JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 737-741

Sistem Penyimpanan Dan Validasi Data Sertifikat Penghargaan Karyawan Berbasis Blockchain Dengan Enkripsi SHA-256

Muhammad Erlangga Sapta Ajie[1], Muhammad Yasser Arafat[2*]

[1,2]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Indonesia
Email: [1]tkj2.0erlangga.sa@gmail.com, [2*]dosen00680@unpam.ac.id
(* : coressponding author)

Abstrak - Data penting sudah seharusnya di amankan se-aman mungkin, baik data digital maupun data fisik, terlebih lagi pada data digital, sebuah keamanan harus di sediakan untuk menyimpan nya. Contoh salah satu data yang sangat penting di kehidupan kita adalah Sertifikat. Sertifikat merupakan data penting yang beberapa orang miliki untuk tujuan tertentu, contoh nya legalitas, mengklaim bahwa kita mempunyai sesuatu secara sah. Pada Penelitian kali ini, Penulis akan meneliti, merancang dan membuat Sistem yang dapat Menyimpan Data Sertifikat Kompetisi Resmi dengan mengandalkan model teknologi yaitu blockchain. Sistem di rancang dan di dibuat secara Konseptual dari Awal hingga membentuk Sistem blockchain yang mirip dengan Aslinya. Pada tahap akhir, akan di lakukan Pengujian dan Evaluasi Sistem, apakah Sistem berjalan sesuai dengan harapan dan Hasil sebuah Data yang di simpan di dalam blockchain..

Kata Kunci: Secured; Certificate; Blockchain; Crypto; SHA-256

Abstract *− Important data must be secured, both digital data and physical data, especially for digital data, a security must be provided to store it. An example of one of the data that is very important in our lives is a Certificate. Certificates are important data that some people have for certain purposes, such as legality, claiming that we legally own something. In this research, the author will research, design and create a system that can submit Official Competition Certificate Data by relying on a technology model, namely blockchain. The system is conceptually designed and built from scratch to form a blockchain system that is similar to the original. In the final stage, System Testing and Evaluation will be carried out, whether the system is running according to expectations and the results of a data stored in the blockchain.*

Keywords*: Secured; Certificate; Blockchain; Crypto; SHA-256*

1. PENDAHULUAN

Data penting sudah seharusnya di amankan sebaik mungkin, baik data digital maupun data fisik, terlebih lagi pada data digital, sebuah keamanan harus di sediakan untuk menyimpan nya. Contoh salah satu data yang sangat penting di kehidupan kita adalah Sertifikat. Sertifikat merupakan data penting yang beberapa orang miliki untuk tujuan tertentu, contoh nya legalitas, mengklaim bahwa kita mempunyai sesuatu secara sah. Sertifikat di simpan dalam wujud fisik dan non fisik (yaitu bentuk digital), ketika sertifikat berupa data digital yang di simpan di dalam Komputer, maka keamanan yang di miliki oleh sistem komputer harus baik. Sekarang semua data sertifikat pada umumnya yang tersimpan di komputer, tersimpan pada komputer server, dan data sertifikat, dibentuk dan diletakan di dalam Basis Data Konvensional, yang di padukan dengan sistem manajemen nya. Basis Data ini memiliki kelemahan, ketika ada sebuah kejadian, data Sertifikat ini dapat di ubah oleh pihak yang tidak bertanggung jawab. Selain Basis Data, ada Alternatif Sistem penyimpanan yang lebih baik dan aman, Yaitu Sistem Blockchain, dimana sistem ini menawarkan konsep Sekumpulan data yang saling berkaitan dan bersamaan dengan validasi yang cukup ketat, yaitu menggunakan pendekatan Teknik Kriptografi. Maka dari itu, Sistem Blockchain akan coba kita terapkan dalam Sistem Penyimpanan Data Sertifikat Penghargaan Karyawan.

2. METODE

2.1 Metode Penelitian

Metodologi Penelitian ini menggunakan Metode Eksperimental, yakni metode yang mengandalkan beberapa pengujian yang sebelumnya belum atau bahkan jarang orang lain lakukan, pada kali ini Blockchain di buat menggunakan sistem yang di jalankan sendiri secara konseptual, tanpa menggunakan Framework atau contoh project yang sudah di buat sebelumnya.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 737-741

2.2. Metode Enkripsi

SHA-256 adalah fungsi hash kriptografi yang lebih baru dan lebih aman yang diusulkan pada tahun 2000 sebagai generasi baru fungsi SHA dan diadopsi sebagai standar FIPS pada tahun 2002. Algoritma SHA-256 menghasilkan nilai hash 256-bit dari padded 512-bit blok pesan, dan ukuran pesan asli hingga 264-1 bit. SHA-256 selalu menghitung hash 256-bit secara internal untuk keamanan, tetapi hasil ini dapat dipotong baik untuk pencetakan maupun penyimpanan 196 atau 128 bit. Dengan demikian, SHA-256 yang terpotong menghasilkan manfaat besar bagi kegunaan manusia dalam kutipan cetak, dan secara signifikan meningkatkan keamanan, dengan biaya pengurangan kecil dalam kinerja terkait MD5. Berbeda dengan algoritma MD5, SHA-256 terpotong tidak tunduk pada serangan yang dikenal. Untuk ukuran Algoritma SHA-256 menghasilkan nilai hash 256-bit dari blok pesan 512-bit empuk, dan ukuran pesan asli hingga 264-1 bit.

