BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

Pada era digital ini terjadi beberapa kasus mengenai pemalsuan data diri, salah satu kasusnya adalah pemalsuan identitas digital pada sebuah sertifikat. Sertifikat merupakan bukti telah menyelesaikan suatu acara tertentu (pelatihan, seminar, dsb). Penerbitan sebuah sertifikat hanya bisa dilakukan oleh badan yang berwenang atau sebuah organisasi yang sudah memiliki izin dari badan berwenang tersebut. Sertifikat dapat menentukan identitas seseorang memiliki pengalaman tertentu. Saat ini diperlukan sebuah sistem untuk mengetahui keaslian data pada sertifikat agar pemalsuan tersebut dapat diminimalisir. Salah satu cara diantaranya untuk mengamankan keaslian suatu data dapat menggunakan sistem blockchain.

Blockchain merupakan ledger terdistribusi berdasarkan *database* terdistribusi dan rantai *hash* yang bekerja pada jaringan *Peer-to-Peer* (P2P) untuk memberikan lebih banyak privasi dan keamanan dalam pembangunan desentralisasi topologi. Blockchain dapat dikatakan sebagai basis data terdistribusi yang tidak memerlukan otoritas pusat sehingga menghilangkan perlunya verifikasi dari pihak ketiga. Blockchain terdiri atas sekumpulan blok yang terhubung satu dengan lainnya dengan metode *hash*, sehingga membentuk sebuah rantai dari kumpulan blok.

Pada permasalahan tersebut penulis akan memfokuskan penelitian untuk masalah sistem verifikasi dan integritas pada data sertifikat dengan menggunakan sistem blockchain dan dengan bantuan kode QR. Oleh karena itu penelitian ini mengangkat judul "*Digital Credential* Dengan QR *Code* Untuk Sertifikat Menggunakan Blockchain". Penelitian tentang kredensial digital berbasis blockchain dengan kode QR untuk sertifikat diharapkan dapat memberikan penulis dan pembaca dengan sistem yang menjamin integritas data, terutama dalam konteks sertifikat. Hasil penelitian diharapkan akan berkontribusi pada kemajuan sistem kredensial digital, membuka jalan bagi proses verifikasi sertifikat yang lebih dapat diandalkan dan terpercaya. Selain itu, temuan dari penelitian ini dapat memiliki implikasi yang signifikan di berbagai sektor, termasuk pendidikan, sertifikasi profesional, dan pengembangan tenaga kerja, dengan meningkatkan efisiensi, transparansi, dan kredibilitas pengelolaan sertifikat.

1.2 Informasi Pendukung Masalah

Blockchain diperkenalkan oleh Satoshi Nakamoto [38] dalam sebuah *whitepaper* yang diterbitkan pada tahun 2008, sebagai dasar konseptual untuk pengembangan *cryptocurrency*

Bitcoin. *Whitepaper* tersebut menjelaskan konsep fundamental blockchain sebagai teknologi yang memungkinkan jaringan terdesentralisasi untuk transaksi peer-to-peer yang aman dan transparan. Selain itu, *whitepaper* tersebut memperkenalkan konsep *Proof of Work* (PoW) sebagai mekanisme konsensus untuk memvalidasi transaksi dan memastikan keamanan jaringan blockchain. Sebagai hasilnya, karya bersejarah ini menetapkan dasar untuk pengembangan konseptual dari *cryptocurrency* Bitcoin.

Ze Wang et al [42] mengusulkan desain *Certificate Transparency* (CT) dan *Revocation Transparency* (RT) berbasis blockchain untuk menjaga keseimbangan otoritas absolut dari *Certificate Authorities* (CAs). Mereka memperkenalkan blockchain sertifikat global di mana sertifikat yang ditandatangani oleh CA dan informasi status pencabutan dari server web *Secure Socket Layer* (SSL) / *Transport Layer Security* (TLS) dipublikasikan sebagai transaksi oleh subjek (yaitu, server web). Blockchain sertifikat berfungsi sebagai catatan publik tambahan untuk memantau operasi penandatanganan sertifikat CA dan pencabutan, sambil memberikan kontrol yang berkoordinasi atas sertifikat kepada server web SSL/TLS. Sistem ini diimplementasikan menggunakan Firefox dan Nginx, memungkinkan pemantauan operasi CA melalui catatan publik.

