

Implementasi Sistem Pendeteksi Ijazah dan Transkrip Palsu dengan Menggunakan IPFS dan *Smart Contract Blockchain*

Proposal Tugas Akhir

Kelas MK Penulisan Proposal (CCH4A3)

1301174433

Muhammad Danil Muis



Program Studi Sarjana Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2020

Lembar Persetujuan

Implementasi Sistem Pendeteksi Ijazah dan Transkrip Palsu dengan Menggunakan IPFS dan *Smart Contract Blockchain*

Implementation of Dummy Education Certificate and Transcript Detection System Using IPFS and Smart Contract Blockchain

NIM : 1301174433

Muhammad Danil Muis

Proposal ini diajukan sebagai usulan pembuatan tugas akhir pada

Program Studi S1 Informatika

Fakultas Informatika Universitas Telkom

Bandung, November 2020

Menyetujui,

Calon Pembimbing I

Calon Pembimbing II

Parman Sukarno, S.T., M.Sc., Ph.D
NIP.

Aulia Arif Wardana, S.Kom., M.T.
NIP.

ABSTRAK

Ijazah merupakan surat izin yang diberikan sebagai tanda tamat belajar. Peran ijazah sangat dibutuhkan terutama dalam jabatan pekerjaan. Pentingnya ijazah menyebabkan maraknya kasus pemalsuan ijazah maupun transkrip yang berisi kumpulan nilai. Dalam mengatasi permasalahan tersebut, Lembaga Layanan Pendidikan Tinggi (LL Dikti) meluncurkan program Penomoran Ijazah Nasional (PIN) dan Sistem Verifikasi Ijazah Elektronik (SIVIL). Solusi yang ditawarkan oleh pemerintah masih memiliki kekurangan dimana sistem rentan terhadap serangan SQLInjection yang mengakibatkan data hilang ataupun rusak. Oleh karena itu, dibutuhkan sistem yang dapat menyimpan data ijazah dan transkrip dengan sistem terdistribusi. Salah satu hasil dari perkembangan teknologi adalah *Inter Planetary File System* (IPFS). IPFS memberikan jaminan yang lebih aman untuk penyimpanan data karena menggunakan arsitektur terdistribusi. Pada tahun 2009, teknologi baru bernama Blockchain ditemukan dan semakin populer seiring dengan perkembangan Bitcoin. Blockchain menyimpan data dengan lebih aman sehingga tidak dapat dirusak atau dipalsukan. Dengan memanfaatkan teknologi Blockchain dan IPFS, maka penelitian ini akan membangun suatu sistem yang dapat mendeteksi ijazah dan transkrip palsu. Selain itu, penelitian ini juga akan melakukan pengujian kualitas layanan dengan menganalisis *Quality of Service* (QoS) dari sistem yang dibangun. Hal ini untuk menguji keterkaitan antara kualitas layanan yang ditawarkan dengan jumlah node pada sistem. Penelitian ini diharapkan mampu meminimalisir kasus pemalsuan ijazah dengan cara meningkatkan keamanan sistem.

Kata Kunci : *Blockchain, IPFS, Ijazah, QoS.*

DAFTAR ISI

Lembar Persetujuan.....	ii
ABSTRAK.....	iii
BAB I.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan Penelitian.....	2
1.4. Batasan Masalah.....	3
1.5. Rencana Kegiatan.....	3
1.5.1. Perumusan masalah.....	3
1.5.2. Studi literatur	3
1.5.3. Perancangan arsitektur sistem.....	4
1.5.4. Pengimplementasian sistem.....	4
1.5.5. Pengujian sistem	4
1.5.6. Evaluasi pengujian sistem.....	4
1.5.7. Penyusunan Dokumen Akhir	4
1.6. Jadwal Kegiatan	5
BAB II.....	6
2.1. Penelitian Sebelumnya	6
2.2. Dasar Teori	11
2.2.1. Ijazah.....	11
2.2.2. Penomoran Ijazah Nasional (PIN) dan Sistem Verifikasi Ijazah Secara Elektronik (SIVIL).....	11
2.2.3. Blockchain	11
2.2.4. Ethereum.....	12
2.2.5. <i>Smart Contract</i>	13
2.2.6. <i>Interplanary File System (IPFS)</i>	13
2.2.7. <i>Quality of Service (QoS)</i>	13
BAB III	15
3.1. Perancangan Sistem.....	15
3.2. Alur Sistem.....	16
3.3. Skenario Pengujian.....	17
DAFTAR PUSTAKA	18

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi informasi menghasilkan beragam produk teknologi yang sangat canggih. Namun, produk hasil perkembangan teknologi tidak selamanya digunakan secara bijak. Pertumbuhan tingkat kejahatan berbanding searah dengan tingkat kemajuan teknologi [1]. Oknum – oknum yang ingin meraup keuntungan material sering kali melakukan penyelewengan dokumen cetak seperti ijazah. Menurut KBBI, ijazah merupakan surat izin yang diberikan sebagai tanda tamat belajar [2]. Pada tahun 2018, berdasarkan investigasi yang dilakukan oleh Tirto terdapat 873 ijazah yang diproduksi oleh kampus swasta di Tangerang. Namun, mahasiswa yang lulus hanya 145 orang, sehingga terdapat 728 ijazah palsu yang diterbitkan [3].

