PROGRAM KEGIATAN PENELITIAN

Penyimpanan Transkrip Nilai Semester Pada Ekosistem Blockchain : Studi Kasus Lingkungan Telkom University

Diusulkan oleh:
1103184150 / DENDI ARYA RADITYA PRAWIRA PUTRA (Teknik Komputer)
1103194142 / RENALDI AZHAR (Teknik Komputer)

SECURITY LABORATORY
UNIVERSITAS TELKOM
BANDUNG
2022

PENGESAHAN KEGIATAN PENELITIAN

1. Judul Kegiatan : Penyimpanan Transkrip Nilai Semester Pada Ekosistem Blockchain : Studi Kasus Lingkungan Telkom UniversityKetua Pelaksana Kegiatan
   a. Nama Lengkap :
   b. NIM :
   c. Jurusan :
   d. Universitas/Institut/Politeknik :
   e. Alamat Rumah dan No Tel/HP :
2. Alamat email :
3. Anggota Pelaksana Kegiatan/Penulis :
4. Dosen Pembina Laboratorium
   a. Nama Lengkap dan Gelar :
   b. NIDN :
   c. Alamat Rumah dan No Tel/HP :
5. JangkaWaktu Pelaksanaan : Bulan

Bandung, 17 Oktober 2022

Disetujui Oleh:

Koordinator Asisten Lab Security Laboratory	Ketua Pelaksana Kegiatan
Irene Gloria Paulina Nainggolan	Ketua
NIM 1103174282	NIM

Mengetahui,

Ketua Kelompok Keahlian	Dosen Pembina Lab Security Laboratory
Dr. Yudha Purwanto,S.T.,M.T.	**Muhammad Faris Ruriawan,S.T.,M.T.**
NIK 02770066	**NIP 18920117**

DAFTAR ISI

DAFTAR GAMBAR

RINGKASAN

Penelitian ini ditunjukan untuk merancang sebuah prototipe sistem yang dapat menyimpan dan memvalidasi transkrip nilai dengan memanfaatkan teknologi *blockchain*. Hal ini ditunjukan untuk mencegah adanya pemalsuan dokumen transkrip nilai yang marak terjadi belakangan ini. Sistem yang kami usulkan menggunakan teknologi Eteherum *blockchain* dan teknologi *smart contract* yang terdapat didalamnya untuk menyimpan nilai kedalam jaringan *blockchain*. Dengan memanfaatkan *blockchain* ini akan dapat menjamin integritas dan kesahan dari sebuah data. Dengan adanya pembuatan ini diharapkan aksi dalam pemalsuan transkrip nilai di kalangan masyarakat dapat dihindari dan tidak terjadi lagi.

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Latar belakang kami melakukan sebuah riset mengenai implementasi blockchain untuk verifikasi transkrip nilai adalah dikarenakan kami melihat pada tahun-tahun sebelumnya adanya ditemukan orang-orang yang menggunakan transkrip nilai palsu untuk mereka gunakan untuk melamar pekerjaan ataupun melamar CPNS[2], hal ini bukan saja hanya ada di Indonesia, melainkan seluruh negara pun ada saja oknum yang menggunakan transkrip nilai palsu mereka.

1.2 Pandangan penulis sebelumnya

Dalam makalah tugas akhir [3] diusulkan sebuah sistem yang menyimpan salinan file pdf dari transkrip nilai atau ijazah yang telah ditandatangani kedalam *blockchain*. Namun sistem yang ditawarkan penulis hanya berakhir pada proses verifikasi data apabila dibutuhkan. Penulis tidak memberikan solusi terhadap penyimpanan data agar dapat diambil kembali semisal dibutuhkan dikemudian hari.

1.3 Kondisi dan Potensi wilayah

Kondisi transkrip nilai saat ini mengharuskan seseorang atau sebuah lembaga untuk memverifikasikannya secara manual yang dimana akan memakan banyak waktu dan tidak efisiensi, untuk percobaan kali ini kami akan menerapkannya di lingkungan kampus Telkom University.

1.4 Manfaat Jangka Panjang

Manfaat jangka panjang dari riset ini adalah dapat digunakan sebagai referensi dalam riset-riset selanjutnya, selain itu pun dari riset ini diharapkan tidak adanya ditemukan lagi oknum-oknum yang menggunakan transkrip nilai palsu mereka di luar sana.