Jayesh G. Dongre et al [26] mengatasi tantangan saat ini dalam sistem verifikasi sertifikat dengan mengusulkan platform yang memberikan perspektif global yang komprehensif bagi mahasiswa dan organisasi. Sistem mereka menggunakan kombinasi dari tanda tangan digital dan skema tanda waktu yang diimplementasikan dengan teknologi blockchain. Dalam makalah ini, mereka menyajikan dua model keuangan seimbang di mana biaya layanan didistribusikan antara lulusan dan pemberi kerja sebagai pemangku kepentingan utama layanan. Verifikasi bukti sertifikat mahasiswa dilakukan dengan biaya rendah, dan otentikasi sertifikat dapat dilakukan dengan mudah dari sumber-sumber terpercaya saat pemberi kerja merekrut kandidat. Penggunaan blockchain untuk verifikasi sertifikat memberikan manfaat signifikan bagi masyarakat dengan menghilangkan penipuan sertifikat.

Rana F. Ghani et al [35] telah mengusulkan sistem sertifikasi berbasis blockchain di tingkat universitas untuk memberikan waktu respons yang cepat dalam penerbitan, berbagi, dan verifikasi sertifikasi ini. Makalah mereka menyajikan kerangka kerja berbasis blockchain yang diusulkan untuk berbagi sertifikasi elektronik (*e-certifications*) dan mengevaluasi kerangka kerja tersebut, termasuk mengukur waktu rata-rata untuk penerbitan sertifikasi dan latensi transaksi. Sistem ini dibangun di atas blockchain pribadi Hyperledger dan menggunakan *smart contract* dan teknik *hashing* untuk memastikan penerapan sertifikasi yang aman dan

terkontrol. Keuntungan utama dari sistem yang diusulkan ini terletak pada *throughput* yang luar biasa baik untuk penerbitan maupun verifikasi sertifikasi, jauh melampaui metode tradisional. Berbeda dengan pendekatan konvensional yang memerlukan waktu sekitar satu minggu hingga 10 hari, *e-certifications* dapat diterbitkan dan diverifikasi dalam waktu satu menit. Selain itu, kerangka kerja yang diusulkan ini mencakup mekanisme pengendalian distribusi data yang kuat sambil menjaga privasi klien.

Mega Adi Kusuma et al [30] telah melakukan penelitian tentang pengembangan sistem keamanan sertifikat tanah berbasis blockchain dan skema validasi kode QR untuk mengatasi masalah pemalsuan sertifikat tanah dan biaya ilegal dalam proses sertifikasi tanah di Indonesia. Proses saat ini melibatkan banyak pemangku kepentingan, yang menyebabkan kompleksitas dan kepanjangan waktu. Sertifikat kertas tradisional rentan terhadap pemalsuan dan kehilangan, sementara sistem sertifikat elektronik terpusat pemerintah rentan terhadap peretasan. Sistem mereka mengimplementasikan validasi kode QR, di mana kode QR yang dipindai didekodekan dan dicocokkan dengan data sertifikat yang diimpor dari jaringan blockchain. Proses pendaftaran dilakukan melalui aplikasi, memastikan transparansi dan mengurangi praktik korupsi. Sistem ini menggunakan Ethereum dan Truffle sebagai platform blockchain yang mendasarinya. Hasil eksperimen menunjukkan kemampuan sistem untuk memvalidasi data melalui *smart contract* dan mekanisme konsensus, memastikan transparansi dan ketidakubahannya dalam proses berbasis blockchain dengan data yang tersimpan secara global dalam jaringan *peer-to-peer*.

