

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Terobosan teknologi informasi, komunikasi dan keamanan akan terus berkembang seiring dengan perkembangan zaman. Tantangan yang dihadapi itu pun akan menyongsong setiap pembaruan teknologi baru. *Blockchain* adalah buku besar digital terdistribusi yang memiliki tingkat keamanan dan biasanya tanpa ada otoritas pusat [1]. Teknologi *blockchain* diperkenalkan oleh Satoshi Nakamoto dengan mengandalkan kriptografi tanda tangan digital, *time stamp*, dan *Prof of work*. *Blockchain* akan membuat *time stamp* dari setiap kegiatan yang berlangsung pada sistem, selanjutnya akan dilakukan fungsi *hashing* dan akan di masukan ke *Prof of Work* (PoW) [2]. Teknologi buku besar terdistribusi tersebut membuat terobosan sehingga menarik perhatian dan memicu terobosan di berbagai industri [3]. *Blockchain* memiliki cara kerja dengan membuat banyak blok sehingga bisa saling berkomunikasi dan memiliki fungsi mempermudah proses transaksi dan proses eksekusi. Teknologi ini memberikan tiga asas dalam pelepasannya, diantaranya adalah desentralisasi, transparan, dan kekal, ketiga dasar tersebut membuat *blockchain* menjadi pusat perhatian di bidang industri yang mana teknologi tersebut memiliki tingkat keamanan yang tinggi. Penciptaan *blockchain* digunakan sebagai bentuk yang memungkinkan pencatatan dan pendistribusian atau penyebaran informasi digital tanpa memiliki akses untuk di ubah, dimusnahkan, dibuang, dihilangkan dan dihapus. Pada aspek mengelola identitas digital individu atau entitas, teknologi *blockchain* berperan membantu untuk mengatasi masalah keamanan, privasi, dan kepemilikan identitas data. Pada *blockchain* sistem manajemen identitas, terdapat sejumlah besar *nodes* (komputer) yang terdistribusi [4]. Node-node tersebut berfungsi untuk menyediakan penyimpanan dan akses komputasi, secara sederhannya *node* dapat bertindak sebagai *client* atau *server*. Dalam industri telekomunikasi satelit, *blockchain* dapat dimanfaatkan dalam bidang keamanan. Dalam jaringan *blockchain* yang dijalankan secara *peer to peer* (P2P). *node* memiliki peran penting berpartisipasi dalam validasi dan verifikasi.

Teknologi komunikasi satelit memegang peran penting dalam sektor, seperti telekomunikasi, pertahanan, navigasi, dan penelitian. Sistem komunikasi satelit memiliki cakupan yang lebih luas dibandingkan dengan sistem komunikasi lain. Dengan bertambahnya kebutuhan akan jaringan komunikasi di daerah yang sulit dijangkau, *Very Small Aperture Terminal* (VSAT) memberikan solusi terhadap hal tersebut. VSAT merupakan teknologi komunikasi berbasis satelit yang menggunakan antena berdiameter kurang dari 2.5-meter dan mampu menghubungkan *point to multipoint* atau *multipoint to point* [5].

Sistem komunikasi satelit dan *blockchain* memiliki perbedaan, *blockchain* sendiri adalah sebuah sistem untuk menyimpan sebuah informasi digital yang tersusun dari berbagai macam rangkain *block* sementara sistem komunikasi satelit merupakan sebuah sistem komunikasi yang memanfaatkan satelit sebagai *repeater* / penguat di luar angkasa. Dengan peran yang kompleks pada sistem komunikasi satelit, sejumlah tantangan seperti keamanan, otentikasi, izin akses dan kontrol terhadap data identitas menjadi isu yang menghambat di sektor ini baik dari sisi *ground segment*, *space segment* hingga pengguna. *Identity Management* (IdM) memiliki tiga sintesis yaitu ShoCard yang menggunakan teknologi *blockchain* untuk keamanan dan fokus pada *digital signature* atau tanda tangan digital dan jejak audit, uPort memanfaatkan teknologi Ethereum (*Self-Sovereign Identity*) dan memberikan kontrol langsung kepada pemilik identitas, dan Sovrin menggunakan teknologi buku besar yang terdistribusi [6]. Teknik ShoCard pada manajemen identitas menerapkan keamanan dan ketahanan data dari teknik enkripsi serta diperkuat dengan menerapkan teknik kriptografi [6].