Dalam menyikapi permasalahan tersebut, Lembaga Layanan Pendidikan Tinggi (LL Dikti) menggagas kebijakan Penomoran Ijazah Nasional (PIN) sejak tahun 2017 [4]. Solusi lain yang diterapkan oleh LL Dikti adalah Sistem Verifikasi Ijazah Secara Online (SIVIL) yang terintegrasi dengan Pangkalan Data Pendidikan Tinggi (PD Dikti) secara online [5]. Sayangnya sistem yang dibangun masih menggunakan penyimpanan secara terpusat sehingga rentan terhadap peretasan yang dapat mengakibatkan perubahan data, kerusakan bahkan kehilangan data. Selain itu, penggunaan ijazah dan transkrip berbentuk cetak juga memiliki kelemahan seperti kerusakan dan kehilangan dokumen.

Pada penelitian ini akan membahas tentang implementasi sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain*. *InterPlanetary File System* (IPFS) merupakan *distributed file system* yang bersifat *Peer to Peer* (P2P) dengan tujuan untuk menggantikan HTTP (*Hypertext Transfer Protocol*). HTTP dianggap gagal untuk memanfaatkan *file* dengan teknik terdistribusi. Hal ini disebabkan HTTP yang biasa digunakan ditemukan pada tahun 1997, sedangkan teknik terdistribusi baru ditemukan sekitar tahun 2000. Perubahan infrastruktur web sulit dilakukan karena besarnya skala

dari HTTP. IPFS berusaha untuk menghubungkan semua perangkat komputasi dengan sistem *file* yang sama dan memberikan kebaruan dalam pengalaman pengguna (*user experience*) [6]. Selain IPFS, penelitian ini juga menggunakan *blockchain* dan *smart contract* yang terintegrasi. Hal ini akan memberikan keuntungan dimana transaksi *peer to peer* dan *database* dapat dikelola secara aman dan terpercaya [7].

Penelitian ini juga akan melakukan pengujian performansi *Quality of Service* (QoS) pada sistem pendeteksi ijazah dan transkrip palsu dengan IPFS dan *smart contract blockchain*. QoS merupakan metode pengukuran tentang seberapa baik jaringan yang digunakan dan suatu usaha untuk mendefinisikan karakteristik dari suatu layanan [8]. Analisis ini akan menghasilkan waktu yang dibutuhkan dalam proses pengiriman data ke penerima (*throughput*), lama waktu yang dibutuhkan pada proses pengiriman (*delay*) dan banyaknya paket yang hilang dalam proses transmisi (*packet loss*).

1.2. Rumusan Masalah

Pemalsuan ijazah dan transkrip masih marak dilakukan. Dalam mengatasi hal tersebut Lembaga Layanan Pendidikan Tinggi (LL Dikti) meluncurkan Penomoran Ijazah Nasional (PIN) dan Sistem Verifikasi Ijazah Secara Online (SIVIL). Solusi ini masih menimbulkan masalah lain dimana sistem penyimpanan terpusat rentan terhadap serangan SQLInjection. Dengan demikian rumusan masalah yang diangkat dalam penelitian ini adalah membangun sistem pendeteksi ijazah dan transkrip palsu dengan penyimpanan terdistribusi menggunakan IPFS dan *smart contract blockchain*. Arsitektur terdistribusi ini terdiri dari beberapa nodes. Oleh karena itu, dibutuhkan pengujian *Quality of Service* (QoS) untuk mengetahui pengaruh jumlah nodes pada performansi sistem.

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Membangun sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain*.

2. Mengetahui performa *Quality of Service* (QoS) pada sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain*.
3. Mengetahui pengaruh jumlah *node* pada *cluster* terhadap performa *Quality of Service* (QoS) pada sistem pendekteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain*.

1.4. Batasan Masalah

Batasan masalah dari penelitian ini adalah :

1. Sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain* akan menggunakan dua sampai lima *node*.
2. Parameter QoS yang akan dianalisis adalah *throughput*, *delay* dan *packet loss*.

1.5. Rencana Kegiatan

Rencana kegiatan yang akan dilakukan dalam penelitian tugas akhir ini adalah sebagai berikut :

1.5.1. Perumusan masalah

Penelitian ini diawali dengan membuat rumusan masalah yang akan dibahas. Hal ini bertujuan untuk menentukan pedoman pembahasan yang akan dijabarkan dalam penelitian ini. Berdasarkan latar belakang yang sudah disimpulkan, maka rumusan masalah penelitian ini adalah implementasi sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain* serta menganalisis performansi QoS dari sistem yang sudah diimplementasikan.

1.5.2. Studi literatur

Pada tahap ini, peneliti melakukan pengumpulan data – data yang berkaitan dengan IPFS, *smart contract*, *blockchain* dan QoS. Data – data pendukung ini diperoleh dari jurnal, buku maupun artikel. Tujuan dari tahap ini adalah untuk memperkuat permasalahan yang diangkat pada penelitian ini serta menjadi dasar untuk melakukan pengembangan selanjutnya.