1.3 Analisis Umum

1.3.1 Aspek Keberlanjutan (*sustainability*)

Penelitian ini membangun teknologi yang berkelanjutan sehingga dapat menganalisa dan menyelesaikan masalah yang baru atau yang belum terselesaikan.

1.3.2 Aspek Ekonomi (*economy*)

Integritas sebuah dokumen sangat penting untuk perkembangan aspek ekonomi dalam lingkungan perusahaan. Apabila terdapat pemalsuan dalam sebuah dokumen maka akan berdampak pada ekonomi dan keuangan pada pihak perusahaan. Sehingga di pihak perusahaan akan mendapatkan kerugian yang tidak sedikit.

1.3.3 Aspek Hukum (*legality*)

Pemalsuan dokumen oleh seorang oknum yang menimbulkan suatu hak perikatan dan berdampak merugikan salah satu pihak dapat dikenakan hukuman sesuai pasal Kitab Undang-

undang Hukum Pidana (KUHP) pasal 263 [5] dan 264 [6] dengan hukuman penjara selama-lamanya enam tahun.

1.3.4 Aspek Hukum (*legality*)

Keaslian data merupakan aspek yang penting dalam segi keamanan. Dengan banyaknya kasus pemalsuan identitas digital dapat merugikan berbagai pihak. Maka dari itu untuk meminimalisir kasus pemalsuan identitas diperlukan sistem yang dapat memverifikasi keaslian identitas.

1.4 Kebutuhan yang Harus Dipenuhi

Berdasarkan permasalahan yang telah dijabarkan, terdapat beberapa kebutuhan yang harus dipenuhi untuk menyelesaikan permasalahan integritas *digital credential*, yaitu :

1. Sistem dapat mengidentifikasi integritas dari sertifikat;
2. Sistem dapat menampung informasi integritas data kedalam blockchain;
3. Sistem dapat diakses melalui situs web interaktif.

1.5 Solusi Sistem

1.5.1 Karakteristik Produk

Untuk menyelesaikan permasalahan di atas maka diperlukan beberapa fitur dari solusi yang akan dibuat :

- Fitur Utama:
  - Data yang ada di sertifikat akan diubah menjadi bentuk *hash* yang kemudian akan dimasukan ke dalam jaringan Blockchain. Lembaga yang berwenang dapat menerbitkan akun admin yang akan digunakan untuk memasukan informasi sertifikat.
- Fitur Dasar:
  - Dapat mendownload *softcopy* sertifikat menggunakan QR *code.*
  - Sudah menggunakan *smart contract*
  - Menggunakan teknologi *Blockchain*
- Fitur Tambahan:
  - Data tidak bisa di *decode* karena data akan berbentuk *hash*.
- Sifat solusi yang diharapkan
  - Mudah digunakan oleh *end user*.
  - Data terjaga dan tidak bisa diubah sembarangan.
  - Pemalsuan data sertifikat berkurang bahkan menghilang.

1.5.2 Usulan Solusi

Berdasarkan konstrain dan karaktereistik dari produk, maka terdapat 2 alternatif solusi yang dapat ditawarkan antara lain:

1) Solusi 1: Penerapan Blockchain menggunakan Hyperledger Fabric

Gambar 1.1 Logo Hyperledger Fabric

Penerapan Blockchain menggunakan Hyperledger fabric. Hyperledger fabric merupakan platform *Distributed Ledger Technology* (DLT) tingkat perusahaan yang bersifat *open-source*. Hyperledger fabric ini memiliki fitur utama berupa verifikasi keaslian sebuah dokumen menggunakan teknologi blockchain.

- **Skenario Penggunaan**

  Pengguna melakukan *scan* kode QR atau *scan* sertif kemudian sistem akan melakukan verifikasi data untuk menentukan bahwa sertifikat tersebut asli atau tidak.