INPUT DATA	HASH OUTPUT (SHA-256)
My name is Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
My name is Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1ead4e15ac7f9
My name is Toby and this is my project	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfac14fadd143d212c

Gambar 1. Contoh Input dan Output Enkripsi SHA-256

3. ANALISA DAN PEMBAHASAN

Pada bagian ini berisi hasil dari kegiatan penelitian yang sudah dilakukan

3.1 Analisa Data

Rencana Sistem yang akan dibuat, dimana Sistem ini akan berbasis web dan Mobile, dimana di Web akan di gunakan oleh Admin Pembuat Sertifikat, untuk menggenerate dan Menyimpan Sertifikat Penghargaan Karyawan di Blockchain, dan di Mobile di gunakan Oleh pemilik sertifikat (Karyawan) untuk memvalidasi Sertifikat yang ia Pegang. Di Sistem Penyimpanan Sertifikat ini berbasis penyimpanan Blockchain dimana data di simpan di dalam skema Blockchain, yang berarti Data Sertifikat tersimpan secara Kriptografik, tidak bisa di palsukan, di duplikasi bahkan di hapus, dapat di verifikasi keaslian data Sertifikat Penghargaan Karyawan. Data yang pasti di pakai di Sistem ini Antara lain :

a. Data Admin
b. Data Karyawan
c. Data Pejabat
d. Data Sertifikat Penghargaan.

3.2 Basis Data

Sistem ini di bagi menjadi 2 Media penyimpanan, 1 Database dan 1 Blockchain. Untuk Data Admin, Karyawan, Pejabat di simpan di Database, sedangkan data Sertifikat di Simpan di Blockchain. Data pada Database data pendukung untuk melakukan input data Sertifikat di Blockchain.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 737-741

Tabel 1. Lokasi Penyimpanan Data

Database	Blockchain
Admin	Sertifikat Penghargaan Karyawan
Karyawan	
Pejabat	

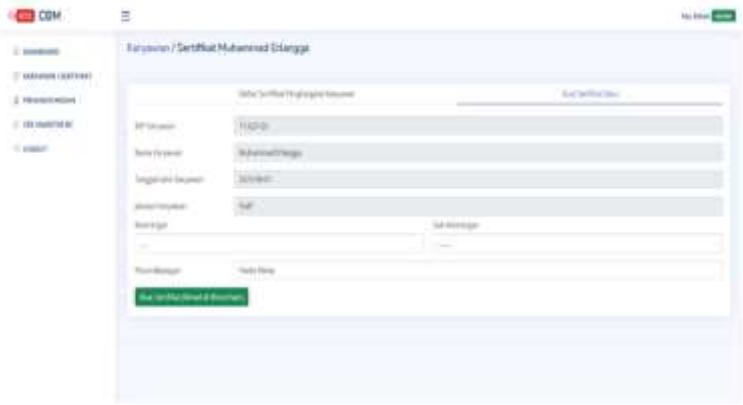
3.3 Basis Data

Sistem ini di bagi menjadi 2 Media penyimpanan, 1 Database dan 1 Blockchain. Untuk Data Admin, Karyawan, Pejabat di simpan di Database, sedangkan data Sertifikat di Simpan di Blockchain. Data pada Database data pendukung untuk melakukan input data Sertifikat di Blockchain.

3.4 Pembuatan dan Penyimpanan Sertifikat

Gambar 2. Daftar Sertifikat yang sudah terdaftar

Ini adalah daftar Sertifikat pada Sebuah Kompetisi, Data Sertifikat ini tersimpan pada Blockchain, dan cara mendapatkan data tersebut menggunakan url API. *http://${blockchain_ip}:5000/blockchain_get_by_id_karyawan*



Gambar 3. Form Pengisian Sertifikat

Ini adalah Halaman untuk Membuat Sebuah Sertifikat dan di Simpan di Blockchain (di mined), terdiri dari Kolom :

a. NIP Karyawan (Tidak dapat di Edit)

b. Nama Karyawan (Tidak dapat di Edit)