1.5 Luaran Kegiatan

Luaran dari kegiatan ini kami harapkan kami dapat lebih mengenal dan mengeksplorasi lagi lebih lanjut untuk penggunaan sistem *blockchain* ini, selai itu pun kami mengharapkan akan diterapkan sistem verifikasi pada transkrip

nilai tidak hanya di lingkungan kampus Telkom University tetapi dapat di adopsi secara nasional.

1.6 Manfaat Kegiatan

Manfaat dari kegiatan riset ini dapat dijadikan referensi dalam penerapan *blockchain* sebagai penyimpanan transkrip nilai mahasiswa yang aman dan terjamin keasliannya.

BAB 2
TINJAUAN PUSTAKA

1.1 Kondisi umum lingkungan

Di lingkungan Telkom Univerisity saat ini proses cetak transkrip nilai melalui igracias tidak memiliki proses untuk melakukan validasi. Oleh karenanya diperlukan suatu sistem yang dapat menjamin keaslian dari dokumen transkrip nilai tersebut dan dapat diakses oleh orang/institusi di luar lingkungan Telkom University.

1.2 Literatur yang terkait

Marc Eisenstadt, Manoharan Ramachandran, Niaz Chowdhury,2020, COVID-19 Antibody Test/Vaccination Certification: There's an App for That. Penelitian ini menggunakan desain berdasarkan (a) standar World Wide Web Consortium 2019 yang disebut 'Verifiable Credentials', (b) platform data pribadi terdesentralisasi Tim Berners-Lee 'Solid', dan (c) blockchain berbasis Konsorsium Ethereum. Kerjakan (d) skenario kasus penggunaan yang masuk akal, lalu (e) jelaskan langkah-langkah 'onboarding' dan sertifikasi kunci secara rinci; dan (f) menyediakan uji *benchmark* untuk mengantisipasi kinerja penskalaan. Hasil dari penelitian ini meliputi karakteristik aplikasi 'Covid-19 antibody test certificate' (CAT/VC) yang dibangun di atas Verifiable Credentials dan Solid framework, dan hasil *benchmarking* kinerja, yang membandingkan antara waktu untuk mengeluarkan 100 permintaan paralel untuk menerbitkan sertifikat ,memverifikasi, mengunggah data, dan ping standar dasar.

Ishaq Azhar Mohammed, 2019, A Systematic Literature Mapping On Secure Identity Management Using Blockchain Technology. Belakangan ini banyak muncul kekhawatiran signifikan terkait dengan revolusi digital, terutama terkait dengan pertukaran informasi, dan layanan dikarenakan kebanyakan hal tersebut dilakukan melalui organisasi digital yang tersentralisasi. Dalam paper 9 ini pernulis mengangkat isu terkait pengembangan metoda dalam penyimpanan, pertukaran dan validasi data yang bersifat sensitif. Pada dasrnya teknologi *blockchain* memungkinkan tercapainya prinsip dasar dari identitas yang diatur sendiri. Hal tersebut dapat tercapai tentunya dikarenakan model dari jaringan blockchain yang terdesentralisasi.

BAB 3
METODE PELAKSANAAN

3.1. Analisis kebutuhan

Pada dasarnya sistem yang akan dirancang harus bisa menyelesaikan permasalahan yang telah diidentifikasi sebelumnya. Secera umum penulis disini mengklasifikasikan kebutuhan aplikasi sebagai berikut :

1. Sistem dapat melakukan prosses *issuing* transkrip nilai dan memasukannya ke dalam jaringan *blockchain*.
2. Melakukan verifikasi keaslian dari dokuman transkrip nilai.
3. Melakukan pencarian terhadap dokumen transkrip nilai berdasarkan nomor induk mahasiswa.

3.2. Arsitektur sistem yang diusukan

Pada bagian ini penulis akan memaparkan rancangan sistem yang diusulkan dalam riset ini. Sistem ini nantinya akan dibangun menggunakan diatas jaringan *blockchain Ethereum* yang mana nantinya akan memanfaatkan *smart contract* untuk melakukan fungsionalitas secara otomatis pada jaringan *blockchain* scara aman dan *trustless*. Selain itu untuk menyimpan salinan dari transkrip nilai dingunakan penyimpanan external yang akan mengkaitkan hash dari NIM pengguna ke data transkrip nilai.

