

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Hubungan internasional didefinisikan sebagai hubungan antar negara. Hubungan internasional merupakan suatu kajian mengenai seluruh interaksi antar aktor-aktor negara yang melewati batas negara, termasuk didalamnya meliputi politik luar negeri atau politik internasional, perkembangan nilai-nilai dan etika internasional. Skema dasar hubungan internasional yaitu mengkaji perilaku aktor-aktor negara maupun non-negara dalam fenomena internasional yang kompleks. Adanya kesenjangan dalam hal pemerataan sumber daya alam dan perkembangan industri melatarbelakangi saling ketergantungan dari setiap negara sehingga mendorong untuk terjalinnya hubungan internasional (Suryana et al., 2015: 31).

Perkembangan peradaban manusia yang bergerak dinamis dalam masyarakat lintas wilayah dan kehadiran teknologi informasi dan komunikasi menimbulkan akselerasi proses globalisasi yang berakibat pada pudarnya batas-batas wilayah negara sehingga meningkatkan intensitas interaksi antar masyarakat dunia. Globalisasi merupakan suatu upaya penyatuan masyarakat dunia yang berarti bahwa proses dimana berbagai peristiwa, keputusan dan aktivitas masyarakat dibelahan dunia yang satu dapat berdampak pada masyarakat di belahan dunia yang lain (Nugroho, 2020: 36).

Dewasa ini perkembangan teknologi yang didukung dengan inovasi digital menjadi salah satu faktor lahirnya trend transformasi digital yang secara masif

berpengaruh terhadap peningkatan produktivitas kegiatan manusia. Inovasi merupakan sebuah kalimat sakral yang selalu disuarakan untuk menginspirasi, memotivasi dan berkreasi dalam menghasilkan suatu nilai pada suatu produk, jasa, proses, hingga sistem manajemen (Nasution & Kartajaya, 2018: 1). Teknologi melahirkan inovasi, dan inovasi mencetak profesi. Tidak diragukan lagi bahwa teknologi, informasi dan komunikasi telah memberi banyak kontribusi, seperti kemudahan mengakses informasi, menunjang efektivitas kerja dan membawa kemudahan dalam menopang kegiatan ekonomi. Meski demikian, dampak positif tentu di iringi dengan dampak negatif pula dan tentu memberikan peluang serta tantangan baru dalam pelaksanaannya.

Eskalasi perkembangan teknologi informasi dan komunikasi sangat berdampak terhadap pola interaksi dalam hubungan internasional. Pola interaksi yang pada umumnya dilakukan secara nyata, kini dapat dilakukan secara maya, kemunculan ruang maya atau virtual (*cyberspace*) menjadi arena baru dalam menjalin hubungan internasional guna mencapai kepentingan nasional suatu negara, keamanan *cyberspace* menjadi isu penting dan prioritas bagi pemerintahan secara global (Triwahyuni & Yani, 2018: 3).

Kemunculan ruang baru virtual telah mengubah jarak dan waktu menjadi tidak terbatas juga membentuk kelompok masyarakat baru atau *cyber society* yaitu interaksi masyarakat yang terkoneksi pada jaringan komputer yang menempatkan pada struktur jaringan komunikasi yang kompleks, hingga mengakibatkan terjadinya disrupsi informasi. Fenomena digitalisasi secara luas memicu timbulnya suatu tantangan yaitu krisis data atau ancaman terhadap informasi. Keamanan

informasi menimbulkan dilematis tersendiri terhadap pengadopsian teknologi baru. Penyalahgunaan dampak dari teknologi dalam mengakses informasi menjadi celah untuk melakukan tindakan kriminalitas seperti penipuan, pencurian data ataupun penyerangan di ruang siber (Nugroho, 2020:100).