- **Karakteristik**
  a. *Private* Blockchain
  b. *Open source*
  c. Tidak memerlukan *Proof-of-Work* (PoW) atau Konsensus untuk memvalidasi transaksi
  d. *Programming Language* : Golang, JavaScript, atau Java
  e. *Participation* : Organisasi yang memiliki sertifikat otorisasi

2) Solusi 2: Penerapan Blockchain menggunakan Metamask

Gambar 1.2 Logo Metamask

Penerapan Blockchain menggunakan Metamask. Metamask merupakan *plugin* browser yang berfungsi sebagai *wallet* Ethereum. Metamask ini memiliki fitur utama berupa manajemen akun dan verifikasi keaslian sebuah dokumen menggunakan teknologi blockchain.

- **Skenario Penggunaan**

Pengguna melakukan *scan* kode QR atau *scan* sertif kemudian sistem akan melakukan verifikasi data untuk menentukan bahwa sertifikat tersebut asli atau tidak.

- **Karakteristik**
  a. *Public* Blockchain
  b. *Open source*
  c. Menggunakan mekanisme *Proof-of-Work* (PoW) atau mekanisme konsensus
  d. *Programming Language* : Solidity
  e. *Participation* : Semua orang

1.5.3 Solusi yang diambil

Berdasarkan latar belakang dan *constraint* yang ada, solusi yang dipilih adalah solusi 1 yaitu Penerapan Blockchain menggunakan Hyperledger Fabric dengan pertimbangan platform Hyperledger Fabric yang memiliki karakteristik yang merupakan *private network*. Pengembangan sistem dapat menggunakan banyak opsi bahasa pemrograman sehingga pengembangannya dapat lebih flexibel. Selain itu sistem dapat terhindar dari *gas fee* karena tidak menggunakan konsep PoW. Jaringan bersifat pribadi sehingga jika ada yang akan menggunakan jaringan maka perlu perizinan dari administrator jaringan.

Tabel 1.1 Usulan Solusi

Alternatif Solusi	Aspek Keberlanjutan	Aspek Ekonomi	Aspek Keamanan
Solusi 1	**Kelebihan**: – Menggunakan bahasa pemrograman yang lebih banyak dan lebih populer dalam *developing* sehingga projek dapat dilanjutkan di masa depan. – Memiliki cakupan *stakeholder* yang lebih luas **Kekurangan**: Pembuatan jaringan memerlukan waktu yang lebih lama dikarenakan harus	**Kelebihan**: – *Open source* sehingga mudah terjangkau oleh banyak pihak. – Tidak memiliki *gas fee* karena tidak menggunakan konsep PoW. **Kekurangan**: Membutuhkan sumber daya manusia lebih besar ketika pengembangan sistem.	**Kelebihan**: - Jaringan yang digunakan bersifat *private* - Hanya berjalan di jaringan yang telah diizinkan **Kekurangan**: Penerapan teknologi masih sedikit.

	membuat jaringan sendiri.		
Solusi 2	**Kelebihan**: Pembuatan jaringan memerlukan waktu yang lebih cepat karena sudah menggunakan jaringan ethereum. **Kekurangan**: - Pengembangan sistem hanya menggunakan satu bahasa. - Cakupan *stakeholder* terbatas.	**Kelebihan**: Memerlukan sumberdaya yang lebih sedikit ketika pengembangan. **Kekurangan**: Transaksi menggunakan *gas fee* karena menggunakan konsep PoW	**Kelebihan**: Teknologi telah menggunakan PoW yang sudah banyak diterapkan. **Kekurangan**: Dapat terjadi serangan *selfish mining attack*.