Rancangan sistem yang diusulkan terdiri atas dua proses utama :

1. Proses *issuing* transkrip nilai
2. Proses verifikasi transkrip nilai
3. Proses mendapatkan transkrip nilai

Untuk mendukung proses tersebut digunakan fitur *smart contract* pada *Ethereum*. Nama dari *Smart contract* yang akan dibuat adalah *certificate_sc*. *Certificate_SC* nantinya akan digunakan untuk menyimpan hash dari sertifikat yang telah ditandangani sebelumnya oleh *issuer*. Pada *certificate_sc* akan meiliki

mapping yang diberi nama *studentToTranscript* yang akan menyimpan hash NIM mahasiswa dengan tipe data sturktur yang memliki anggota *hash* dari transkrip nilai dan *time stamp* dari transaksi. *Certificate_sc* juga memiliki sebuah variable array yaitu *transcriptHashStorge* yang digunakan untuk menyimpan hash dari data transkrip nilai sehingga memudahkan dalam proses verifikasi nantinya. Selanjutnya *Certificate_sc* memiliki fungsi sebagai berikut :

1. **Register Transkrip**

Algoritma :

```
Struct Transcript {
    transcript:bytes32
    timestamp:uint
}
 Transcript private transcriptData
register_transcript(transcript_hash,student_id)
if sender == owner
        if  studentToTranscript[student_id] exist
            If studentToTranscript[student_id] contains transcript
                return false
            else
                studentToTranscript[student_id].append(transcriptData)
                transcriptHashStorge.append(transcript_hash)
                return true

        else
                newTranscriptArray : Array of bytes32
```

neTranscriptArray.append(transcriptData)

Map newTranscriptArray to student_id

transcriptHashStorge.append(transcript_hash)

return true

end

else

return false;

End

2. **Mengambil transkrip nilai mahasiswa**

Algoritma

retrieve_student_transcript(student_id)

if sender == owner and studentToTranscript[student_id] exist

return studentToTranscript[student_id]

else

return false

end

3. **Verifikasi transkrip nilai mahasiswa**

Algoritma

verify_transcript(transcript)

If transcriptHashStorge.contains(transcript)

Return true

Else

Return false

End

4. **Mengambil *public key* rektor/dekan**

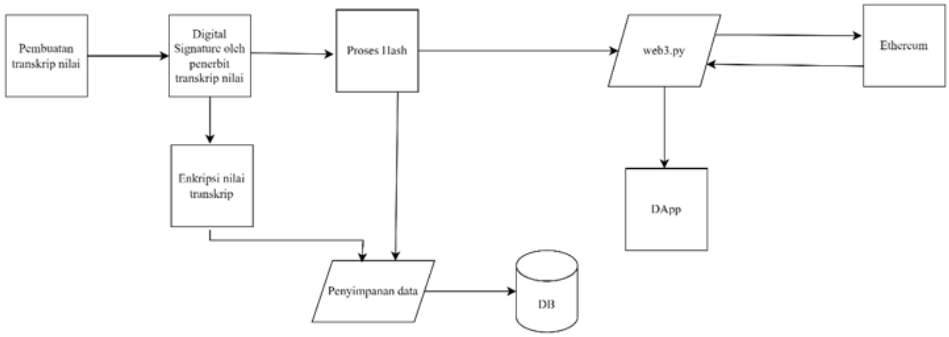
Algoritma

get_public_key

return publicKey

Selanjutnya masing – masing proses dapat dijelaskan sebagai berikut :

a. Proses *issuing* transkrip nilai



Flowchart 1 Skematik proses issuing transkrip nilai

1. Pembuatan transkrip nilai

Pada tahap ini admin membuat dokumen transkrip nilai elektronik, dengan memasukkan informasi mahasiswa. Nantinya file berformat pdf akan dihasilkan pada akhir proses *issuing* transkrip nilai dan sebuah *QR code* sebagai tanda tangan digital. Sedangkan pada sistem untuk penyimpanan data akan disimpan dalam bentuk JSON.