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 737-741

c. Tanggal Lahir Karyawan (Tidak dapat di Edit)

d. Jabatan Karyawan ((Tidak dapat di Edit)

e. Keterangan

f. Sub Keterangan

g. Penadatangan (Pejabat) Ketika Mengklik "Buat Sertifikat (Mined di Blockchain), maka data Form akan tersimpan pada database, di belakang layar, akan melakukan Request Post : http://${blockchain_ip}:5000/insert_new_certificate Menggunakan Metode POST.

```
#ADD NEW BLOCK AT BLOCKHAIN
@app.route("/insert_new_certificate", methods=['POST'])
def insert_new_block():
        now = datetime.now()
        localarray = bc.blockchain_data()
        nip_karyawan = request.form['nip_karyawan']
        nama_karyawan = request.form['nama_karyawan'] #FROM UI WEB
        tanggal_lahir_karyawan = request.form['tanggal_lahir_karyawan']
        jabatan_karyawan = request.form['jabatan_karyawan']
        keterangan = request.form['keterangan']
        sub_keterangan = request.form['sub_keterangan']
        nama_penandatangan = request.form['nama_penandatangan']
        owner_id = request.form['owner_id']
        jabatan_penandatangan = request.form['jabatan_penandatangan']
        prevHash = localarray[len(localarray) - 1]['hash']
        salt = "0601200"
        mined_at = now.strftime("%Y-%m-%d %H:%M:%S")

        attr = {
            'index' : len(localarray),
            'prev_hash' : prevHash,
            'nip_karyawan' : nip_karyawan,
            'nama_karyawan' : nama_karyawan,
            'tanggal_lahir_karyawan' : tanggal_lahir_karyawan,
            'jabatan_karyawan' : jabatan_karyawan,
            'keterangan' : keterangan,
            'sub_keterangan' : sub_keterangan,
            'nama_penandatangan' : nama_penandatangan,
            'owner_id' : owner_id,
            'jabatan_penandatangan' : jabatan_penandatangan,
            'mined_at' : mined_at,
            'hash' : hashlib.sha256(f'{prevHash}{nip_karyawan}{nama_karyawan}{
        }
```

Gambar 4. Form Pengisian Sertifikat

Pada sertifikat yang di input dari form sebelumnya, akan di proses pembuatan hash pada node Blockhain, dimana semua field dari sertifikat di jadikan 1 hash, lalu hash tersebut di letakan di field "prev_hash" (previous hash) Block selanjutnya, jadi jika ada perubahan data yang di sengaja, tidak valid, karena data hash nya sudah berubah.

Gambar 5. Contoh Sertifikat yang sudah di Generate

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 737-741

Sertifikat yang sudah di Download/Print, akan mengeluarkan Barcode yang dapat di scan, yang berisih Hash yang menggunakan Teknologi *SHA-256* dari sekumpulan data field Sertifikat itu sendiri.

4. KESIMPULAN

Blockchain menerapkan Sistem chaining Kriptografi menggunakan Metode Enkripsi SHA-256 yang sangat sulit di pecahkan dan di palsukan datanya dari pihak yang tidak bertanggung Jawab, Selain ter enkripsi juga saling berkaitan dengan seluruh data yang ada di dalam Blockchain. ID Pada Setiap Sertifikat sudah otomatis Generate dari Hasil mined pada blockchain dan Sifat nya unik, tidak perlu lagi menentukan bedasarkan Urutan ID Terakhir secara Manual. Pada Aplikasi Mobile yang berfungsi Memvalidasi Sertifikat yang di miliki karyawan, memiliki fitur untuk meng-scan Barcode Sertifikat dan Mevalidasi apakah Sertifikat Asli atau Palsu secara cepat dan tepat, jadi tidak perlu mengidentifikasi dan memvalidsi secara manual.

REFERENCES

Swastika, W. (2022). *Rancang bangun website akademik dengan penyimpanan sertifikat digital menggunakan teknologi blockchain*. Malang: Universitas Ma Chung.

Yusup, M. (2019). *Pemanfaatan teknologi blockchain pada program sertifikasi dosen*. Tangerang: Universitas Raharja.

Prasetyo, T. (2021). *Implementasi teknologi blockchain di perpustakaan: Peluang, tantangan, dan hambatan*. Pamulang: UIN Syarif.

Nurdany, A. (2022). *Blockchain dan inovasi teknologi keuangan Indonesia: Sebuah tinjauan khusus pada startup Alumnia*. Yogyakarta: Universitas Yogyakarta Sunan Kalijaga.

Aini, Q. (2021). *Aplikasi berbasis blockchain dalam dunia pendidikan dengan metode systematics review*. Tangerang: Universitas Raharja.

Liza, W., Suwanto, T., & Lengkey, C. (2022). Implementasi algoritma konsensus proof-of-work dalam blockchain terhadap rekam medis. Jurnal Pekommas, 7(1), 41-52. https://karya.brin.go.id/id/eprint/14673

Zufria, I., & Kom, M. (2019). Analisis algoritma SHA-256 pada proses mining teknologi blockchain bitcoin. Repository UIN Sumatera Utara. https://repository.uinsu.ac.id/id/eprint/4623

Dharmawan, A. (2023). Penerapan algoritme kriptografi SHA-256 dan AES-256 untuk pengamanan file pada PT Pelangi Sentral Kreasi. Jurnal Sistemasi, 1, 194-205.

Sulastri, S. (2018). Implementasi enkripsi data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada proses pengamanan kata sandi sistem penjadwalan karyawan. *Jurnal Teknik Elektro*, 7(1), https://journal.unnes.ac.id/nju/index.php/jte/article/view/18628.