BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah dan Pendukung

Pada era digital saat ini, salah satu aspek di internet yang perlu diperhatikan keamanannya adalah sistem autentikasi. Sistem autentikasi biasanya menggunakan *username* dan *password* sebagai sistem validasi akun yang umum digunakan karena mudah dalam pengimplemantasiannya. Data *username* dan *password* sangat rentan diretas sehingga perlu dilakukan peningkatan keamanan pada sistem autentikasi.

Autentikasi merupakan suatu pembuktian identitas terhadap suatu entitas seperti pada mesin, kartu kredit, dan orang [1]. Masalah autentikasi dapat muncul dalam database konvensional, seperti halnya dalam sistem apa pun yang melibatkan akses pengguna dan keamanan data. Masalah-masalah ini dapat mencakup masalah seperti akses yang tidak sah, pelanggaran data, dan pencurian identitas. Beberapa masalah autentikasi umum dalam database konvensional mencakup kata sandi yang lemah, kontrol akses yang tidak memadai, dan kerentanan yang dapat dieksploitasi oleh pelaku kejahatan [2]. Salah satu teknologi yang mampu menyelesaikan permasalahan tersebut adalah teknologi *Blockchain*.

Blockchain adalah sebuah teknologi di balik revolusi *Bitcoin*. *Bitcoin* merupakan sebuah *cryptocurrency* yang menjamin kepercayaan dan keamanan melalui penerapan program yang memverifikasi dan memvalidasi transaksi [3]. *Blockchain* pada dasarnya adalah database terdistribusi, atau *public ledger* dari semua transaksi atau peristiwa digital yang telah dieksekusi dan diverifikasi oleh pihak-pihak yang berpartisipasi. Setiap transaksi dicatat dalam *public ledger* dan diverifikasi melalui konsensus *Proof of work* (PoW) atau *proof of stake* (PoS). Sekali terverifikasi, transaksi tersebut tidak akan pernah bisa dihapus dari *blockchain* [4]. Jaringan *blockchain* menggunakan sistem *peer to peer* dan *hash* kriptografi dimana pengguna dapat melakukan transaksi satu sama lain tanpa bergantung pada perusahaan atau lembaga terpusat [5].

Dibandingkan dengan database terpusat konvensional, data yang sudah tercatat dalam *blockchain* tidak dapat dimanipulasi karena sistem terdistribusi dalam *blockchain* itu sendiri. *Blockchain* terdiri dari kata "*block*" dan "*chain*". *Block* merupakan struktur data yang menyimpan data transaksi, *bitcoin* memiliki ukuran *block* satu *megabyte* dan terdiri dari beberapa transaksi. Setiap ada transaksi yang diverifikasi, transaksi tersebut dimasukan ke dalam *block*, jika *block* sudah penuh, transaksi baru membentuk *block* baru dan rantai dengan *block* sebelumnya. *Block* dan rantai ini yang disebut dengan *blockchain* [6]. Dengan kelebihan

blockchain tersebut diharapkan dapat menjamin keamanan data yang terdapat di *database* dengan lebih baik.

Website Certifichain merupakan sebuah sistem yang akan berjalan aktif selama 24 jam dan pihak yang memiliki akun dapat mengakses sistem secara publik. Sertifikat yang diterbitkan oleh organisasi akan terhubung kedalam jaringan *blockchain* pada sistem dan memiliki kode *QR* sebagai tanda verifikasi. Namun, terdapat beberapa kekurangan pada *Website Certifichain* sehingga perlu di lakukan perbaikan pada *Capstone* kali ini.

Pada permasalahan tersebut penulis akan memfokuskan penelitian untuk masalah verifikasi *login* pada *Website Certifichain* dengan menggunakan sistem *Blockchain* untuk melakukan verikasi pengguna. Oleh karena itu, penelitian ini mengangkat judul "*Secure Authentication* pada *Website Certifichain*". Penelitian mengenai *secure authentication* ini diharapkan dapat memberikan penulis dan pembaca dengan sistem yang menjamin integritas data, terutama pada penggunaan *Website Certifichain* sehingga membuka jalan bagi proses verifikasi yang lebih dapat diandalkan dan terpercaya. Selain itu, penyempurnaan dari *Website Certifichain* ini diharapkan memiliki implikasi yang signifikan di berbagai sektor, terutama pada sektor pendidikan, sertifikat profesional, dan pengembangan tenaga kerja dengan meningkatkan efisiensi, transparansi, dan kredibilitas pengelolaan sertifikat.