2. Digital Sign

Pada proses ini data JSON dari nilai transkrip yang telah dibuat ditandatangani secara digital, menggunakan algoritma *asymmetric*. Pada bagian ini akan dimanfaatkan teknologi JSON Web Token untuk melakukan tanda tangan digital.

JSON data akan ditandantangin menggunakan *private key* milik rector/dekan yang memiliki wewenang dalam penerbitan transkrip nilai.

3. Enkripsi transkrip nilai

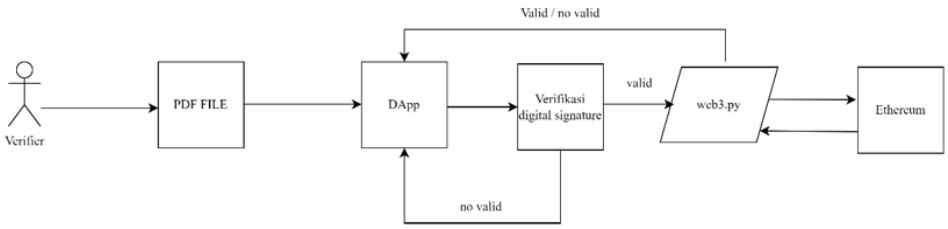
Dokumen yang telah ditandantanani selanjutnya dienkripsi dengan *public key* milik *issuer* dan disimpan kedalam eksternal *database*. Dokumen transkrip nilai yang disimpan di dalam eksternal *database* akan memiliki relasi dengan *hash* dari dokumen transkrip nilai sehingga nantinya apabila dibutuhkan *admin* dapat melakukan proses pengambilan transkrip nilai.

4. Web3.py

Web3.py memiliki peran dalam menghubungkan sistem ke *blockchain*. Pada proses ini dilakukan penyimpanan data transkrip yang telah di-*hash* ke jaringan *Ethereum blockchain*.

Setelah semua proses dilakukan sistem akan menampilkan status dari transaksi ke *smart contract certificate_sc*. Apabila sukses sistem akan menampilkan nilai *hash* dari transkrip nilai dan juga *transaction hash*. Sistem juga akan memperoses data JSON dari transkrip nilai kedalam bentuk PDF dengan sebuah *QR code* dari data JSON teresbut untuk melakukan verifikasi apabila dibutuhkan nantinya.

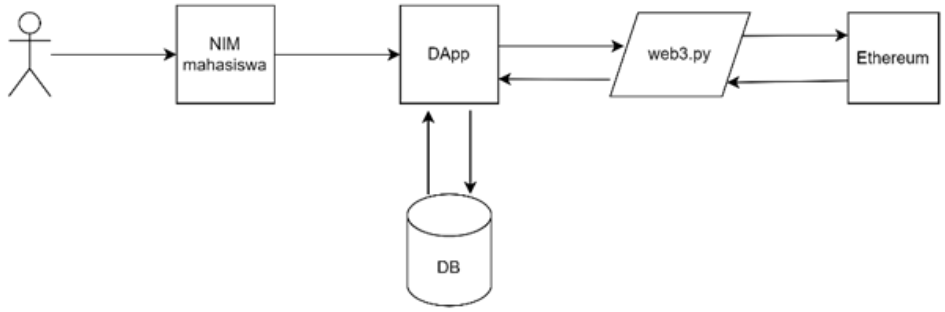
b. Proses verifikasi transkrip nilai



Flowchart 2 Skematik proses verifikasi transkrip nilai

Proses verifikasi dimulai dari mengirimkan dokumen transkrip nilai ke DApp. Selanjutnya sistem akan melakukan verifikasi *digital signature*. Apabila hasilnya valid sistem akan melakukan pengecekan dari nilai *hash* dokumen. Apabila nilai *hash* ditemukan pada jaringan *blockchain* maka sistem akan menyatakan *valid*.

c. Proses mendapatkan transkrip nilai



Flowchart 3 Skematik proses untuk mendapatkan transkrip nilai

Proses untuk mengambil transkrip nilai dilakukan dengan melakukan *input* NIM ke DApp. NIM yang diinput akan di-*hash* lalu sistem akan mencari catatan transkrip nilai di *blockchain*. Apabila tersedia makan akan dikembalikan *array hash* dari transkrip nilai mahasiswa terkait. Selanjutnya sistem akan mencari data di *database* menggunakan *hash* transkrip yang tersedia, dan akan diperoleh data yang telah di-enkripsi. Menggunakan *private key* milik *issuer*. Sistem nantinya akan mengembalikan *file* dalam bentuk PDF dari data tersebut.