Pemalsuan identitas pada sebuah sertifikat dapat terjadi karena tidak adanya sebuah sistem yang dapat melakukan identifikasi perubahan atau perbedaan pada data pengguna dengan *database*. Integritas sertifikat perlu dipublikasi secara resmi dan didistribusi dalam suatu lingkungan yang aman. Integritas file dapat disimpan kedalam blockchain agar ketika terjadi perubahan pada sertifikat, maka integritas data tersebut tidak sama dengan integritas yang terdapat dalam sistem blockchain. Ketidaksamaan data ini membuat sertifikat tersebut hilang integritasnya dan dapat dikatakan menjadi tidak sah. Sehingga dari permasalahan tersebut diusulkan solusi berupa pembuatan aplikasi verifikasi dan integritas digital credential pada data sertifikat

BAB 2

DESAIN KONSEP SOLUSI

2.1 Spesifikasi Produk

Tabel 2.1 Spesifikasi Produk

No	Hal	Rincian
1	Pengembangan Sistem Verifikasi Sertifikat Berbasis Web	Sistem akan diakses melalui *website* dengan internet. IP public akan menjadi jembatan antara internet dengan server. Adapun spesifikasi dari *Developing Website* sebagai berikut: • *Dev Language*: JavaScript, CSS dan HTML • *Front-End Framework*: React • *Back-End Framework*: Node.js • *Database*: MySQL • *Web server*: Apache
2	Pengembangan Sistem Deteksi Sertifikat Berbasis QR *Code*	Sistem dapat membaca data yang terdapat pada kode QR. Adapun spesifikasi dari kode QR sebagai berikut : • Model: Statis (model 2) • Data: URL sertifikat • *Dev language*: JavaScript
3	Pengembangan Sistem Jaringan Blockchain	Jaringan Blockchain yang digunakan akan menggunakan *framework* Hyperledger Fabric. Pada *framework* Hyperledger Fabric dilakukan pembuatan jaringan blockchain dan *database* sistem. Adapun spesifikasi dari Hyperledger Fabric sebagai berikut : • *Network*: Fabric • *API Dev Language*: Node.js • *Smart Contract* (*Chaincode*): JavaScript • *Deployment*: Docker, Docker-ce, Portainer
4	Pengembangan Sistem Integrasi Server	Server yang digunakan ada 2 jenis, V*irtual Private Server* (VPS) dan server O*n-premise*. VPS akan

		menjadi penghubung server *on-premise* dan internet. Koneksi website akan di *tunnel* melalui ip public VPS. Server *on-premise* menjadi tempat jaringan blockchain dan mesin virtual webserver berjalan. Adapun spesifikasi mesin virtual webserver adalah sebagai berikut : • Model : Dell PowerEdge R740 • CPU : 10 CPUs x Intel(R) Xeon(R) Silver 4210R CPU @ 2.40GHz RAM : 48 GB • Storage : 2.5 TB • OS : Linux versi 22 Dan spesifikasi dari server VPS sebagai berikut : • Model : Jagoan Hosting VPS KVM - X VM 2 • CPU : 1 Core • RAM : 2 GB • *Storage* : 40 GB • OS : Linux versi 20

2.2 Verifikasi

2.2.1 Verifikasi Spesifikasi 1: Pengembangan Sistem Verifikasi Sertifikat Berbasis Web

Tabel 2.2 Verifikasi Spesifikasi 1 Metode 1

Hal	Metode 1: Pengguna membuat akun
Rincian	Pengguna mendaftarkan diri pada halaman sign up dan melakukan pengecekan data kredensial yang masuk kedalam *database*.
Metode Pengujian	Memasukan informasi pada halaman sign up
Prosedur Pengujian	Pihak organisasi mengisi beberapa informasi berupa nama organisasi, email, password, *re-type* password dan memasukan bukti berkas pada halaman sign up.

Tabel 2.3 Verifikasi Spesifikasi 1 Metode 2

Hal	Metode 2: Pengguna melakukan login
Rincian	Pengguna melakukan login pada halaman login dan melakukan cek apakah pengguna dapat masuk kedalam sistem.
Metode Pengujian	Memasukan informasi login pada halaman login
Prosedur Pengujian	Pihak organisasi mengisi kolom email dan password pada halaman login dengan kombinasi yang telah dimasukan pada saat pendaftaran akun.