Era revolusi industri 4.0 memicu perkembangan dan penerapan teknologi dalam berbagai bidang, begitupula dengan teknologi *blockchain* yang berkembang pesat dengan menawarkan sistem keamanan data terhadap penggunaannya. Pada mulanya, Blockchain dibentuk dan dikembangkan untuk melengkapi kebutuhan akan sistem yang lebih efisien, hemat biaya, aman dan terjamin untuk melakukan tugas mendata berbagai transaksi keuangan yang terjadi di masa depan. Teknologi *blockchain* mulai populer sejak tahun 2009 berbarengan dengan munculnya fenomena Bitcoin, bermula dari munculnya keresahan yang diakibatkan karena terjadinya krisis finansial di dunia. Popularitas *Blockchain* sering kali dikaitkan dengan Bitcoin yang merupakan salah satu mata uang virtual, kenyataannya bitcoin hanyalah salah satu produk yang berbasis pada sistem *blockchain* (ASEAN Digital Senior Official Meeting, 2021).

Blockchain dan Bitcoin tidak terlepas dari permasalahan finansial, akan tetapi pengaplikasian sistem Blockchain dapat digunakan pada semua aspek kehidupan, contohnya blockchain dapat digunakan dalam pengumpulan data, akses data, dan simplifikasi kinerja sistem. Konsep implementasi Bitcoin berbasis teknologi *Blockchain* yang sukses memecahkan permasalahan pengeluaran ganda (*double spending*) yaitu transaksi berbeda dengan uang yang sama telah banyak menginspirasi berbagai aplikasi seperti *smart contract*, layanan keuangan lintas

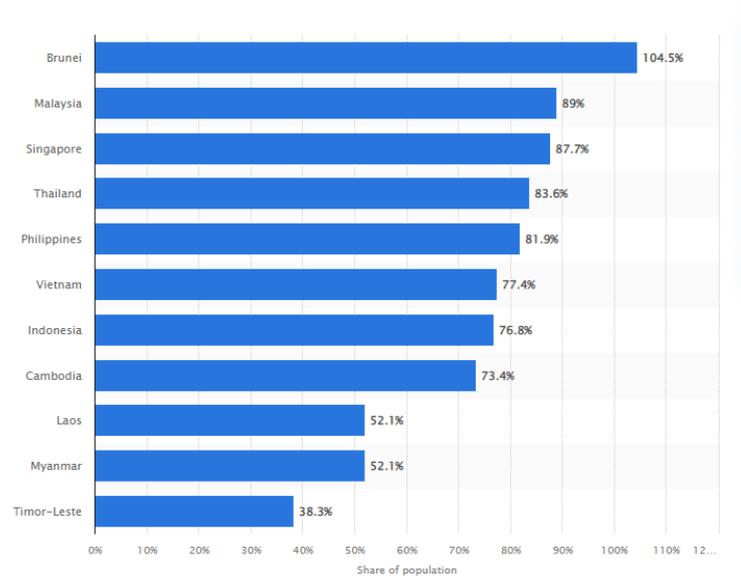
batas, sistem kustodian yang tidak dapat dihapus, rantai pasokan *blockchain*, dan beberapa aplikasi atau platform yang berkaitan dengan transaksi dan penyimpanan aset (Center for Innovation Policy and Government, 2018) .

Dalam perkembangannya, inovasi teknologi yang ditawarkan sistem *blockchain* dalam hal eskalasi keamanan data siber, dapat menjadi infrastruktur pendukung dalam menghadapi ancaman siber yang kompleks. Sistem jaringan *blockchain* tidak memiliki perantara pihak ketiga yang mengelola informasi dan data dari setiap pengguna. Jaringan yang menggunakan teknologi ini melakukan proses perekaman, validasi dan verifikasi serta konfirmasi otomatis oleh setiap pengguna (Yahya, 2019).

Tingkat keamanan informasi yang memakai teknologi ini dilindungi oleh teknologi kriptografi dengan tujuan mengamankan data agar tidak mudah diretas dan dimanipulasi, yang dimana peretas informasi di jaringan ini membutuhkan waktu yang lama. Namun, kekuatan teknologi ini sering disalahgunakan untuk menutupi transaksi ilegal oleh penjahat dunia maya. Jaringan *blockchain* merupakan alternatif yang sering dipilih oleh para pelaku kriminalitas sebagai tempat yang aman untuk bertransaksi karena kesulitan dalam melacak identitas dan transaksi yang terjadi dalam jaringan ini (Yahya, 2019).

