul pada layar. Kemudian gambar QR *code* ini dapat di-*save* sebagai alat verifikasi ijazah. Pada skenario percobaan ini akan disimpan QR ini dalam file ‘QRBambang.png’ dan akan disimpan juga QR palsu yang isi data nya salah dengan file ‘QR Palsu.png’ untuk melakukan skenario pengujian selanjutnya.



Gambar 5. Hasil penyimpanan data blok setelah transaksi penerbitan QR *code* ijazah

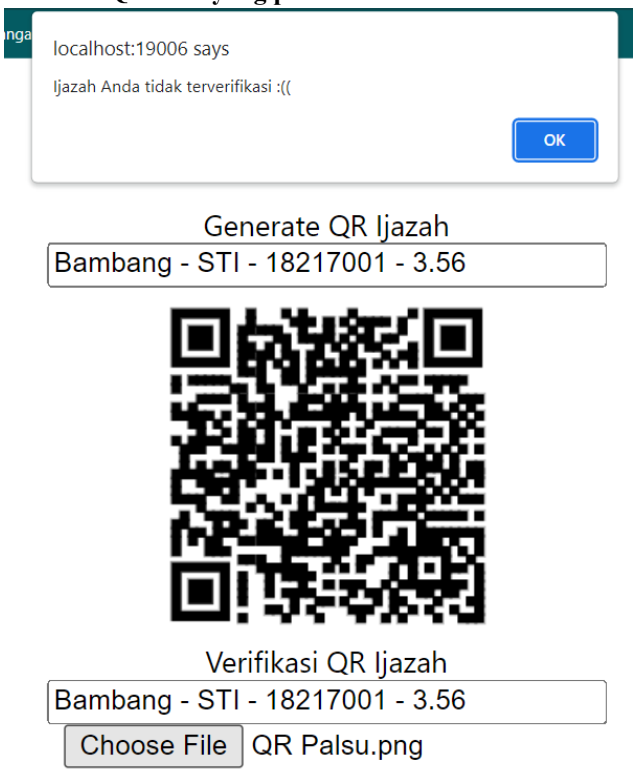
Pengujian fungsi verifikasi QR *code* ijazah dengan masukkan data dan QR yang benar.



Gambar 6. Hasil pengujian verifikasi QR *code* ijazah 1

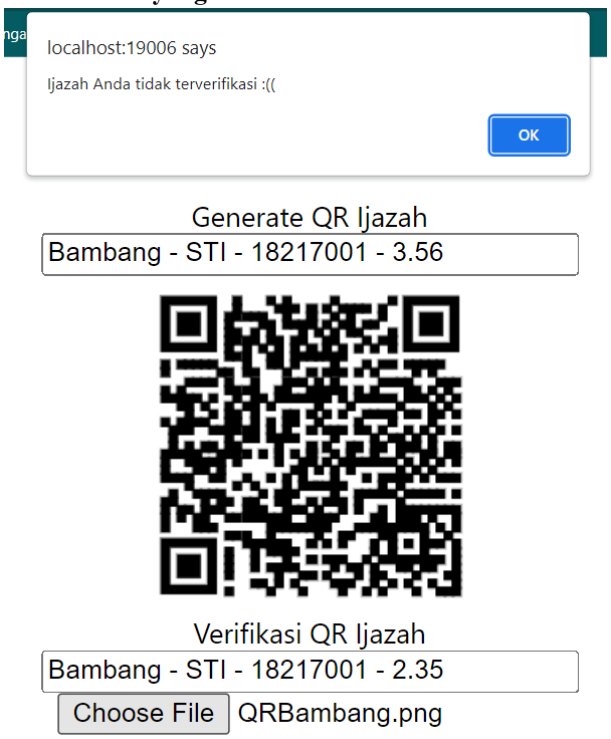
Dapat dilihat pada gambar di atas, bahwa setelah data yang akan dicek dan QR ijazah dimasukkan, terdapat notifikasi bahwa ‘Ijazah berhasil terverifikasi’. Dengan berhasilnya verifikasi QR ijazah, artinya QR dan data yang dimasukkan adalah asli dan benar.

Pengujian fungsi verifikasi QR *code* ijazah dengan masukkan QR *code* yang palsu.



Gambar 7. Hasil pengujian verifikasi QR *code* ijazah 2

Pengujian fungsi verifikasi QR *code* ijazah dengan masukkan data yang salah.



Gambar 8. Hasil pengujian verifikasi QR *code* ijazah 3

Pada percobaan gambar 6, file QR *code* yang dimasukkan adalah file 'QR Palsu.png' yang isinya adalah hasil *hash* yang salah. Dapat dilihat walaupun data verifikasi yang dimasukkan sudah benar, karena file QR yang dimasukkan salah ijazah menjadi tidak terverifikasi. Hal tersebut juga ditandai dengan adanya notifikasi 'Ijazah Anda tidak terverifikasi :((‘.