1.5.3. Perancangan arsitektur sistem

Pada tahap ini, peneliti akan membuat rancangan sistem pendeteksi ijazah dan transkrip palsu dengan menggunakan IPFS dan *smart contract blockchain*.

1.5.4. Pengimplementasian sistem

Pada tahap ini dilakukan pengimplementasian terkait masalah yang diangkat sesuai dengan arsitektur sistem yang sudah dirancang sebelumnya.

1.5.5. Pengujian sistem

Pada tahap ini, peneliti akan membuat replika dari ijazah/transkrip dan mengirimkan ijazah/transkrip ke IPFS. Selain itu, peneliti juga akan melakukan verifikasi ijazah/transkrip yang dihasilkan oleh sistem. Pengujian akan dilakukan sebanyak 20 kali untuk setiap jumlah *node*.

1.5.6. Evaluasi pengujian sistem

Jika sistem sudah berjalan dengan baik dan proses pengambilan data sudah selesai dilakukan, maka tahap selanjutnya adalah melakukan evaluasi pengujian sistem. Pada tahap ini akan dilakukan perhitungan nilai *throughput*, *delay* dan *packet loss*. Pengujian akan dilakukan dengan jumlah *node* yang berbeda. Nilai yang didapat dari hasil perhitungan akan dievaluasi dengan menggunakan standar QoS oleh TIPHON.

1.5.7. Penyusunan Dokumen Akhir

Pada tahap ini, peneliti akan melakukan penyusunan dokumen akhir yang berisi hasil dari penelitian yang sudah dilakukan.

1.6. Jadwal Kegiatan

Penelitian ini akan dikerjakan dengan rencana jadwal kegiatan yang dipaparkan pada **Tabel 1.1** berikut :

Tabel 1.1 Jadwal Kegiatan Pengerjaan Tugas Akhir

Kegiatan	Bulan ke -						
	1	2	3	4	5	6	7
Perumusan masalah							
Studi literatur							
Perancangan arsitektur sistem							
Pengimplementasian sistem							
Pengujian sistem							
Evaluasi pengujian sistem							

BAB II

KAJIAN PUSTAKA

2.1. Penelitian Sebelumnya

Pada penelitian yang akan dilakukan oleh peneliti berkaitan dengan implementasi sistem untuk memverifikasi ijazah dan transkrip serta penggunaan teknologi IPFS dan *smart contract blockchain* untuk penyimpanan *file*. Penelitian ini memiliki perbedaan dibandingkan penelitian sebelumnya. Adapun perbedaan tersebut dari segi masalah yang diangkat, metode yang digunakan serta teknologi yang diimplementasikan. Berikut ini beberapa penelitian sebelumnya yang berkaitan dengan penelitian yang akan diangkat oleh peneliti.

Pada penelitian dengan judul “Analisis dan Implementasi Komunikasi Antar *Node* IPFS (*Interplanary File System*) Pada *Smart Contract Ethereum*” mengimplemmentasikan sistem berbasis *web* untuk menyimpan *file*. Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) untuk membangun sistem. Hasil dari penelitian ini adalah aplikasi *web* terdistribusi dengan menggunakan IPFS dan *smart contract* untuk menyimpan *file*. Penelitian ini memiliki kelebihan dimana pengujian *Quality of Service* (QoS) menggunakan kapasitas *file* yang bervariasi. Namun, penelitian ini tidak membahas berapa banyak gas yang digunakan untuk setiap transaksi serta pengujian QoS tidak dijelaskan metodenya [9].

Pada penelitian dengan judul “*Blockchain-Based, Decentralized Access Control for IPFS*” membahas tentang implementasi aplikasi untuk menambahkan *file* dengan informasi sensitif dan membatasi akses ke *file* tersebut. Penelitian ini menggunakan Acl-IPFS untuk meningkatkan keamanan. Kelebihan dari penelitian ini adalah keamanan lebih terjamin. Namun, penggunaan Acl-IPFS memberikan perbedaan kecepatan yang signifikan dalam penyimpanan ke IPFS. Selain itu, pengujian juga hanya dilakukan dengan tiga kapasitas *file* yang berbeda [10].

Pada penelitian dengan judul “Validasi Ijazah dengan Menggunakan *Watermarking* dan *QR Code* pada Fakultas Teknik UNIS Tangerang” membahas tentang implementasi sistem yang digunakan untuk melakukan validasi ijazah.

Sistem ini menggunakan *watermark* dan *QR code* dan pengujian sistem menggunakan metode kuisioner. Kelebihan dari penelitian ini adalah menggunakan dua pengamanan yaitu *watermark* dan *QR code*. Namun, aplikasi yang dirancang masih berbasis *desktop* dan sistem tidak terdistribusi [11].

Pada penelitian dengan judul “Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah” yang membahas tentang sistem verifikasi ijazah dengan *digital signature* menggunakan RSA dan SHA-512. Metode yang digunakan untuk membangun sistem ini adalah *waterfall*. Kelebihan penelitian ini adalah algoritma yang diterapkan memiliki hasil uji yang aman. Namun, sistem yang dibangun tidak terdistribusi dan dokumen tanda tangan digital yang disisipkan sangat banyak [12].