Tabel 2.4 Verifikasi Spesifikasi 1 Metode 3

Hal	Metode 3: Pengujian organisasi status "not_*approved*".
Rincian	Pada saat akun organisasi pertama kali terbuat, akun tersebut belum memiliki hak untuk melakukan aktifitas dalam sistem. Ketika organisasi yang belum di-*approve* melakukan login, akan tampil pesan bahwa akun belum terverifikasi dan perlu menunggu proses approval.
Metode Pengujian	Organisasi belum di-*approve* mencoba mengakses dashboard.
Prosedur Pengujian	Untuk menguji sistem approval organisasi, diperlukan akun organisasi yang memiliki status "not_approved". Setelahnya, akun tersebut login untuk memasuki halaman dashboard organisasi.

Tabel 2.5 Verifikasi Spesifikasi 1 Metode 4

Hal	Metode 4: Pengujian approval organisasi
Rincian	Proses approval organisasi dilakukan pada halaman dashboard admin. Pada pengujian ini akun "Organisasi Keamanan" masih memiliki status "not_approved" yang perlu dilakukan proses approval. Setelah melakukan approval, akun tersebut akan masuk kedalam jenis organisasi yang terpercaya.
Metode Pengujian	Admin melakukan approval organisasi pada dashboard
Prosedur Pengujian	Admin memantau dashboard admin untuk melihat akun yang telah melakukan pendaftaran, dan menekan tombol checklist *approve* untuk organisasi tersebut.

Tabel 2.6 Verifikasi Spesifikasi 1 Metode 5

Hal	Metode 5: Pengecekan *query backend*
Rincian	Menjalankan perintah *query* kedalam *database* pengguna dan memonitor apakah hasil yang terdapat dalam *query* menghasilkan *output* yang benar atau tidak.
Metode Pengujian	Admin melakukan approval organisasi pada dashboard.
Prosedur Pengujian	Untuk mengetahui layanan yang berjalan pada *backend*, dilakukan uji request dan response dari beberapa fungsi API yang terdapat dalam sistem *backend*.

2.2.2 Verifikasi spesifikasi 2: Pengembangan Sistem Deteksi Sertifikat Berbasis QR *Code*

Tabel 2.7 Verifikasi Spesifikasi 2 Metode 1

Hal	Metode 1: Verifikasi file digital
Rincian	Memproses masukan data sertifikat yang sudah berisi kode QR dengan informasi digital credential sertifikat pada halaman utama situs web dan mengetahui jika file tersebut sudah valid untuk diproses oleh sistem atau tidak.
Metode Pengujian	Melakukan pemindaian kode QR.
Prosedur Pengujian	Pengguna memasukan file sertifikat file sertifikat yang memiliki kode QR yang isi ID sesuai dengan ledger blockchain dan format filenya bisa diterima sistem. Pada halaman verifikasi pengguna kemudian menekan tombol informasi, *hash*, dan tambahan untuk melihat informasi yang ada pada ledger.

Tabel 2.8 Verifikasi Spesifikasi 2 Metode 2

Hal	Metode 2: Verifikasi file fisik
Rincian	Memproses data sertifikat yang sudah berisi kode QR dengan informasi digital credential sertifikat pada halaman utama situs web dan mengetahui jika file tersebut sudah valid untuk diproses oleh sistem atau tidak dengan menggunakan file hasil *scan* menggunakan kamera.
Metode Pengujian	Melakukan pemindaian kode QR.

Prosedur Pengujian	Seorang pengguna menerima sertifikat dalam bentuk fisik dan ingin melakukan verifikasi terhadap sertifikat tersebut. Pengguna tersebut kemudian melakukan *scanning* sertifikat dengan menggunakan kamera saja.