DAFTAR PUSTAKA

[1] Taiwan zhi shi chuang xin xue hui, *Applied system innovation : proceedings of 4th IEEE International Conference on Applied System Innovation 2018 (IEEE ICASI 2018) : Chiba, Japan, April 13-17, 2018*.

[2] Thomas T. Limahekin, "Nekad! Sejumlah Pendaftar CPNS di Kepri Gunakan Transkrip Nilai Palsu Artikel ini telah tayang di TribunBatam.id dengan judul Nekad! Sejumlah Pendaftar CPNS di Kepri Gunakan Transkrip Nilai Palsu, https://batam.tribunnews.com/2014/10/03/nekad-sejumlah-pendaftar-cpns-di-kepri-gunakan-transkrip-nilai-palsu.," *Tribun News Batam*, Oct. 03, 2014. Nekad! Sejumlah Pendaftar CPNS di Kepri Gunakan Transkrip Nilai Palsu Artikel ini telah tayang di TribunBatam.id dengan judul Nekad! Sejumlah Pendaftar CPNS di Kepri Gunakan Transkrip Nilai Palsu, https://batam.tribunnews.com/2014/10/03/nekad-sejumlah-pendaftar-cpns-di-kepri-gunakan-transkrip-nilai-palsu. (accessed Jan. 30, 2022).

[3] Nero Chaniago, Parman Sukarno, Aulia Arif Wardana," Blockchain dan Smart Contract untuk Keamanan Dokumen Elektronik: Studi Kasus Ijazah dan Transkrip". Tugas akhir.Bandung: Telkom University.

[4] *A Systematic Literature Mapping On Secure Identity Management Using Blockchain Technology.* **Mohammed, Ishaq Azhar.** s.l. : ScienceDirect, 2021.

LAMPIRAN

Lampiran 1 : Biodata Ketua, Anggota dan Dosen Pembimbing
Biodata Ketua

A. Identitas Diri

1.	Nama Lengkap (dengan gelar)	Renaldi Azhar
2.	Jenis Kelamin	Laki-laki
3.	Program Studi	Teknik Komputer
4.	NIM	1103194142
5.	Tempat dan Tanggal Lahir	Bandung, 20 November 2001
6.	*E-mail*	renaldivanza@student.telkomuniversity.ac.id
7.	Nomor Telepon/HP	+6282213874993

B. Riwayat Pendidikan

	SD	**SMP**	**SMA**
Nama Institusi	SDS Asy-Syifa 1	SMPN 30 Bandung	SMAN 25 Bandung
Jurusan			
Tahun Masuk-Lulus			

C. Pemakalah Seminar Ilmiah *(Oral Presentation)*

No	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat

D. Penghargaan 10 Tahun Terakhir

No.	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam kegiatan penelitian ini.

Bandung, 17 Oktober 2019
Pengusul,

(Ketua)

Biodata Anggota 1

A. Identitas Diri

1.	Nama Lengkap (dengan gelar)	Dendi Arya Raditya Prawira Putra
2.	Jenis Kelamin	Laki - laki
3.	Program Studi	S1 Teknik Komputer
4.	NIM	1103184150
5.	Tempat dan Tanggal Lahir	Ciamis, 29 September 2001
6.	*E-mail*	dendiaryar@student.telkomuniversity.ac.id
7.	Nomor Telepon/HP	081339419724

B. Riwayat Pendidikan

	SD	**SMP**	**SMA**
Nama Institusi	SDN 01 Ampenan	SMPN 02 Mataram	SMAN 02 Mataram
Jurusan			
Tahun Masuk-Lulus	2007-2012	2012-2015	2015-2018

C. Pemakalah Seminar Ilmiah *(Oral Presentation)*

No	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat

D. Penghargaan 10 Tahun Terakhir

No.	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam kegiatan penelitian ini.