Tabel 2.1. Perbandingan Referensi

No.	Penulis	Judul	Metode	Hasil	Kelebihan	Kekurangan
1.	Achmad Muhaimin Aziz, dkk	Analisis dan Implementasi Komunikasi Antar Node IPFS (<i>Interplanetary File System</i>) Pada <i>Smart Contract</i> <i>Etherum</i> [9]	Metode yang digunakan dalam mendukung penelitian ini adalah <i>Network Development Life Cycle</i> (NDLC) untuk membangun sistem.	Hasil dari penelitian ini adalah aplikasi <i>web</i> yang bersifat <i>Dapp</i> untuk menyimpan file dengan menggunakan IPFS dan <i>smart contract</i> . Penelitian ini juga menganalisis QoS level 0, 1, 2 dengan hasil nilai indeks 3 dengan kategori "Memuaskan".	Penelitian ini melakukan pengujian dan menganalisis jenis file yang bervariasi.	Hasil penelitian belum memiliki fungsionalitas sistem yang jelas.

2.	Mathis Steichen, dkk.	<i>Blockchain-Based, Decentralized Access Control for IPFS</i> [10]	Penelitian ini menggunakan Acl-IPFS untuk meningkatkan keamanan terutama dalam mengakses <i>file</i> dengan informasi yang sensitif.	Hasil dari penelitian ini adalah membangun aplikasi untuk menambahkan <i>file</i> yang sensitif dan membatasi akses ke <i>file</i> tersebut.	Penelitian ini menggunakan Acl-IPFS untuk menangani <i>access control list</i> .	Pengujian sistem hanya menggunakan tiga kapasitas <i>file</i> yang berbeda. Penggunaan Acl-IPFS membuat perbedaan yang signifikan dalam penyimpanan file ke IPFS.
3.	Asep Hardiyanto Nugroho	Validasi Ijazah dengan Menggunakan <i>Watermarking</i> dan QR <i>Code</i> pada Fakultas Teknik UNIS Tangerang [11]	Metode yang digunakan untuk memvalidasi ijazah digital adalah <i>watermark</i> dan QR <i>code</i> . Pengujian sistem menggunakan metode kuisioner.	Hasil dari penelitian ini adalah membangun sistem yang digunakan untuk melakukan validasi ijazah dengan menggunakan <i>watermark</i> dan QR <i>cod</i> .	Menggunakan dua pengamanan yaitu QR <i>code</i> dan <i>watermarking</i> .	Aplikasi yang dirancang berbasis <i>desktop</i> . Sistem yang dibangun juga tidak terdistribusi.

4.	Fitri Nuraeni, dkk.	Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah [12]	Metode yang digunakan untuk membangun sistem adalah metode <i>waterfall</i> .	Hasil dari penelitian ini adalah sistem verifikasi ijazah dengan menggunakan algoritma RSA dan SHA-512 untuk <i>digital signature</i> .	Penerapan algoritma RSA dan SHA-512 untuk <i>digital signature</i> telah diuji dan aman.	Dokumen tanda tangan digital yang disisipkan sangat banyak. Sistem yang dibangun tidak terdistribusi.
----	---------------------	--	---	---	--	---

2.2. Dasar Teori

2.2.1. Ijazah

Menurut KBBI, Ijazah adalah surat izin yang diberikan sebagai tanda tamat belajar [2]. Menurut peraturan Menteri Pendidikan dan Kebudayaan Nomor 81 tahun 2004, Ijazah adalah dokumen pengakuan prestasi belajar dan/atau penyelesaian suatu jenjang pendidikan tinggi setelah lulus ujian yang diselenggarakan oleh perguruan tinggi [13]. Ijazah dapat diperoleh seseorang jika sudah menyelesaikan pendidikan formal, seperti Sekolah Dasar (SD) selama enam tahun, Sekolah Menengah Pertama (SMP) selama tiga tahun, Sekolah Menengah Atas (SMA) selama tiga tahun bahkan perguruan tinggi. Pentingnya kepemilikan ijazah didasari sebagai bukti yang digunakan untuk beberapa urusan penting terutama jabatan pekerjaan.