Ancaman keamanan siber dapat terjadi kepada siapapun bahkan negara maju pun tidak terlepas dari ancaman siber, termasuk negara-negara di kawasan Asia Tenggara tidak dapat terhindar dari ancaman siber bahkan menjadi sasaran serangan siber karena jumlah pengguna internet yang tinggi. Pada tahun 2020 berdasarkan laporan *Global Digital Report*, wilayah ASEAN menjadi pangsa pasar

terbesar ketiga didunia dengan jumlah populasi 663,47 juta jiwa dan persentase pengguna internet yang relatif tinggi (INTERPOL Report Charts Top Cyberthreats in Southeast Asia, 2021: 5).



**Gambar 1.1** Penetrasi Internet Asia Tenggara (%)

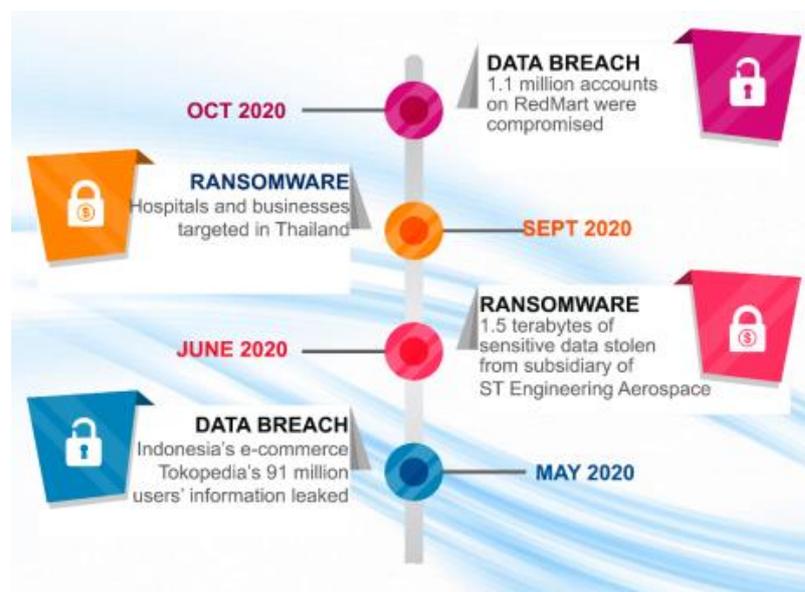
Sumber: Statista.com

Berdasarkan laporan data *Statista Research Department* penetrasi internet dikawasan Asia Tenggara per Juni 2021 persentase tertinggi di tempati oleh Brunei 104.5%, diurutan kedua Malaysia 89%, selanjutnya Singapura 87.7%, Thailand 83.6%, Filipina 81.9%, Vietnam 77.4%, Indonesia 76.8%, Kamboja 73.4%, Laos dan Myanmar 52.1% (<https://www.statista.com/statistics/487965/internet-penetration-in-southeast-asian-countries/> diakses 18 April 2022).

Pertumbuhan eksponensial di ASEAN pada sektor teknologi digital khususnya teknologi keuangan dan *e-commerce* dianggap menjadi salah satu pasar paling kompetitif didunia menjadi daya tarik investor global dan sasaran jaringan kriminal untuk melakukan serangan yang kompleks hingga menyebabkan

kerusakan berskala besar yang dapat menghambat kepercayaan dan ketahanan dalam ekonomi digital. Dengan demikian, perlu diimbangi dengan peningkatan pertahanan keamanan siber dan regulasi yang tepat serta meningkatkan literasi dalam penggunaan ruang siber (INTERPOL Report Charts Top Cyberthreats in Southeast Asia, 2021: 11).