Bandung, 17 Oktober 2019
Pengusul,

(Anggota 1)

Biodata Dosen Pembina Laboratorium

A. Identitas Diri

1.	Nama Lengkap (dengan gelar)	
2.	Jenis Kelamin	
3.	Program Studi	
4.	NIDN	
5.	Tempat dan Tanggal Lahir	
6.	*E-mail*	
7.	Nomor Telepon/HP	

B. Riwayat Pendidikan

	S1	**S2**	**S3**
Nama Institusi			
Jurusan			
Tahun Masuk-Lulus			
Judul Skripsi / Tesis / Disertasi			
Nama Pembimbing / Promotor			

C. Pemakalah Seminar Ilmiah *(Oral Presentation)*

No	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat

D. Penghargaan 10 Tahun Terakhir

No.	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila dikemudian hari ternyata dijumpai ketidaksesuaian dengan kenyataan, saya sanggup menerima sanksi. Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam kegiatan penelitian ini.

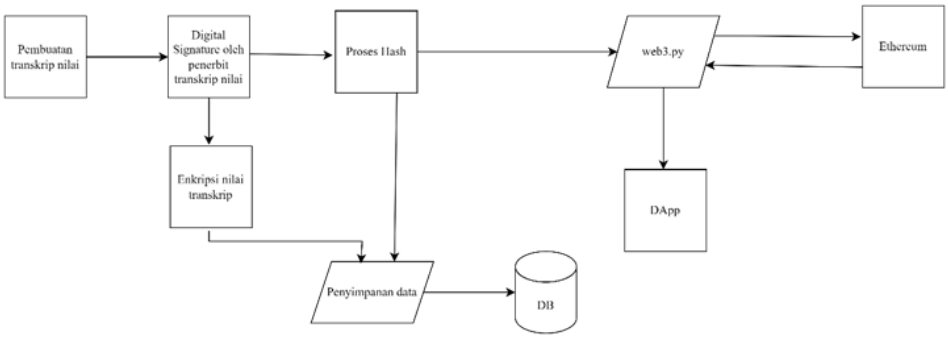
Kota, Tanggal-Bulan-Tahun
Pengusul,

(Nama Lengkap)
NIDN.

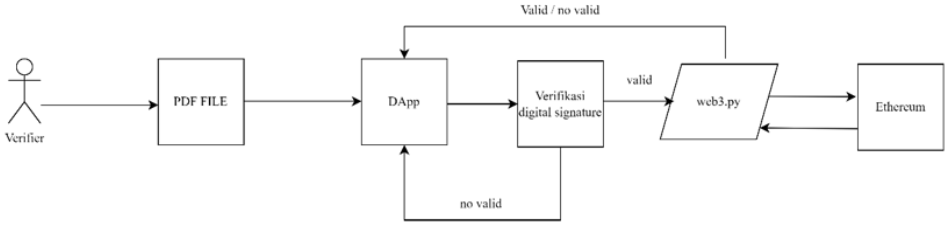
Lampiran 2. Susunan Organisasi Tim Kegiatan dan Pembagian Tugas

NO	Nama / NIM	Program Studi	Bidang Ilmu	Alokasi Waktu (jam/minggu)	Uraian Tugas
1					
2					
3					

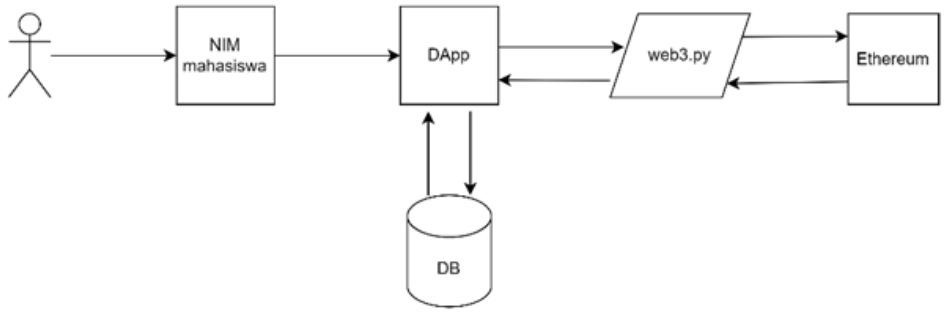
Lampiran 3. Gambaran Teknologi yang Hendak Diterapkembangkan



Flowchart 4 Proses issuing transkrip nilai



Flowchart 5 proses verifikasi transkrip nilai



Flowchart 6 proses mendapatkan transkrip nilai