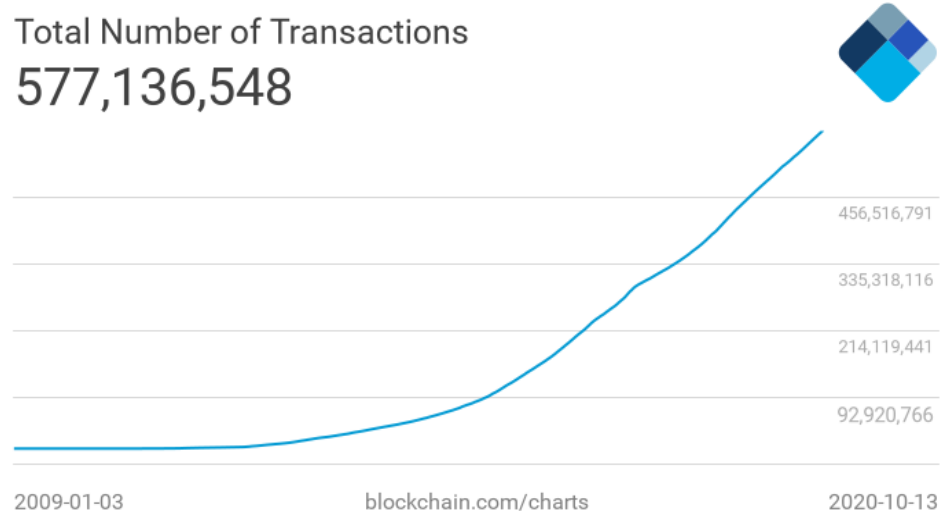
2.2.2. Penomoran Ijazah Nasional (PIN) dan Sistem Verifikasi Ijazah Secara Elektronik (SIVIL)

Penomoran Ijazah Nasional (PIN) merupakan proses penomoran ijazah nasional dengan menggunakan aplikasi yang disebut PIN. Nomor ijazah nasional ini akan dicantumkan pada ijazah yang diterbitkan oleh perguruan tinggi. Proses ini memiliki dua tahap yaitu reservasi atau *booking* nomor ijazah untuk calon lulusan dan pemasangan nomor ijazah dengan Nomor Induk Mahasiswa (NIM) calon lulusan. Nomor Ijazah Nasional ini terdiri dari 15 digit yang meliputi kode prodi, tahun lulusan, nomor urut dan *check digit*. Sistem Verifikasi Ijazah Secara Elektronik (SIVIL) merupakan aplikasi yang digunakan untuk memverifikasi nomor ijazah yang pernah diterbitkan dan memverifikasi keabsahan serta pengesahan nomor ijazah nasional [14].

2.2.3. Blockchain

Blockchain merupakan teknologi dasar dari Bitcoin yang sangat populer. Blockchain adalah sejenis struktur rantai yang mengkombinasikan blok data dalam urutan waktu dan menyerupai *ledger* terdistribusi atau *database*. Keamanan Blockchain dijamin oleh kriptografi asimetris dan tidak dapat dirusak ataupun dipalsukan [6]. Blockchain menggunakan mekanisme *consensus*. Setiap transaksi yang menyebabkan perubahan pada *ledger*

Blockchain akan ditandai, diverifikasi dan divalidasi oleh *nodes* yang menyimpan duplikasi dari *ledger* [14]. Berdasarkan kelebihan dan infrastruktur terdesentralisasi, teknologi Blockchain digunakan untuk permasalahan yang berkaitan dengan kepercayaan, efisiensi, privasi dan *data sharing* [14]. Hal ini menyebabkan teknologi Blockchain banyak digunakan pada seluruh sektor industri seperti keuangan, kesehatan, logistik, dll.



Gambar 2.1 Jumlah Total Transaksi pada Blockchain

Berdasarkan **Gambar 2.1** teknologi Blockchain berkembang setiap tahunnya. Hal ini dapat dilihat dari proyeksi transaksi Blockchain pada tahun 2009 sampai dengan tahun 2020 [15].

2.2.4. Ethereum

Ethereum merupakan *platform* terbuka yang digunakan untuk membangun aplikasi terdesentralisasi di atas Blockchain [16]. Semua komputasi yang diprogram pada Ethereum dikenakan biaya dan ditentukan dalam unit *gas* [17]. *Gas* adalah satuan ukuran yang digunakan untuk menghitung jumlah pekerjaan yang diselesaikan untuk suatu operasi [18]. Ethereum menggunakan Ether (ETH) digunakan sebagai *cryptocurrency* untuk melakukan pembayaran atas transaksi yang dilakukan pada Blockchain Ethereum. Setiap partisipan pada Ethereum dapat diidentifikasi melalui Ethereum Address (EA) [14].

Ethereum menggunakan *Proof of Work* (POW) sebagai protokol *consensus*. Model keamanan yang diberikan oleh POW dilengkapi dengan

digital signatures dan ditambahkan ke *ledger* atau *database* untuk memastikan bahwa *history* tidak bisa dirusak dan tidak bisa dipalsukan [17]. Ethereum Blockchain mengekspansi fungsionalitasnya dengan mengimplementasikan *smart contract*.

2.2.5. Smart Contract

Smart Contract adalah perwujudan dari kontrak atau perjanjian dalam dunia maya. Kontrak ini berbentuk sebuah kode dimana dapat tercipta apabila seluruh syarat pembuatan kontrak sudah terpenuhi [19]. Misalnya, ada transaksi antara penjual dan pembeli. Dalam dunia maya biasanya penjual akan meletakkan barang dagangannya di suatu *marketplace* agar ada yang bisa membeli. Kemudian, pembeli yang tertarik dapat langsung membeli barang tersebut. Ketika uang sudah berhasil diterima, *smart contract* akan terbentuk antara pembeli dan penjual. Kemudian, masing-masing pihak mendapatkan barangnya. Biasanya barang yang diperjual belikan adalah *cryptocurrency*.