Dalam laporan INTERPOL *Cyberthreats in Southeast Asia* (2021) melaporkan bahwa percepatan transformasi digital yang didorong oleh adanya pandemi covid-19 memberikan peluang terhadap pelaku kejahatan siber untuk mengeksploitasi situasi guna meraih keuntungan. Pada tahun 2020, di masa pandemi covid-19 industri layanan kesehatan menjadi target utama pelaku kejahatan siber.



**Gambar 1. 2** Mayoritas Insiden Siber di ASEAN 2020

Sumber: INTERPOL.int

Gambar diatas menunjukkan beberapa insiden pelanggaran data serius yang terjadi di kawasan ASEAN. Serangan siber terhadap infrastruktur kritis menjadi salah satu bentuk kejahatan siber yang tumbuh dengan cepat dan meningkatnya

jumlah sistem kontrol yang terhubung dan terpusat. Serangan terhadap infrastruktur bukan hanya merugikan perekonomian, melainkan juga berimbas pada kepercayaan publik terhadap layanan kritis dan pemerintahan. Selain serangan siber dan pelanggaran data, penipuan online terkait covid-19 juga marak terjadi dengan modus penjualan alat kesehatan dan pelindung diri. Dibandingkan 2019, tahun 2020 terjadi peningkatan modus penipuan (*fraud*) online dengan meniru pejabat pemerintahan dari Kementerian Kesehatan, kepala polisi dan pejabat lainnya untuk mendapatkan informasi rahasia (INTERPOL Report Charts Top Cyberthreats in Southeast Asia, 2021: 12).

Pada dasarnya, segala bentuk jenis ancaman siber akan mengganggu stabilitas politik dan perkembangan ekonomi digital di ASEAN. Oleh karena itu, dalam pertemuan Menteri Digital ASEAN yaitu *ASEAN Digital Ministers Meeting* (ADGMIN) dalam rangka percepatan transformasi digital, sepakat untuk meningkatkan kerjasama disektor teknologi dan informasi, yaitu kerjasama dalam isu perlindungan data dan pertukaran data lintas batas negara (*cross-border data flow*). Sejalan dengan yang dikemukakan oleh Menteri Kominfo Republik Indonesia bahwa pentingnya perlindungan data pribadi dan keamanan data. Dimana saat ini, data menjadi aset penting dan bernilai ekonomi yang signifikan sehingga diperlukan pengelolaan dan penggunaan yang tepat dengan mengedepankan prinsip kedaulatan data, yaitu *a reciprocal, lawful, fair, and transparent manner* ((Ditjen Aptika, n.d. 2021 melalui <https://aptika.kominfo.go.id/2021/01/pertemuan-menteri-digital-asean/> diakses pada 29/05/2022)

Sejak kemunculannya, teknologi blockchain mulai menarik perhatian pemerintah negara-negara di dunia termasuk pemerintah negara anggota ASEAN yang ditandai dengan dilaksanakannya pertemuan *ASEAN Digital Senior Official Meeting (ADGSOM) and Related Meetings* yaitu pengkajian mengenai tren perkembangan teknologi blockchain serta manfaatnya bagi layanan digital pemerintahan dan berbagi gagasan serta pengalaman untuk mengevaluasi penerapan teknologi blockchain.

Menyadari arti penting kehadiran teknologi blockchain dan kebutuhan untuk mengaplikasikan teknologi blockchain berskala besar yang dimana beberapa negara telah menjadikan teknologi blockchain sebagai prioritas strategis dalam rencana pembangunan digitalnya. Dalam perkembangannya, teknologi blockchain telah diadopsi oleh beberapa perusahaan yang diaplikasikan dibidang pertanian, rantai pasok, dan layanan finansial. Mayoritas negara anggota ASEAN sepakat bahwa teknologi blockchain sangat penting sebagai infrastruktur kritis terhadap *e-service* yang mengutamakan kepercayaan dan cocok diaplikasikan pada layanan pemerintahan (ASEAN Digital Senior Official Meeting, 2021: 38).

