BAB 1
PENDAHULUAN

1.1 Latar Belakang

Transformasi digital yang berlangsung dalam beberapa tahun terakhir telah mendorong peningkatan signifikan dalam penggunaan sistem transaksi elektronik. Bersamaan dengan hal tersebut, risiko kejahatan siber juga mengalami peningkatan, baik dalam bentuk pencurian data, manipulasi informasi, maupun akses tidak sah terhadap sistem penyimpanan digital. Beberapa penelitian menunjukkan bahwa keamanan data menjadi faktor krusial dalam menjaga stabilitas dan kepercayaan terhadap sistem transaksi modern [1].

Dalam konteks pengamanan data, teknologi blockchain mulai banyak diperkenalkan sebagai alternatif terhadap sistem penyimpanan konvensional. Implementasi blockchain dinilai mampu meningkatkan transparansi dan memperkuat mekanisme validasi transaksi melalui pendekatan desentralisasi [2]. Di Indonesia, adopsi teknologi digital juga mendorong eksplorasi blockchain sebagai salah satu solusi untuk memperbaiki tata kelola dan perlindungan data dalam berbagai sektor [3].

Secara arsitektural, sistem penyimpanan data umumnya dibedakan menjadi dua model utama, yaitu pendekatan terpusat (centralized database) dan pendekatan terdistribusi (blockchain). Perbedaan mendasar antara keduanya terletak pada struktur kontrol data, metode verifikasi transaksi, serta model pengamanan informasi yang diterapkan [4].

Database konvensional yang bersifat terpusat masih banyak digunakan karena efisiensinya dalam pengolahan data dan kemudahan manajemen sistem. Namun, sejumlah studi mengungkapkan bahwa model ini memiliki potensi kerentanan apabila terjadi serangan terhadap server utama atau penyalahgunaan hak akses oleh pihak internal [5]. Tantangan tersebut mendorong perlunya inovasi dalam sistem penyimpanan yang mampu meningkatkan integritas serta ketahanan data terhadap manipulasi.

Sebagai respons terhadap kebutuhan tersebut, konsep verifiable database dan sistem berbasis blockchain dikembangkan untuk memberikan jaminan keaslian serta konsistensi data [6]. Blockchain menerapkan mekanisme kriptografi dan konsensus jaringan yang memungkinkan data yang telah dicatat menjadi sulit untuk diubah tanpa persetujuan kolektif. Pendekatan ini mengintegrasikan prinsip confidentiality, integrity, dan availability dalam satu sistem yang

terdistribusi [7].

Selain itu, penerapan blockchain dalam lingkungan komputasi awan juga telah diteliti sebagai upaya meningkatkan keamanan serta ketahanan sistem terhadap gangguan dan serangan siber [8]. Penelitian lain membahas berbagai bentuk ancaman pada jaringan blockchain serta metode deteksi dan mitigasinya [9], termasuk kajian komprehensif mengenai manajemen keamanan sistem informasi berbasis blockchain [10].

Berdasarkan berbagai temuan tersebut, terlihat bahwa blockchain dan database konvensional memiliki karakteristik keamanan yang berbeda, baik dari sisi arsitektur maupun mekanisme perlindungan data. Oleh karena itu, diperlukan kajian komparatif berbasis literatur ilmiah untuk menganalisis secara sistematis perbedaan serta keunggulan masing-masing teknologi dalam mendukung keamanan transaksi digital.

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) dengan protokol PRISMA guna memastikan proses identifikasi, seleksi, dan analisis literatur dilakukan secara sistematis, transparan, dan dapat direplikasi.

1.2 Rumusan Masalah

Penelitian ini berfokus pada analisis perbandingan tingkat keamanan antara teknologi blockchain dan database konvensional dalam konteks transaksi digital. Perkembangan pesat sistem keuangan berbasis digital menempatkan aspek perlindungan dan integritas data sebagai isu yang sangat krusial.

Model database konvensional yang bersifat terpusat masih banyak digunakan dalam berbagai sistem informasi, namun pendekatan ini memiliki potensi risiko, seperti serangan siber terhadap server utama, penyalahgunaan hak akses, serta kemungkinan terjadinya manipulasi atau kebocoran data. Di sisi lain, blockchain menghadirkan pendekatan terdesentralisasi dengan mekanisme pencatatan transaksi yang terbuka dan terdistribusi, sehingga perubahan data tidak dapat dilakukan secara sepihak.

Meskipun menawarkan keunggulan dalam transparansi dan ketahanan terhadap manipulasi, blockchain juga memiliki tantangan, antara lain terkait efisiensi operasional, kebutuhan sumber daya, dan kompleksitas implementasi. Oleh sebab itu, diperlukan kajian yang komprehensif untuk mengevaluasi sejauh mana kedua teknologi tersebut mampu menjamin keamanan transaksi digital serta membandingkan performanya dari aspek keandalan sistem, transparansi, dan integritas data.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengkaji serta menjelaskan arsitektur dan mekanisme keamanan yang diterapkan pada blockchain dan database konvensional dalam mendukung keamanan transaksi digital.