2.2.6. Interplanary File System (IPFS)

Interplanary File System (IPFS) merupakan *file system* terdistribusi yang bekerja dengan cara membuat seluruh *node* yang terhubung saling berbagi atau menggunakan *file system* yang sama [20]. *File* yang disimpan akan dipecah menjadi blok-blok kemudian didistribusikan ke *node* yang terhubung dengan IPFS [21]. IPFS dibuat untuk mengatasi sistem penyimpanan yang masih terpusat sehingga membutuhkan banyak *storage*. IPFS juga bisa memastikan bahwa hanya ada 1 *file* yang ada dalam *cluster*, sehingga tidak terjadi duplikasi dan lebih hemat *storage*.

2.2.7. Quality of Service (QoS)

Quality of Service (QoS) adalah kemampuan dari sebuah jaringan untuk menyediakan layanan yang lebih baik lagi bagi trafik yang melewatinya. QoS dapat diukur dengan menggunakan beberapa parameter, yaitu [22]:

1. Throughput

Throughput merupakan kecepatan (*rate transfer*) dalam pengiriman paket data dalam satuan kbps (*kilo bit per second*). *Throughput* memiliki

jumlah total paket yang sukses diterima selama interval waktu tertentu dan dibagi dengan interval waktu tersebut.

2. *Packet loss*

Packet loss merupakan paket yang hilang pada proses transmisi ke tujuannya. *Packet loss* dapat terjadi karena beberapa faktor seperti *overload traffic* atau tabrakan dalam jaringan, *error* pada media fisik, *interface* atau *router down* dan kegagalan yang terjadi pada sisi penerima seperti *overflow* pada *buffer*.

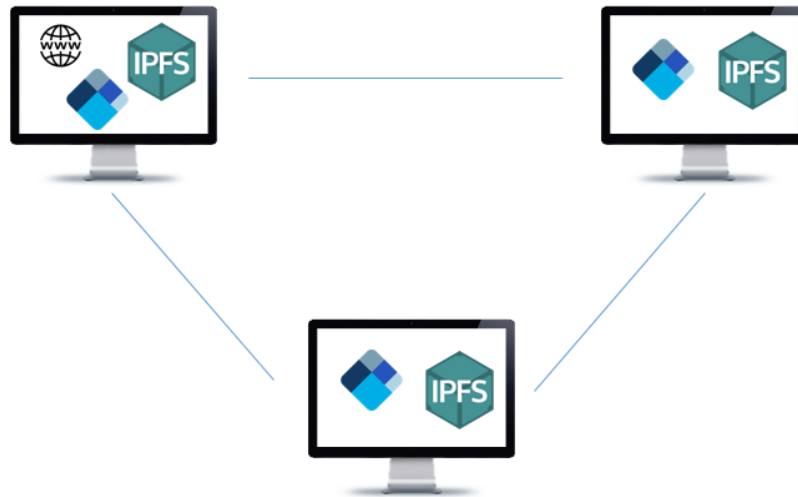
3. *Delay*

Delay merupakan waktu tunggu yang dibutuhkan untuk proses pengiriman dari *transmitter* sampai diterima oleh *receiver*.