Pemerintah Indonesia mulai beradaptasi dengan keberadaan teknologi blockchain dengan pembaharuan regulasi dan implementasinya, yang dilatarbelakangi oleh tren asset kripto yang nilai transaksinya terus meningkat mencapai 2,3 T. Dimana investor asset kripto mencapai 7,4 juta orang meningkat 85% dari tahun 2020 sebanyak 4 juta orang. Asosiasi Blockchain Indonesia (ABI) bertujuan untuk menggerakkan dan menata pelaku teknologi Blockchain dalam menciptakan lingkungan bisnis berkualitas yang memacu pemahaman,

pemanfaatan, kemajuan dan daya saing teknologi Blockchain. Inovasi Finhack Blockchain ditetapkan sebagai hackathon terbesar di Asia Tenggara oleh BCA dan ABI. Pada tahun 2021, dewan blockchain didirikan sebagai lembaga yang mengamati dan mengawasi industri blockchain di Indonesia (ASEAN Digital Senior Official Meeting, 2021: 39).

Laos memfokuskan adopsi perkembangan teknologi blockchain pada *cryptocurrency* dan layanan finansial. pemerintah Laos telah memberi wewenang kepada enam perusahaan untuk memperdagangkan dan menambang *cryptocurrency* sementara kementerian terkait akan menyusun peraturan yang mengatur penggunaannya termasuk peraturan aset digital. Bank sentral Laos telah menandatangani nota kesepahaman dengan badan kerjasama internasional Jepang untuk meninjau perkembangan mata uang digital bank sentral. Selain blockchain untuk layanan keuangan (ASEAN Digital Senior Official Meeting, 2021: 40).

Malaysia melihat teknologi blockchain yang mencakup blockchain dan DLT sebagai satu kesatuan, bersamaan dengan gagasan yang dituju di tingkat ISO, seperti TC 307 (*Committee for Blockchain and Distributed Ledger Technology*), di mana Malaysia adalah salah satu anggota pendirinya. Tahun 2018, Malaysia menggunakan Blockchain untuk memperbaiki layanan keuangan Syariah, energi terbarukan, dan sektor kelapa sawit. Tahun 2019, Bursa Malaysia menggunakan blockchain dalam *proof-of-concept* (PoC) yang diarahkan untuk transparansi yang lebih besar dan operasi yang lebih lancar di layanan Pinjam Meminjam Efek (ASEAN Digital Senior Official Meeting, 2021: 42).

Pada tahun 2021, dibentuknya ASEAN Blockchain Konsorsium kolaborasi antara Asosiasi Blockchain Indonesia (ABI), *Blockchain Association Singapore* (BAS), *Distributed Ledger Technology Association of the Philippines* (DLTAP), *Labuan International Business and Financial Centre* (Labuan IBFC), *Thailand Digital Asset Operators Trade Association* (TDO) and *Blockchain Australia* (BA) yang bertujuan untuk memperkuat hubungan lintas batas dan mendorong edukasi blockchain, berbagi pengetahuan terkait pengembangan aset digital dan mempromosikan adopsi teknologi blockchain di ASEAN dan Australia (Labuan IBFC, n.d. 2021 melalui <https://www.labuanibfc.com/resources-events/media/press-releases/asean-blockchain-consortium-formed-to-collaborate-on-digital-assets-and-enterprise-blockchain-strengthening-cross-border-relationship/> diakses pada 1/06/2022).