1.2 Analisis Masalah

Aspek analisis yang terdapat pada masalah ini mencakup beberapa aspek, yaitu:

1.2.1 Aspek Teknis

1. Autentikasi

   Analisis masalah aspek teknis pada autentikasi (*authentication*) melibatkan pemahaman tentang cara sistem komputer mengidentifikasi dan memverifikasi identitas pengguna atau entitas yang mencoba mengaksesnya. Beberapa masalah teknis yang dapat terjadi pada aspek teknis autentikasi yaitu: kelemahan *password*, keamanan data autentifikasi atau keamanan database dan serangan *cyber* seperti *Man in the Middle Attack* (MITM).

2. Validasi Dokumen

   Analisis masalah aspek teknis pada validasi dokumen melibatkan pemahaman tentang proses validasi dokumen melibatkan berbagai elemen yang harus diperhatikan, termasuk memastikan keaslian dan ketentuan hukum yang berlaku mengenai dokumen tersebut. Dokumen juga mungkin memerlukan tanda tangan

atau legalisasi untuk menunjukkan validasi mereka, dan dalam beberapa kasus, terjemahan dokumen ke bahasa yang sesuai dapat diperlukan.

3. Validasi *User*

   Analisis masalah aspek teknis pada validasi *user* melibatkan pemahaman konsep *Authentication, Authorization,* dan *Accounting* (AAA). Integrasi ketiga aspek sangat penting dalam menjaga keamanan, keandalan, dan ketertelusuran dalam pengelolaan akses pengguna ke sumber daya dan layanan, pentingnya dalam merancang dan mengelola sistem dengan benar untuk memastikan bahwa pengguna hanya memiliki akses yang sesuai dan bahwa aktivitas mereka dapat dipantau dan diverifikasi.

1.2.2 Aspek Hukum

Pencurian identitas data *user* yang dilakukan oleh seorang oknum dapat merugikan ke banyak pihak dan dapat dikenakan hukuman sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 67 ayat (1) UU PDP [7]. Dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

1.2.3 Aspek Ekonomi

Pelanggaran data user dapat menghasilkan biaya investigasi, pemulihan data, dan kerugian reputasi yang signifikan, sementara kepatuhan terhadap regulasi menyebabkan denda yang mahal, investasi awal dalam keamanan data dapat mengurangi biaya jangka panjang dan menghasilkan peluang bisnis serta meningkatkan kepercayaan pelanggan.

1.2.4 Aspek Keamanan

Keaslian data user merupakan aspek penting dalam hal keamanan. Dengan banyaknya kasus penipuan identitas digital, hal ini dapat merugikan banyak pihak. Oleh karena itu, untuk meminimalisir kasus penipuan identitas, diperlukan suatu sistem yang dapat memverifikasi keaslian identitas. Mengamankan data pengguna mencakup langkah-langkah seperti enkripsi data, manajemen akses yang ketat, pemantauan aktivitas, perlindungan dari serangan dunia maya, dan kebijakan keamanan yang jelas untuk perlindungan. Melindungi data sensitif pengguna dari ancaman dan pelanggaran. Ini adalah praktik penting untuk menjaga privasi dan kepercayaan pengguna.

1.2.5 *Blockchain*

Analisa aspek *blockchain*, sebagai teknologi baru untuk mewujudkan *Distributed Ledger Technology* (DLT) telah menarik perhatian penelitian yang luas baru-baru ini. Buku besar tersebut bertujuan untuk mencapai manajemen transaksi.meskipun merupakan teknologi canggih yang membawa perubahan besar pada berbagai industri, juga menimbulkan sejumlah permasalahan dan tantangan yang perlu diatasi berikut adalah penjelasan singkat dan jelas mengenai aspek permasalahan *blockchain*:

a. Skalabilitas:
   Blockchain mengalami kesulitan dalam memproses volume transaksi yang tinggi dengan cepat, menyebabkan penundaan dan biaya transaksi yang tinggi.
b. Keamanan dan privasi:
   Meskipun transaksi tidak dapat diubah, identitas pemiliknya tidak sepenuhnya anonim dan serangan dunia maya tetap menjadi ancaman.
c. Peraturan dan kepatuhan:
   Peraturan yang tidak jelas dan kompleksitas hukum menciptakan ketidakpastian bagi pengguna dan dunia usaha.
d. Kesulitan interoperabilitas:
   Kurangnya antarmuka standar antara platform *blockchain* menghambat adopsi teknologi secara luas.
e. Biaya energi dan lingkungan:
   Konsumsi energi yang tinggi di beberapa *blockchain*, terutama *bitcoin*, menimbulkan kekhawatiran mengenai dampak lingkungan.
f. Ketergantungan pada infrastruktur digital:
   Kegagalan infrastruktur digital dapat mengakibatkan *downtime* yang signifikan.
g. Tantangan penerimaan dan kesadaran:
   Kurangnya pemahaman dan kesadaran masyarakat terhadap teknologi *blockchain* menghambat adopsi secara luas.