BAB III

PERANCANGAN SISTEM

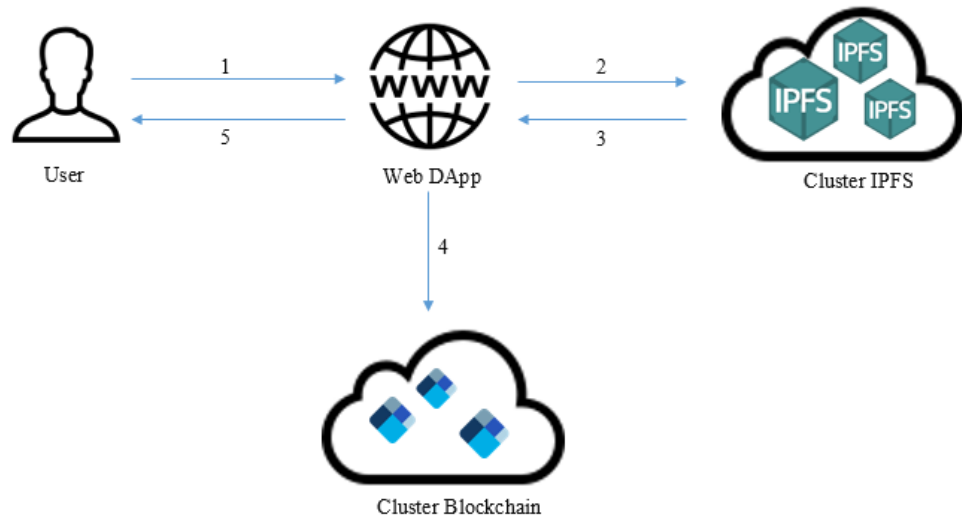
3.1. Perancangan Sistem



Gambar 3.1 Arsitektur Sistem yang Akan Dibangun

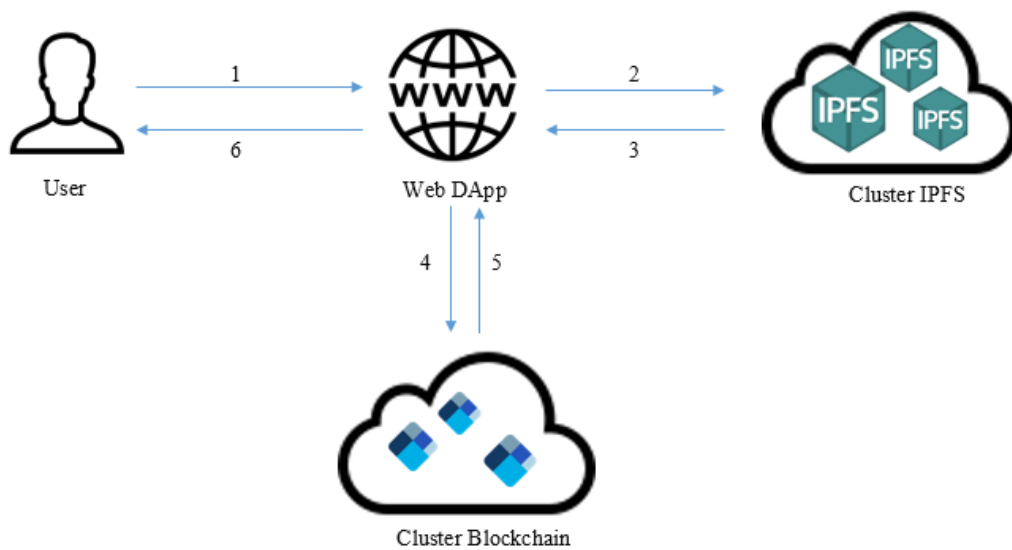
Sistem dirancang dengan menggunakan 3 *node*. Penggunaan jumlah *node* dimaksudkan untuk membuktikan sistem terdistribusi dan kaitannya dengan kualitas layanan yang akan dihasilkan sistem. *Node* yang berisi web DApp akan diinstall IPFS dan akan membuat *cluster* IPFS. *Node* ini juga akan diinstall *geth* untuk membuat *blockchain*. *Node* yang lain akan diinstall IPFS dan bergabung dengan *cluster* yang sudah dibuat. Pada sistem yang akan dibangun tidak menggunakan metamask sehingga penyimpanan dilakukan secara otomatis. Hal ini bertujuan untuk memberikan kemudahan bagi *user*.

3.2. Alur Sistem



Gambar 3.2 Alur Sistem Pembuatan Ijazah/Transkrip

Pada proses pembuatan ijazah/transkrip, terdapat beberapa tahapan pada (1) *user* melakukan *input form* pada *web DApp* lalu *web DApp* akan membuat *file* ijazah/transkrip berdasarkan data yang dimasukkan. Selanjutnya (2) ijazah/transkrip yang sudah dibuat akan dikirimkan ke *cluster* IPFS dan mengubah *file* ijazah/transkrip menjadi blok-blok untuk didistribusikan ke *node* yang berada pada *cluster*. Selanjutnya (3) hash dari *file* akan dikirimkan kembali ke *web DApp*. Selanjutnya (4) *web DApp* akan mengirimkan *hash* tersebut ke *cluster blockchain* lalu *hash* tersebut akan didistribusikan ke *node* yang berada pada *cluster*. Terakhir (5) *web DApp* akan mengirimkan *file* ijazah/transkrip ke *user* untuk diunduh.



Gambar 3.3 Alur Sistem Validasi Ijazah/Transkrip

Pada Proses validasi ijazah/transkrip, terdapat beberapa tahapan pada (1) *user* mengunggah *file* ijazah/transkrip ke *web DApp* lalu (2) *web DApp* akan mengirimkan *file* tersebut ke *cluster IPFS* untuk diubah menjadi *hash*. Selanjutnya (3) *hash* akan dikirimkan kembali ke *web DApp*. Selanjutnya (4) *web DApp* akan mengirimkan *hash* untuk divalidasi oleh *cluster blockchain*. Selanjutnya (5) hasil dari validasi akan dikirimkan kembali ke *web DApp* dan (5) hasilnya akan ditampilkan ke *user*.

3.3. Skenario Pengujian

Pengujian dilakukan dengan *user* membuat sebuah ijazah/transkrip pada *web DApp* sampai *user* menerima *file* ijazah/transkrip untuk diunduh. Selain itu juga dilakukan pengujian ketika *user* mengunggah ijazah/transkrip ke *web DApp* lalu divalidasi oleh *blockchain* dan *web DApp* mengirimkan hasilnya ke *user*. Pengujian dilakukan dengan menambah jumlah *node* secara bertahap dari 3 *node*. Untuk setiap jumlah *node* akan dilakukan pembuatan ijazah/transkrip sebanyak 10 kali dan validasi ijazah/transkrip sebanyak 10 kali lalu akan dilihat pengaruh dari jumlah *node* terhadap *Quality of Service* (QoS) dari sistem yang dibangun.