Perangkat VSAT terdiri dari tiga komponen utama yaitu *Block Up Converter* (BUC), modem, router dan antenna. Modem satelit menjadi perangkat kunci dalam sistem komunikasi satelit karena perannya dalam mengatur dan mengintegrasikan ke jaringan *blockchain*. Dengan permasalahan yang kompleks uji coba harus dilakukan dari sistem yang paling dasar yaitu waktu komputasi dalam teknik keamanan yang terdapat pada manajemen identitas / *Identity Management* (IdM) *blockchain*. *Blockchain* dalam aspek manajemen identitas dapat diimplementasikan dalam komunikasi satelit dengan mengintegrasikan sistem *unique id* pada modem satelit VSAT. Penggabungan jaringan *blockchain*

dan jaringan satelit dapat diterapkan sesuai fungsi pada sistem *blockchain* yang mengelola dan memiliki penambang sehingga membentuk *node* pada sistem komunikasi satelit yang memiliki *ledger* [7]. Kolaborasi dari penggabungan *blockchain network, space, air*, serta *ground* memberikan peningkatan keamanan yang tinggi [8]. Solusi penerapan ini melibatkan penggunaan modem satelit pada VSAT untuk memberikan *unique id* dan terhubung ke jaringan *blockchain*.

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, maka dapat di deskripsikan permasalahan di atas sebagai berikut:

1. Menerapkan aspek keamanan manajemen identitas *blockchain* pada komunikasi satelit.
2. Menerapkan sistem integrasi teknologi keamanan *blockchain* dan kriptografi dalam manajemen identitas untuk komunikasi satelit berdasarkan waktu komputasi.
3. Menambahkan sistem konsensus Pow, PoA, kriptografi *hash* serta *Elliptic Curve Digital Signature Algorithm (ECDSA)* pada sistem *blockchain*.

## 1.3 Tujuan dan Manfaat

Di bawah ini merupakan tujuan yang diambil dari rumusan masalah yang terjadi:

1. Membuktikan apakah manajemen identitas pada *blockchain* dapat secara efektif diterapkan di komunikasi satelit.
2. Menganalisis dan membuktikan efektivitas penerapan manajemen identitas dengan menggunakan metode keamanan *blockchain* dan kriptografi pada sistem komunikasi satelit berdasarkan waktu komputasi.
3. Menganalisis pengaruh perubahan terhadap variabel waktu pada *block* dan *node* melalui metode keamanan *blockchain* dan kriptografi pada komunikasi satelit.

## 1.4 Batasan Masalah

Adapun batasan masalah terdapat pada poin di bawah:

1. Sistem komunikasi satelit di ambil pada sektor *unique id* yang terdapat pada modem satelit. *Ground segment, space segment*, serta teknik terkait komunikasi satelit di anggap sempurna.
2. Perangkat modem beserta *unique id* telah ditentukan sebelumnya, serta tidak menggunakan perangkat modem asli.
3. Sistem jaringan *blockchain* dirancang dengan menggunakan bahasa pemrograman *Python* dalam bentuk konsep, tidak dijalankan pada arsitektur jaringan *real blockchain*.
4. Kode program dibuat untuk menjalankan satu perintah dalam satu waktu atau beroperasi dalam mode *single threading*.

### **1.5 Metode Penelitian**

Dalam mengerjakan tugas akhir ini menggunakan beberapa tahapan seperti terterang di bawah:

1. Observasi

Pada tahap pertama akan dilakukan observasi masalah. Permasalahan berdasarkan studi kasus lapangan yang terjadi pada saat melakukan kegiatan magang di industri telekomunikasi satelit.

2. Studi literatur

Pada bagian ini akan dilakukan pengumpulan berbagai refefrensi terkait penelitian terdahulu yang relevan dengan topik.

3. Perancangan sistem

Perancangan *system* dilakukan sesuai referensi yang terdapat pada studi literatur.

4. Simulasi

Setelah melakukan perancangan maka akan dilakukan simulasi dengan tujuan menentukan waktu komputasi.

5. Analisis

Langkah terakhir adalah analisis, dengan tujuan pokok menguraikan bagian dan penelaah hubungan antar bagian untuk memperoleh kesimpulan keseluruhan.

## 1.6 Jadwal Penelitian

Acuan dari pengerjaan tugas akhir ini dapat dilihat pada tabel di bawah, dimana pengerjaan akan berlangsung lebih dari empat bulan. Tabel 1.1 dibawah merupakan *timeline* pengerjaan.

**Tabel 1.1 *Timeline* Pengerjaan Tugas Ahir dan *Milestone***

No.	Deskripsi Tahapan	Durasi	Tanggal Selesai	<i>Milestone</i>
1	Desain sistem <i>block</i> menggunakan <i>Proof of Work</i> (PoW)	3 minggu	15/02/2024	Program bisa dijalankan
2	Desain sistem <i>node</i> menggunakan PoW dan <i>Prof of Authority</i> (PoA)	3 minggu	05/03/2024	Program dapat di <i>runing</i> dan menghasilkan <i>output</i>
3	Pengujian desain <i>block</i> dan <i>node</i>	4 minggu	11/04/2024	Mendapatka <i>output</i> sesaauai standarisasi
4	Penyusunan laporan/buku TA	2 minggu	12/04/2024	Buku TA selesai