2.2.3 Verifikasi spesifikasi 3: Pengembangan Sistem Jaringan Blockchain

Tabel 2.9 Verifikasi Spesifikasi 3 Metode 1

Hal	Metode 1: Pengecekan *query* blockchain
Rincian	Menjalankan perintah kueri kedalam jaringan blockchain dan memonitor apakah hasil yang terdapat dalam *query* menghasilkan *output* yang benar atau tidak. Pengujian yang terlibat dalam menilai kemampuan *query* blockchain dilakukan untuk mengevaluasi efisiensi dan akurasi sistem dalam mengambil dan menyajikan data dari blockchain.
Metode Pengujian	Menjalankan perintah *query* kedalam jaringan blockchain
Prosedur Pengujian	Proses skenario melibatkan eksekusi perintah kueri di dalam jaringan blockchain untuk mencocokkan data *query* yang dipanggil dengan informasi yang disimpan di blockchain. Pengujian menggunakan ID sertifikat sebagai sumber data untuk *query*.

Tabel 2.10 Verifikasi Spesifikasi 3 Metode 2

Hal	Metode 2: Input data jumlah tunggal
Rincian	Melakukan *input* data tunggal pada halaman *input* sertifikat dan melakukan pengecekan setelah proses *input* data sertifikat yang dibuat ke dalam sistem.
Metode Pengujian	Melakukan pengujian *input* data tunggal
Prosedur Pengujian	Proses skenario melibatkan pemasukan berbagai detail sertifikat, termasuk Acara, Nama Peserta, Deskripsi, Posisi Penulis, Nama Penulis, Posisi Penulis2, Nama Penulis2, Logo, Tanda Tangan 1, dan Tanda Tangan 2 pada halaman pembuatan sertifikat.

Tabel 2.11 Verifikasi Spesifikasi 3 Metode 3

Hal	Metode 3: Input data jumlah besar
Rincian	Melakukan *input* data berjumlah besar dengan memilih opsi "Input Jumlah Besar" pada halaman *input* sertifikat dan melakukan pengecekan setelah proses *input* data sertifikat yang dibuat ke dalam sistem.
Metode Pengujian	Melakukan pengujian *input* data berjumlah besar
Prosedur Pengujian	Proses melibatkan pemasukan berbagai detail sertifikat seperti pada pengujian *input* data tunggal, termasuk Acara, Nama Peserta, Deskripsi, Posisi Penulis, Nama Penulis, Posisi Penulis2, Nama Penulis2, Logo, Tanda Tangan 1, dan Tanda Tangan 2 pada halaman pembuatan sertifikat. Namun pada pengujian ini, proses memasukan data dengan mengunakan file csv yang berisikan nama-nama yang akan diproses dijadikan sertifikat.

Tabel 2.12 Verifikasi Spesifikasi 3 Metode 4

Hal	Metode 4: Pengecekan *encode* data
Rincian	Melakukan *encode* data, dan decode untuk mengetahui apakah data yang ter-*encode* sesuai dengan data asli setelah di *decode*.
Metode Pengujian	Melakukan pengujian *encode* data, dan *decode* pada jaringan blockchain.
Prosedur Pengujian	Pengujian sub-sistem *encode* data dilakukan dengan membuka aplikasi Postman, kemudian menyalin data gambar sertifikat dan di *decode* menggunakan alat-alat online.

Tabel 2.13 Verifikasi Spesifikasi 3 Metode 5

Hal	Metode 5: *Performance* blockchain
Rincian	Pengujian *performance* ini bertujuan untuk mengevaluasi dan mengukur kinerja sistem blockchain dalam menghadapi beban kerja yang signifikan.
Metode Pengujian	Melakukan pengujian *performance* pada jaringan blockchain.
Prosedur Pengujian	Selama fase pengujian *performance*, dilakukan 10 percobaan yang masing-masing melibatkan pengiriman 200 TX (transaksi) ke sistem. Konfigurasi pengujian meliputi 20 pekerja yang terlibat dalam proses pengujian, dan batas Kecepatan Kirim (*Send Rate*)

	ditetapkan pada 10 tps (transaksi per detik). Selama proses pembandingan, setiap fungsi *smart contract* (chaincode) dievaluasi, termasuk pembuatan sertifikat, pembaruan sertifikat, pembacaan sertifikat, dan penghapusan sertifikat.