Hal serupa juga terjadi pada percobaan gambar 7. Pada skenario percobaan ini input data verifikasi yang dimasukkan salah pada nilai IPK nya. Dikarenakan data input tidak akan ditemukan pada data blok yang disimpan, proses verifikasi akan gagal. Kemudian akan muncul juga notifikasi yang sama yang mengatakan bahwa Ijazah tidak terverifikasi.

Pada hasil implementasi kode program *blockchain* ini, telah dilakukan empat skenario pengujian. Skenario pertama yaitu uji fungsi penerbitan QR *code* untuk ijazah, pengujian verifikasi dengan data yang benar, dan dua skenario lainnya adalah pengujian untuk data input dan file QR yang salah. Untuk keempat skenario pengujian tersebut, semua nya berhasil mendapatkan keluaran yang diinginkan. Dengan demikian, pembuatan program implementasi *blockchain* ini berhasil dilakukan.

V. Kesimpulan

Blockchain merupakan salah satu teknologi dari cabang kriptografi yang dapat menjaga integritas suatu data dan melindungi data dari kegiatan pemalsuan atau pencurian data. *Blockchain* ini sangat cocok untuk diterapkan pada permasalahan pemalsuan ijazah. Dengan teknologi ini, proses penerbitan ijazah dapat dilakukan dengan aman karena setiap proses penerbitan akan terdaftar sebagai satu transaksi dalam blok data pada *blockchain.* Lalu dengan teknologi ini juga, proses verifikasi ijazah dapat berlangsung dengan aman karena verifikasi ini menggunakan fungsi *hash* yang sulit untuk diserang sehingga percobaan untuk pemalsuan dan pencurian data akan sulit dengan digunakannya *blockchain* dan fungsi *hash* dalam implementasi ini. Dengan ada nya hasil percobaan implementasi sederhana ini, diharapkan kedepannya dapat dikembangkan suatu *platform* yang menggunakan konsep ini untuk sistem keamanan dalam penerbitan ijazah pada setiap instansi pendidikan yang ada di Indonesia.

Ucapan Terima Kasih

Penulis ingin mengucapkan puji syukur pada Allah SWT. atas nikmat-Nya yang memberikan penulis ilmu sehingga dapat menyelesaikan makalah ini. Kemudian diucapkan juga terima kasih banyak pada Bapak Dr. Rinaldi Munir, M.T. selaku dosen mata kuliah II4031 yang telah mengajarkan penulis ilmu-ilmu yang bermanfaat seputar kriptografi. Selain itu, penulis juga sangat berterimakasih kepada "Satoshi Nakamoto" sebagai tokoh anonim yang telah mengemukakan konsep *blockchain* dan menciptakan *bitcoin* sehingga penulis dapat menambah wawasan ilmu dan mendapatkan bahan referensi untuk menulis makalah ini. Diharapkan makalah ini bisa bermanfaat untuk pembaca dan penulis dapat mengimplementasikan ilmu ini pada kehidupan sehari-hari.

Video Penjelasan (Youtube)

https://youtu.be/BC-9-zRLDJ0

Referensi

[1] H. Bhanushali, A. Arthena, S. Bhadra, and J. Talukdar, “Digital certificates using blockchain: An overview,” SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372133 (accessed May 20, 2023).

[2] M. A. Kusuma, P. Sukarno and A. A. Wardana, "Security System for Digital Land Certificate Based on Blockchain and QR Code Validation in Indonesia," 2022 International Conference on Advanced Creative Networks and Intelligent Systems (ICACNIS), Bandung, Indonesia, 2022, pp. 1-6, doi: 10.1109/ICACNIS57039.2022.10055114.

[3] A. Rezjki Suljztan Syawaludin and R. Munir, "Registration of Land and Building Certificate Ownership using Blockchain Technology," 2021 International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 2021, pp. 1-7, doi: 10.1109/ICISS53185.2021.9533191.

[4] V. A. Windarni, E. Sediyono and A. Setiawan, "Using GPS and Google maps for mapping digital land certificates," 2016 International Conference on Informatics and Computing (ICIC), Mataram, Indonesia, 2016, pp. 422-426, doi: 10.1109/IAC.2016.7905756.

[5] Munir, Rinaldi. 2023. Slide Kuliah II4031 Kriptografi dan Koding: Blockchain

[6] Munir, Rinaldi. 2023. Slide Kuliah II4031 Kriptografi dan Koding: Fungsi Hash

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Mei 2023

Kirana Shely Sefiana (18220036)