Secara khusus, penelitian ini akan:

1. Mengidentifikasi komponen keamanan utama pada blockchain, termasuk penggunaan kriptografi, mekanisme konsensus, serta struktur data yang bersifat imutabel.
2. Menganalisis lapisan pengamanan pada database konvensional, seperti pengendalian akses, teknik enkripsi pada level aplikasi, serta proteksi jaringan.
3. Menyusun analisis komparatif berbasis sintesis literatur untuk menggambarkan karakteristik, kelebihan, dan keterbatasan masing-masing model keamanan, baik yang bersifat terpusat maupun terdistribusi.

Melalui pendekatan tersebut, penelitian ini diharapkan mampu memberikan pemahaman yang lebih sistematis mengenai perbedaan strategi pengamanan data pada kedua teknologi tersebut.

1.4 Manfaat Penelitian

Penelitian ini diharapkan memberikan kontribusi sebagai berikut:

1. **Kontribusi Akademik**
   Hasil penelitian ini dapat memperkaya kajian ilmiah di bidang keamanan data dan sistem transaksi digital dengan menyajikan analisis komparatif antara blockchain dan database konvensional. Temuan yang diperoleh dapat menjadi referensi bagi peneliti selanjutnya dalam mengembangkan studi terkait teknologi penyimpanan data terdistribusi.
2. **Pertimbangan bagi Organisasi atau Perusahaan**
   Analisis yang dihasilkan dapat digunakan sebagai bahan evaluasi dalam menentukan sistem penyimpanan data yang sesuai dengan kebutuhan organisasi, khususnya dari segi keamanan, efisiensi, dan kemampuan sistem dalam menangani transaksi digital secara berkelanjutan.

3. **Sumber Pembelajaran Akademik**

   Penelitian ini dapat dimanfaatkan sebagai materi pembelajaran bagi mahasiswa maupun pengembang sistem informasi untuk memahami penerapan prinsip keamanan pada arsitektur penyimpanan data modern.
4. **Landasan Pengembangan Sistem Hybrid**

   Temuan penelitian ini juga dapat menjadi dasar konseptual bagi pengembangan model sistem yang mengintegrasikan keunggulan blockchain dan database konvensional guna menghasilkan solusi penyimpanan data yang lebih fleksibel, efisien, dan aman.

1.5 Batasan Masalah

Ruang lingkup penelitian ini dibatasi pada beberapa aspek berikut:

1. Penelitian ini difokuskan pada kajian keamanan dan integritas data dalam transaksi digital melalui perbandingan antara teknologi blockchain dan database konvensional. Analisis dilakukan menggunakan pendekatan *Systematic Literature Review* serta didukung oleh analisis bibliometrik untuk mengidentifikasi perbedaan karakteristik dan tingkat keamanan masing-masing sistem.
2. Data yang digunakan bersumber dari literatur sekunder yang telah terverifikasi, seperti artikel jurnal ilmiah, publikasi akademik, dan penelitian terdahulu yang membahas isu keamanan pada sistem blockchain maupun database konvensional.
3. Penelitian ini tidak mencakup implementasi teknis maupun pengujian sistem secara langsung. Seluruh pembahasan didasarkan pada analisis konseptual serta sintesis temuan empiris dari studi sebelumnya untuk menilai efektivitas dan efisiensi kedua teknologi tersebut.
4. Pembahasan mengenai blockchain dibatasi pada aspek mekanisme keamanan, penggunaan kriptografi, serta konsep desentralisasi jaringan. Sementara itu, analisis terhadap database konvensional difokuskan pada pengelolaan data terpusat dan potensi risiko keamanan siber, tanpa membahas fitur lanjutan seperti *smart contract* atau tokenisasi.
5. Proses identifikasi dan seleksi literatur dilakukan dengan protokol PRISMA, dengan sumber utama berasal dari basis data Scopus yang diakses melalui aplikasi Publish or Perish dalam rentang publikasi tahun 2019–2024.

1.6 Keterbaruan

Penelitian ini menawarkan pendekatan komparatif yang disusun secara sistematis melalui metode *Systematic Literature Review* berbasis kerangka PRISMA terhadap publikasi ilmiah terindeks Scopus periode 2019–2024.

Berbeda dari penelitian terdahulu yang cenderung membahas blockchain dan database konvensional secara terpisah, studi ini secara khusus:

1. Mengidentifikasi dan membandingkan mekanisme keamanan inti pada blockchain, termasuk kriptografi, konsensus, dan sifat imutabilitas data.
2. Menganalisis lapisan pengamanan pada database konvensional, seperti kontrol akses, teknik enkripsi, dan manajemen sistem terpusat.
3. Mengkaji pola ancaman keamanan yang dominan pada kedua pendekatan penyimpanan data tersebut.
4. Mengeksplorasi peluang pengembangan model sistem hybrid berdasarkan sintesis hasil literatur.

Selain itu, penelitian ini memanfaatkan analisis bibliometrik dengan bantuan perangkat lunak VOSviewer untuk memetakan tren dan perkembangan riset terkait keamanan blockchain dan database dalam enam tahun terakhir, sehingga menghasilkan gambaran evolusi penelitian secara kuantitatif maupun kualitatif.