Ekosistem HARA adalah platform terdesentralisasi, aman dan transparan yang dibangun di atas blockchain Ethereum. HARA merupakan perusahaan asal Indonesia berfokus pada sektor pertanian dan pangan di negara-negara berkembang karena sektor pertanian memiliki peran penting bagi pembangunan ekonomi negara. Potensi dampak dari akses data global dan transparan pada sektor pertanian dan pangan adalah peningkatan produktivitas, rantai pasok dan efisiensi pasar. Pertumbuhan di sektor ini secara langsung mempengaruhi sektor kesehatan, seperti meningkatnya kemampuan untuk membeli dan mengonsumsi makanan yang lebih ekonomis dan lebih baik. Fitur yang menonjol dari Platform HARA Data Exchange adalah:

- Akses data yang aman, terbuka, terhubung, dan terdesentralisasi

- Riwayat data yang dapat dilacak dan transparan
- Izin akses data yang terdesentralisasi dan individu
- Fasilitasi pertukaran token cair dan tanpa batas yang dapat ditransaksikan secara global

Pengaplikasian teknologi blockchain pada platform Pertukaran Data HARA yaitu menggunakan *Ethereum* untuk membuat *smart contract*, melacak dan memvalidasi transaksi dan hak kepemilikan, melakukan transaksi melalui HARA token, dan memungkinkan token untuk diperdagangkan di bursa token pihak ketiga (HARA, 2019 melalui <https://www.hara.ag/white-paper> diakses pada 1/06/2022).

Pada dasarnya, blockchain menggunakan jaringan terdistribusi *peer-to-peer* untuk mengkonfirmasi sistem yang terdesentralisasi. Blockchain akan menyimpan segala jenis pertukaran data yang dalam sistem blockchain disebut transaksi. Setelah transaksi diverifikasi, ia masuk ke dalam sistem dan tersimpan sebagai blok.

Dalam penelitian ini menggunakan beberapa penelitian terdahulu yang relevan dan referensi salah satunya penelitian yang dilakukan oleh Iqbal Ramadan (2019) dari Universitas Pertamina yang berjudul, Strategi Keamanan *Cyber Security* di kawasan Asia Tenggara: *Self - Helf* atau *Multilateralism*. Metode yang digunakan dalam penelitian ini yaitu metode analisis kualitatif dengan menggunakan pendekatan *neorealism* dan *neoliberal*. Fokus kajian yaitu isu keamanan dengan konsep *defensive realisme* dan *multilateralism*. Tujuan dari penelitian ini untuk membahas strategi paling tepat dalam menjaga keamanan siber di Asia Tenggara. Hasil penelitian menjelaskan bahwa negara di Asia Tenggara dapat menggabungkan strategi *self help* dari interpretasi *realis* yaitu negara perlu

meningkatkan kapabilitas dan kapasitasnya secara teknologi dengan strategi kerjasama multilateral dari interpretasi *neoliberalis institusionalis* dalam upaya mengantisipasi ancaman *cyber* yang berpotensi mengganggu stabilitas politik, sosial, ekonomi dan militer di kawasan Asia Tenggara.

Penelitian selanjutnya yang berjudul *Blockchain Technology Immutability Framework Design in e-Government* yang dilakukan oleh Ahmad, D., Lutfiani, N., Ahmad, A.D.A.R., & Rahardja, U. (2021). Penelitian ini menggunakan metode analisis kualitatif dengan tujuan penelitian membahas penerapan teknologi *blockchain* dalam meningkatkan pelayanan publik dan keamanan data. Hasil penelitian menerangkan bahwa utilitas penerapan teknologi *blockchain* berdampak utama pada aspek keamanan, transparansi data dan kepercayaan publik. Seperti pemerintah Dubai yang mulai mengadopsi teknologi *blockchain* dalam upaya mengurangi penggunaan kertas dengan mentransformasikan semua dokumen penting secara digital.

Selanjutnya penelitian yang dilakukan oleh Chikelue .C. Nwabuikie, Vincent.A. Onodugo, Austine Arachie, Ugonna .C.Nkwunonwo (2020) dengan judul *Blockchain Technology for Cyber Security: Performance Implications on Emerging Markets Multinational Corporations, Overview of Nigerian Internationalized Bank*. Penelitian ini menggunakan desain penelitian eksploratif dengan maksud mengeksplorasi manfaat, kelebihan dan kekurangan dari sistem keamanan siber berbasis *blockchain* pada kinerja bisnis Perusahaan Multinasional di pasar negara berkembang. Hasil penelitian ini menjelaskan bahwa teknologi *blockchain* untuk keamanan siber menjadi tolak ukur tertinggi dalam menghadapi