Tabel 2.14 Verifikasi Spesifikasi 3 Metode 6

Hal	Metode 6: Beban blockchain
Rincian	Pengujian beban ini bertujuan untuk mengevaluasi dan stabilitas sistem blockchain di bawah tingkat aktivitas pengguna yang diharapkan atau diantisipasi. Tujuan utamanya adalah untuk menentukan kapasitas sistem untuk menangani sejumlah besar pengguna, transaksi, atau pemrosesan data secara bersamaan.
Metode Pengujian	Melakukan pengujian beban pada jaringan blockchain
Prosedur Pengujian	Pada tahap pengujian beban dilakukan 10 kali percobaan yang masing-masing melibatkan penyerahan 20 TX sampai dengan 200 TX (transaksi) ke sistem. Konfigurasi pengujian menyertakan 20 pekerja yang terlibat dalam proses pengujian, dan batas Kecepatan Kirim ditetapkan sebesar 10 tps (transaksi per detik).

Tabel 2.15 Verifikasi Spesifikasi 3 Metode 7

Hal	Metode 7: Ketahanan dan keamanan data ledger
Rincian	Pengujian ini dilakukan untuk mengelihat bahwa keamanan data blockchain serta memastikan blockchain bersifat immutable dan terdistribusi.
Metode Pengujian	Melakukan perubahan data pada ledger blockchain
Prosedur Pengujian	Pegujian dilakukan dengan mensimulasikan situasi di mana pihak yang tidak berwenang berhasil menyusup ke salah satu peer jaringan dan mengubah data yang disimpan dalam ledger.

2.2.4 Verifikasi spesifikasi 4: Pengembangan Sistem Integrasi Server

Tabel 2.16 Verifikasi Spesifikasi 4 Metode 1

Hal	Metode 1: Response Time Server
Rincian	Tujuan dari *performance* test website ini dengan menggunakan metrik response time server adalah untuk mengukur seberapa

	cepat atau lambat server merespons permintaan yang diberikan oleh pengguna atau klien.
Metode Pengujian	*Benchmarking* dengan server *request.*
Prosedur Pengujian	Selama fase pengujian performa, dilakukan 10 kali akses ke server website menggunakan browser, dan alat pemantauan yang digunakan adalah Chrome Developer Tools. Waktu respons sistem terhadap permintaan yang diberikan oleh browser pada komputer penguji diukur untuk mengetahui berapa lama waktu yang dibutuhkan untuk mengakses sistem. Performa muatan website diukur juga untuk mengetahui beban kerja yang nyata.

Tabel 2.17 Verifikasi Spesifikasi 4 Metode 2

Hal	Metode 2: Tes Stabilitas Visual Website
Rincian	Tujuan dari *performance* test website ini dengan menggunakan metrik response time server adalah untuk mengukur seberapa cepat atau lambat server merespons permintaan yang diberikan oleh pengguna atau klien.
Metode Pengujian	*Benchmarking* dengan server *request.*
Prosedur Pengujian	Pada tahap pengujian ini, dilakukan 10 kali percobaan pengukuran LCP dan CLS website pada dua perangkat yang berbeda untuk menggambarkan perbedaan kinerja pada masing-masing perangkat dalam browser Google Chrome dengan fitur *Performance* Insight di Google Developer Tools aktif pada setiap pengujian.

Dokumen ini bertujuan untuk melengkapi konsep solusi yang telah dijelaskan dalam dokumen capstone design sebelumnya dengan memberikan rincian lengkap tentang spesifikasi produk dan proses verifikasinya. Pengembangan produk melibatkan sistem verifikasi berbasis web, sistem deteksi sertifikat berbasis kode QR, sistem jaringan blockchain, dan integrasi server. Semua aspek ini akan diuraikan secara terperinci dalam dokumen ini guna memastikan kelengkapan dan keselarasan dari solusi yang diusulkan.