Semua permasalahan ini memerlukan perhatian yang cermat untuk memastikan bahwa teknologi *blockchain* dapat terus berkembang dan memberikan manfaat yang maksimal.

1.2.6 Permasalahan pada *Website Certifichain*

Pada *Website Certifichain* sebelumnya proses autentikasi *login* hanya dilakukan dengan metode konvensional sehingga perlu dilakukan penambahan algoritma enkripsi pada proses autentikasi. Selain penyempurnaan pada proses autentikasi terdapat 3 garis besar permasalahan

yang ada pada *Website Certifichain* sehingga perlu penyempurnaan, masalah tersebut terdiri dari:

1. *QR Code* yang digunakan untuk pengecekan verifikasi sertifikat sebelumnya berisi data *plaintext* dan *url*, sehingga siapapun yang memiliki *QR Code* tersebut dapat mengakses *url* yang mengarah ke gambar sertifikat kegiatan.
2. Proses verifikasi, pada *Website Certifichain* sebelumnya penyelenggara hanya membuat daftar peserta secara manual tanpa adanya bukti bahwa apakah peserta benar-benar mengikuti kegiatan atau tidak.
3. Tidak adanya *tool* yang dapat memverifikasi keaslian sertifikat, sebelumnya *website certifichain* hanya dapat membuat sertifikat yang dilengkapi *qr code* yang berisi data *plaintext* sehingga sangat rentan untuk dipalsukan oleh peserta kegiatan.

1.3 Kebutuhan yang Harus Dipenuhi

Berdasarkan permasalahan yang telah dijabarkan, terdapat beberapa kebutuhan yang harus dipenuhi untuk menyelesaikan permasalahan integritas pada *Website Certifichain,* yaitu:

1. Pengamanan Data

   Integritas data menjadi permasalahan utama yang membutuhkan perhatian khusus. *Website Certifichain* harus memastikan bahwa data yang disimpan tidak dapat dimanipulasi atau diubah tanpa otorisasi. Langkah-langkah keamanan seperti enkripsi data dan tanda tangan digital harus diimplementasikan untuk memastikan data tetap utuh.
2. Proteksi terhadap Pemalsuan

   Dalam konteks sertifikasi dan dokumentasi, risiko pemalsuan merupakan ancaman serius. *Website Certifichain* harus memastikan bahwa setiap data atau sertifikat yang disimpan tidak dapat dengan mudah dipalsukan. Menggunakan teknologi seperti *blockchain* untuk menciptakan jejak yang transparan dan tidak dapat diubah dapat membantu mengatasi masalah ini.
3. Kontrol akses yang tepat

   Untuk menjaga integritas data, *Website Certifichain* harus memastikan bahwa hanya pengguna yang berwenang yang memiliki akses ke informasi tertentu. Sistem manajemen akses yang canggih dan proses audit tervalidasi yang ketat harus diterapkan untuk memastikan bahwa setiap interaksi dengan data dapat dilacak dan diverifikasi.

4. Autentikasi

   Penting bagi *Website Certifichain* untuk memastikan bahwa pengguna atau organisasi yang terlibat dalam pertukaran data adalah siapa yang mereka katakan. Solusi autentikasi yang kuat, seperti autentikasi dua faktor atau verifikasi identitas tingkat lanjut, perlu diterapkan untuk mencegah serangan dan manipulasi data oleh pihak yang tidak berwenang.

Dengan memperhatikan masalah integritas ini, *Website Certifichain* dapat menciptakan platform yang dapat dipercaya dan andal, memberikan keyakinan kepada pengguna bahwa data yang disimpan di platform aman, terlindungi, dan tidak dapat dimanipulasi karena kelalaian.