DAFTAR PUSTAKA

- [1] Y. Yuwono, "KEBIJAKAN LEGISLATIF DALAM UPAYA PENANGGULANGAN TINDAK PIDANA PEMALSUAN IJAZAH," UNIVERSITAS MUHAMMADIYAH SURAKARTA, 2010, 2010.
- [2] KBBI, "KBBI Daring," Kemdikbud, 2016. [Online]. Available: kbbi.kemdikbud.go.id. [Accessed 2020 Oktober 2020].
- [3] I. Teguh, "Mengapa Orang Indonesia Memalsukan Ijazah?," *tirto.id*, 27 November 2018. [Online]. Available: <https://tirto.id/mengapa-orang-indonesia-memalsukan-ijazah-dau1>. [Accessed 4 Oktober 2020].
- [4] R. Dwinanda, "Cegah Pemalsuan, PTS Diajak Ajukan Penomoran Ijazah Nasional," *Republika*, 26 Agustus 2019. [Online]. Available: <https://republika.co.id/berita/pwudct414/cegah-pemalsuan-pts-diajak-ajukan-penomoran-ijazah-nasional>. [Accessed 4 Oktober 2020].
- [5] Kemenristekbrin, "Cegah dan Antisipasi Ijazah Palsu dengan SIVIL PIN," Kementerian Riset dan Teknologi/Badan Riset dan Inovasi Nasional, 2 Mei 2016. [Online]. Available: <https://www.ristekbrin.go.id/kabar/cegah-dan-antisipasi-ijazah-palsu/>. [Accessed 4 Oktober 2020].
- [6] Y. Chen, H. Li, K. Li and J. Zhang, "An improved P2P File System Scheme based on IPFS and Blockchain," *IEEE*, pp. 2652 - 2657, 2017.
- [7] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use cases in Blockchain Technology," in *9th ICCCNT 2018 IEEE*, India, 2018.
- [8] Y. A. Pranata, I. Fibriani and S. B. Utomo, "ANALISIS OPTIMASI KINERJA QUALITY OF SERVICE PADA LAYANAN KOMUNIKASI DATA MENGGUNAKAN NS-2 DI PT. PLN (PERSERO) JEMBER," *SINERGI*, vol. 20, no. 2, pp. 149-156, 2016.
- [9] A. M. Aziz, A. Budiono and A. Widjajarto, "ANALISIS DAN IMPLEMENTASI KOMUNIKASI ANTAR NODE IPFS (INTERPLANETARY FILE SYSTEM) PADA SMART CONTRACT ETHEREUM," *e-Proceeding of Engineering*, vol. 6, no. 2, pp. 7670 - 7678, 2019.
- [10] M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State, "Blockchain-Based, Decentralized Access Control for IPFS," *IEEE*, pp. 1499-1506, 2018.
- [11] A. H. Nugroho, "VALIDASI IJAZAH DENGAN MENGGUNAKAN WATERMARKING VALIDASI IJAZAH DENGAN MENGGUNAKAN WATERMARKING," pp. 9 - 15.
- [12] F. Nuraeni, Y. H. Agustin and I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan RSA dan Implementasi Tanda Tangan Digital Menggunakan RSA dan," in *Konferensi Nasional Sistem Informasi*, Pangkalpinang, 2018.
- [13] Mendikbud, "PERATURAN MENTERI PENDIDIKAN DAN KEBUDAYAAN REPUBLIK INDONESIA NOMOR 8 1 TAHUN 2014," LLDIKTI, 2014.

- [14] N. Nizamuddina, K. Salah, M. A. Azad, J. Arshad and M. Rehman, "IPFS, Decentralized document version control using ethereum blockchain and," *Computers and Electrical Engineering*, pp. 183-197, 2019.
- [15] Blockchain.com, "Jumlah total transaksi pada blockchain," [Online]. Available: <https://www.blockchain.com/charts>. [Accessed 16 10 2020].
- [16] A.-T. Pănescu and V. Manta, "Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network," Taylor & Francis Group, Romania, 2018.
- [17] G. Wood, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER ETHereum: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER," GAVIN@ETHCORE.IO, 2017. [Online]. Available: <https://gavwood.com/paper.pdf>. [Accessed 16 10 2020].
- [18] G. G. Dagher, P. B. Marella, M. Milojkovic and J. Mohler, "BroncoVote: Secure Voting System using Ethereum's Blockchain," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, Colorado, 2018.
- [19] D. Macrinici, "Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study," *Telematics and Informatics*, 2018. [Online]. Available: doi: <https://doi.org/10.1016/j.tele.2018.10.004>.
- [20] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 14 7 2014. [Online]. Available: <https://arxiv.org/pdf/1407.3561.pdf>. [Accessed 16 10 2020].
- [21] S. Muralidharan and H. Ko, "An InterPlanetary File System (IPFS) based IoT framework," *IEEE International Conference on Consumer Electronics (ICCE)*, 2019.
- [22] T. Novianti and A. Widianoro, "Analisa QOS (Quality of Services) pada Implementasi IPV4 dan IPV6 dengan Teknik Tunneling," *Jurnal Ilmiah Rekayasa*, vol. 9, no. 2, pp. 76-83, 2016.