ancaman keamanan siber dengan sistem kriptografi yang rumit, memungkinkan Perusahaan Multinasional untuk melindungi informasi pengguna dan klien. Perusahaan Multinasional dapat mengadopsi teknologi *blockchain* secara *private* atau *hybrid*. Penerapan teknologi *blockchain* membutuhkan jaringan komputer yang mumpuni dengan kecepatan tinggi untuk menjalankan fungsinya. Hal ini menuntut peningkatan kapasitas perangkat keras dan konsumsi energi.

Penelitian yang dilakukan oleh Inaz.I.N., Reza.P., Salsabila.R.A. (2021) dari Universitas Diponegoro yang berjudul Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan yuridis empiris. Hasil penelitian ini mengemukakan bahwa penerapan sistem keamanan blockchain menjadi solusi sebagai bentuk inovasi dalam sistem keamanan siber di Indonesia terhadap perlindungan data pribadi. Penerapan sistem blockchain membutuhkan peran *stakeholder*, pemangku kebijakan untuk mendesain sebuah payung khusus terkait keamanan siber yang berorientasi pada era disrupsi terhadap perlindungan data.

Berdasarkan beberapa penelitian terdahulu, diantaranya belum terdeskripsikan mengenai penerapan teknologi *blockchain* berdasarkan pada satu kawasan yang terintegrasi. Kesamaan dengan penelitian-penelitian sebelumnya yaitu pembahasan mengenai urgensi keamanan siber dan peran teknologi *blockchain*. Perbedaannya terdapat pada pengkajian masalah dimana penelitian sebelumnya membahas penerapan teknologi *blockchain* pada suatu negara dan perusahaan multinasional. Sedangkan penelitian ini membahas dampak dari

perkembangan dan prospek teknologi *blockchain* terhadap keamanan siber dalam proses transformasi digital di ASEAN (*Association of Southeast Asian Nations*).

Alasan dalam pemilihan topik ini yaitu eksistensi teknologi *blockchain* yang semakin populer dan berkembang dengan menawarkan jaminan sistem keamanan siber terdesentralisasi dan terdistribusi, dan pada implementasinya dapat diadopsi di berbagai sektor industri. ASEAN dipilih karena popularitasnya sebagai salah satu kawasan terintegrasi dengan jumlah populasi yang tinggi dan jumlah pengguna internet yang terus meningkat. Pertahanan keamanan siber masih dalam tahap pengembangan menjadi rentan terhadap ancaman keamanan siber. Hal ini yang mendorong peneliti untuk melakukan penelitian dengan judul **“Dampak Perkembangan Teknologi *Blockchain* Terhadap Keamanan Siber Di ASEAN”**.

Ketertarikan dalam penelitian ini didukung dengan beberapa matakuliah dalam studi Ilmu Hubungan Internasional, yaitu sebagai berikut:

1. Hubungan Internasional di Asia Tenggara

Matakuliah ini mempelajari latar belakang historis dan geografis yang berpengaruh terhadap dinamika sosial, ekonomi, politik dan keamanan di Asia Tenggara serta menggambarkan pola-pola interaksi dalam menjalin kerjasama internasional.

2. Komputer Aplikasi HI-V (ICT for IR)

Matakuliah ini mempelajari bagaimana teknologi berperan penting dalam perkembangan informasi dan komunikasi yang kemudian mempengaruhi pola-pola komunikasi dalam hubungan internasional.

### 3. Keamanan Siber

Matakuliah ini mempelajari konsep keamanan baru dengan potensi menimbulkan kejahatan baru dalam hubungan internasional. Ancaman keamanan baru dengan menggunakan teknologi sebagai perantara untuk melancarkan aksi penyerangan terhadap perangkat komputer sasaran serangan siber.

