# BAB I : PENDAHULUAN

## 1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, keamanan cyber menjadi salah satu aspek kritis yang harus diperhatikan dengan serius. Ancaman keamanan seperti serangan peretasan, pencurian identitas, dan manipulasi data semakin kompleks dan sering terjadi. Oleh karena itu, pengembangan solusi keamanan yang inovatif dan efektif menjadi suatu kebutuhan mendesak.

Salah satu teknologi yang muncul sebagai pionir dalam memberikan solusi keamanan yang potensial adalah Blockchain. Blockchain merupakan konsep teknologi yang pertama kali diperkenalkan melalui mata uang kripto, seperti Bitcoin. Namun, seiring waktu, manfaatnya telah meluas ke berbagai sektor, termasuk keamanan cyber.

Blockchain, sebagai inovasi teknologi yang merevolusi konsep keamanan cyber, membawa kontribusi yang signifikan dalam melindungi data dan sistem informasi. Dengan prinsip desentralisasi, setiap transaksi atau blok data disimpan di berbagai titik dalam jaringan, membuatnya sulit bagi peretas untuk mengakses atau memanipulasi informasi. Keutuhan data diperkuat oleh penggunaan kriptografi yang canggih dan keterkaitan setiap blok melalui fungsi hash, sehingga setiap perubahan dapat terdeteksi dengan cepat oleh seluruh jaringan. Selain itu, fitur smart contracts memungkinkan pelaksanaan otomatis kontrak tanpa intervensi pihak ketiga, mengurangi risiko kecurangan.

Dengan tingkat transparansi dan auditabilitas yang tinggi, Blockchain membantu memitigasi ancaman cyber dengan memberikan visibilitas penuh terhadap setiap transaksi. Meskipun tantangan masih ada, kemajuan terus-menerus dalam teknologi Blockchain menjanjikan perlindungan yang lebih kuat terhadap serangan cyber di masa depan.

## 1.2 Rumusan Masalah

1. Bagaimana tingkat skalabilitas Blockchain dapat mempengaruhi keamanan cyber, terutama ketika volume transaksi meningkat?
2. Apa tantangan terbesar terkait privasi dan anonimitas dalam implementasi Blockchain, dan bagaimana dapat memastikan keseimbangan antara privasi pengguna dan transparansi yang dibutuhkan?
3. Sejauh mana ketergantungan pada kunci pribadi dalam ekosistem Blockchain dapat menjadi potensi kerentanan keamanan, dan bagaimana pengelolaannya dapat ditingkatkan?
4. Apa saja potensi kerentanan keamanan yang mungkin muncul dalam smart contracts, dan bagaimana dapat memitigasi risiko yang terkait?
5. Sejauh mana kesulitan implementasi Blockchain dapat menghambat adopsi dalam sektor keamanan cyber, terutama dalam hal integrasi dengan sistem yang sudah ada?
6. Bagaimana tantangan regulasi dan kepatuhan dapat mempengaruhi implementasi Blockchain untuk keamanan cyber di berbagai yurisdiksi?
7. Bagaimana risiko terkait konsensus algoritma dan potensi serangan mayoritas 51% dapat diatasi untuk memastikan integritas jaringan Blockchain?

## 1.3 Tujuan Penelitian

1. Mengembangkan Solusi Skalabilitas Blockchain

Meneliti dan mengembangkan solusi untuk meningkatkan skalabilitas Blockchain, sehingga dapat menangani volume transaksi yang lebih tinggi tanpa mengorbankan keamanan.

1. Mengatasi Tantangan Privasi dan Anonimitas

Meneliti metode atau protokol baru untuk meningkatkan privasi pengguna dalam konteks Blockchain tanpa mengorbankan transparansi yang diperlukan oleh regulator.

1. Peningkatan Manajemen Kunci Pribadi

Mengidentifikasi dan mengembangkan solusi terbaik untuk meningkatkan manajemen kunci pribadi dalam ekosistem Blockchain, termasuk teknologi otentikasi ganda dan penyimpanan yang aman.

1. Pengembangan Smart Contracts yang Aman

Meneliti keamanan smart contracts dan mengembangkan metode untuk mendeteksi serta mencegah potensi kerentanan atau serangan terhadap kontrak pintar.

1. Optimalisasi Implementasi Blockchain

Mengevaluasi dan mengoptimalkan proses implementasi Blockchain agar lebih mudah diintegrasikan dengan sistem yang sudah ada dalam konteks keamanan cyber.

1. Kajian Regulasi dan Kepatuhan

Meneliti kerangka regulasi yang ada dan mengusulkan kerangka regulasi yang mendukung pertumbuhan dan adopsi teknologi Blockchain dalam konteks keamanan cyber.

1. Keamanan Konsensus dan Ancaman Mayoritas 51%

Mempelajari metode pengamatan dan perlindungan terhadap risiko konsensus, khususnya potensi serangan mayoritas 51%, untuk menjaga integritas jaringan Blockchain.

# BAB II : PEMBAHASAN