1.4 Analisis Solusi yang Ada

Untuk menyelesaikan permasalahan diatas maka diperlukan beberapa penambahan fitur dari masalah tersebut:

1. *Secure QR Code, p*enambahan algoritma enkripsi di *QR Code* untuk data *url* sertifikat kegiatan.
2. Perlu adanya *tool* tersendiri yang dapat mempermudah memverifikasi keaslian peserta, *tool* yang dimaksud dapat berupa sistem yang dapat memimdai *qr code* yang sudah dienkripsi untuk menambah tingkat keamanannya, selain pemindaian *qr code* sistem juga dapat dilengkapi unggah sertifikat untuk memudahkan pengguna sebagai opsi lain.
3. Fitur validasi sertifikat, penambahan fitur untuk verifikasi sertifikat peserta yang terintegrasi dengan *website certifichain* sehingga memudahkan peserta yang menerima sertifikat maupun organisasi yang menerbitkan sertifikat.

Berdasarkan analisa masalah dari poin-poin diatas, solusi dari masalah yang dapat ditawarkan antara lain:

1.4.1 Solusi 1: Penerapan *Blockchain* menggunakan *Ethereum*

Ethereum merupakan *blockchain* dengan komputer yang terintegrasi. Hal ini memberikan dasar untuk membangun pondasi dalam membangun aplikasi diatas *blockchain Ethereum* yang *decentralized, permissionless,* dan tahan *sensor* [8]. Untuk memverifikasi data transaksi, *Ethereum* menggunakan sebuah plugin *Metamask* yang berfungsi sebagai *crypto wallet* (dompet kripto) *Ethereum*. *Metamask* digunakan untuk mengelola *private key* dan menandatangani transaksi pada aplikasi *blockchain* di *web browser* [9].

1. Skenario Penggunaan

   User mengakses *Website Certifichain* kemudian melakukan login dan sistem akan meminta *user* untuk menandatangani transaksi data autentikasi tersebut melalui *crypto wallet.*

2. Karakteristik

   a. *Public Blockchain*

   b. *Open source*

   c. Menggunakan mekanisme konsensus *Proof-of-Stake* (PoS)

   d. Semua orang bisa berinteraksi dengan *smart contract*

   e. Penambahan ECDSA melalui *Metamask* untuk menandatangani kontrak

   f. *Programming Language*: *Solidity*

1.4.2 Solusi 2: Penerapan Blockchain menggunakan *Hyperledger Fabric*

Hyperledger Fabric merupakan platform *Distributed Ledger Technology* (DLT) yang dirancang untuk digunakan ditingkat perusahaan dan bersifat *open source*[10].

1. Skenario Penggungaan

   Fabric menggunakan JWT (*Json Web Token*) sebagai metode autentikasi. Saat *user* melakukan login pada *website certifichain*, server akan men-generate JWT yang berisi data *user* setelah itu *user* dapat berinteraksi dengan jaringan fabric tersebut.

2. Karakteristik

   a. *Private* Blockchain

   b. *Open Source*

   c. Tidak menggunakan *cryptocurrency* sehingga tidak memerlukan konsensus *Proof-of-Stake* (PoS) ataupun *Proof-of-Work* (PoW)

   d. Memiliki struktur blockchain yang hanya dapat diikuti oleh *authorized users*

   e. Memiliki dukungan bawaan untuk ECDSA yang memungkinkan penggunaan sertifikat berbasis ECDSA yang dikeluarkan oleh *Certification Authority* (CA) untuk autentikasi

   f. *Programming Language*: Go, Java, Javascript, Python

1.5 Kesimpulan dan Ringkasan CD-1

Melindungi data melalui enkripsi yang kuat, kontrol akses yang ketat, penerapan autentikasi yang aman dan penerapan kebijakan keamanan yang ketat telah menjadi hal yang penting dalam sebuah pengamanan data. Selain itu, perbaikan pada *Website Certifichain* melalui penambahan fitur algoritma enkripsi pada *QR Code*, pengembangan fitur validasi peserta kegiatan, dan peningkatan proses verifikasi yang lebih aman, merupakan langkah penting yang perlu ditekankan. Hal tersebut membuat *Website Certifichain* mampu meningkatkan akurasi dan keandalan proses verifikasi, memastikan bahwa setiap entitas terverifikasi secara valid. Dengan peningkatan proses verifikasi yang lebih aman, *Website Certifichain* mampu meminimalkan risiko manipulasi data dan memastikan integritas dari setiap sertifikasi yang dikeluarkan.