## 1.2 Rumusan Masalah

### 1.2.1 Rumusan Masalah Mayor

Berdasarkan pada latar belakang masalah yang telah dipaparkan diatas, maka dalam penelitian ini, penulis mengajukan rumusan masalah mayor sebagai berikut: *Bagaimana Dampak dari Perkembangan Teknologi Blockchain terhadap Keamanan Siber di ASEAN ?*

### 1.2.2 Rumusan Masalah Minor

1. Bagaimana konsep implementasi teknologi blockchain terhadap keamanan siber dalam proses transformasi digital di ASEAN?
2. Bagaimana mitigasi penerapan teknologi blockchain terhadap keamanan siber di ASEAN ?
3. Bagaimana prospek teknologi blockchain terhadap keamanan siber dalam proses transformasi digital ASEAN?
4. Apa kendala dalam penerapan teknologi *blockchain* terhadap keamanan siber dalam proses transformasi digital di ASEAN ?

### **1.2.3 Pembatasan Masalah**

Pembatasan masalah mengarah pada pembahasan yang terfokus pada perkembangan teknologi *blockchain* terhadap ancaman serangan siber dalam proses transformasi digital di ASEAN pada rentang waktu 2017 - 2022. Tepatnya 12 November 2017 pada KTT ASEAN ke-31 merupakan babak baru bagi ASEAN dalam upaya meningkatkan transformasi digital dengan disahkannya ASEAN Digital Masterplan 2025. Penelitian dibatasi sampai dengan Maret 2022, karena berkaitan dengan adaptasi perubahan skema kebijakan dalam kerangka kerja dan program percepatan pemulihan ekonomi ASEAN di masa pandemi Covid-19. Pembatasan masalah juga merujuk pada pembahasan yang menempatkan teknologi *blockchain* dalam lima skala prioritas strategis pada adaptasi teknologi baru di ASEAN yaitu Singapura, Indonesia, Malaysia dan Thailand.

## **1.3 Maksud dan Tujuan Penelitian**

### **1.3.1 Maksud Penelitian**

Maksud dari penelitian ini yaitu untuk mengetahui dan memahami bagaimana perkembangan teknologi *blockchain* dapat mempengaruhi pertahanan keamanan siber di ASEAN (*Association of Southeast Asian Nations*).

### **1.3.2 Tujuan Penelitian**

Adapun tujuan penelitian mengenai dampak perkembangan teknologi *blockchain* terhadap keamanan siber di ASEAN, yaitu :

1. Mengetahui bagaimana konsep implementasi teknologi *blockchain* terhadap keamanan siber dalam proses transformasi digital di ASEAN.

2. Mengetahui bagaimana mitigasi penerapan teknologi blockchain terhadap keamanan siber di ASEAN.
3. Mengetahui prospek teknologi blockchain terhadap keamanan siber dalam proses transformasi digital ASEAN.
4. Mengetahui apa saja kendala dalam penerapan teknologi *blockchain* terhadap keamanan siber dalam proses transformasi digital di ASEAN.

## **1.4 Kegunaan Penelitian**

### **1.4.1 Kegunaan Teoritis**

Secara teoritis, peneliti berharap bahwa hasil penelitian ini dapat menjadi referensi baru dan menambah perspektif bahwa Ilmu Hubungan Internasional merupakan sebuah kajian ilmu yang kaya dengan cakupannya yang luas. Dalam penelitian ini terkait perkembangan teknologi, menyelam lebih jauh mengenai dampak dan prospek teknologi *blockchain* terhadap keamanan siber di ASEAN dalam upaya pertahanan keamanan pada aktivitas di dimensi baru yaitu ruang siber.

### **1.4.2 Kegunaan Praktis**

Secara praktis, penelitian ini diharapkan dapat menambah wawasan dan sebagai khazanah keilmuan bagi peneliti sendiri, pembaca dan pengkaji khususnya terkait hubungan internasional mengenai dampak perkembangan teknologi *blockchain* terhadap keamanan siber di ASEAN. Diharapkan penelitian ini juga dapat berguna bagi penelitian kedepannya.