

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di era digital, aplikasi e-commerce telah menjadi salah satu pilar utama dalam ekonomi modern, dengan transaksi online yang terus meningkat setiap tahunnya. Di Indonesia, tren serupa juga terjadi dengan peningkatan signifikan jumlah pengguna e-commerce. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa pada tahun 2022, sekitar 77,02% masyarakat Indonesia terhubung dengan internet, dan sebagian besar di antaranya memanfaatkan layanan e-commerce untuk kebutuhan sehari-hari [1]. Jumlah transaksi e-commerce di Indonesia pada tahun 2023 diperkirakan mencapai lebih dari 55 miliar USD, yang juga sejalan dengan peningkatan data pengguna yang harus dikelola dan diamankan oleh platform tersebut [2].

Pertumbuhan saat ini juga membawa risiko besar terhadap keamanan data pengguna. Data-data pribadi, seperti informasi identitas, riwayat transaksi, dan rincian pembayaran menjadi target utama serangan siber. Menurut Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, telah terjadi lebih dari 349 juta serangan siber di Indonesia yang sebagian besar menyasar sistem e-commerce dan platform online lainnya [3]. Salah satu jenis ancaman yang sering terjadi adalah data breach, yaitu ketika data pengguna bocor atau dicuri oleh pihak yang tidak bertanggung jawab. Insiden seperti ini berpotensi merusak reputasi perusahaan ecommerce dan menurunkan kepercayaan pengguna terhadap platform digital. Di Indonesia, kasus kebocoran data pengguna pada layanan digital semakin sering terjadi serta berdampak pada hilangnya kepercayaan konsumen dan kerugian finansial. Berkaca pada peristiwa kebocoran data pengguna diberbagai platform, di mana data sensitif seperti nama, alamat, nomor telepon hingga data finansial terekspos, masyarakat semakin khawatir akan privasi mereka saat bertransaksi online. Kekhawatiran ini dikarenakan insiden kebocoran data secara langsung berpotensi menimbulkan kerugian besar bagi pengguna. Di sektor e-commerce, misalnya kerugian yang timbul akibat serangan siber dan pencurian data diestimasi mencapai 3 miliar USD per tahun dikawasan Asia Tenggara, yang berdampak pada kepercayaan

pengguna dan berkelanjutan bisnis digital [4]. Banyaknya data pribadi yang harus dikelola oleh platform e-commerce juga meningkatkan tantangan dalam menjamin keamanan data tersebut. Menurut data dari Bank Indonesia (2023), di Indonesia sekitar 210 juta transaksi e-commerce dilakukan setiap bulan, dengan lebih dari 60% transaksi menggunakan metode pembayaran digital. Tingginya volume transaksi digital ini menimbulkan kebutuhan akan sistem keamanan data yang tidak hanya mampu melindungi kerahasiaan, tetapi juga memastikan integritas data dalam proses pengolahan dan penyimpanan.

Untuk mengatasi masalah ini, banyak penelitian dan inovasi teknologi telah dikembangkan gunanya untuk meningkatkan keamanan data pengguna dalam aplikasi e-commerce. Salah satu pendekatan yang mulai banyak diterapkan adalah teknologi Blockchain. Teknologi Blockchain menawarkan solusi yang sangat dibutuhkan dalam permasalahan ini karena sifatnya yang terdesentralisasi, sulit untuk dimanipulasi dan mampu menyediakan audit trail yang jelas untuk setiap transaksi. Blockchain dengan fitur keamanan kriptografi dan struktur decentralized ledger-nya, dinilai sangat efektif dalam menjaga integritas dan kerahasiaan data. [5] Sebuah studi menyatakan bahwa blockchain memiliki potensi besar dalam menciptakan sistem yang lebih transparan dan aman karena setiap transaksi atau perubahan data dicatat secara permanen dan dapat diverifikasi. Dalam konteks e-commerce, blockchain dapat digunakan untuk membangun sistem keamanan yang terdesentralisasi, di mana data pengguna tersimpan dalam blok blok yang sulit dimodifikasi atau diakses tanpa izin.

Penelitian [6] mengungkapkan bahwa blockchain memiliki potensi dalam meningkatkan data integrity dan data availability dalam aplikasi e-commerce. Penelitian ini menunjukkan bahwa dengan menggunakan algoritma konsensus seperti proof-of-work atau proof-of-stake, blockchain mampu memastikan setiap transaksi yang tercatat telah diverifikasi oleh seluruh jaringan. Hal ini dapat mengurangi resiko pencurian data atau manipulasi informasi. penelitian yang lebih aplikatif terkait penggunaan blockchain dalam sistem e-commerce juga telah dilakukan oleh [7]. Dalam penelitian ini, mereka merancang sebuah prototype sistem keamanan data berbasis blockchain yang terintegrasi pada platform e-commerce. Hasil dari penelitian menunjukkan bahwa sistem tersebut mampu meningkatkan kecepatan verifikasi transaksi hingga 25% lebih cepat dibandingkan dengan sistem tradisional, serta

meningkatkan efisiensi dalam pengolahan data pengguna.

Meskipun blockchain memiliki berbagai kelebihan, ada beberapa tantangan dalam penerapannya di platform e-commerce. Tantangan ini meliputi masalah skalabilitas, integrasi dengan sistem yang sudah ada, serta penggunaan sumber daya yang cukup besar untuk memelihara jaringan blockchain [8]. Teknologi ini juga memerlukan kemampuan komputasi yang tinggi untuk menjalankan proses enkripsi dan verifikasi, yang dapat mempengaruhi kecepatan transaksi jika tidak didesain dengan baik. Oleh karena itu, diperlukan penelitian lebih lanjut untuk merancang protokol keamanan data berbasis blockchain yang dapat mengatasi tantangan ini tanpa mengorbankan performa dan kenyamanan pengguna. Penelitian ini tidak hanya bertujuan untuk memperkenalkan blockchain sebagai solusi, tetapi juga mendesain protokol keamanan yang dapat mengatasi keterbatasan-keterbatasan tersebut.

Melihat peluang tersebut, penelitian ini penting dilakukan untuk mengembangkan **Desain Protokol Keamanan Data Berbasis Blockchain pada Pengolahan Data Pengguna dalam Aplikasi E-Commerce**. Desain ini diharapkan dapat memastikan keamanan data pengguna melalui penggunaan teknologi blockchain, sekaligus menawarkan solusi terhadap tantangan skalabilitas dan efisiensi yang ada. Dengan adanya desain protokol ini, diharapkan platform e-commerce dapat mengurangi resiko keamanan, meningkatkan kepercayaan pengguna, serta memberikan perlindungan yang baik terhadap data sensitif yang dikelola dalam setiap transaksi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas maka didapatkan rumusan masalah pada penelitian ini yaitu bagaimana desain protokol keamanan data berbasis blockchain dapat diterapkan dalam pengolahan data pengguna di aplikasi e-commerce?

1.3 Tujuan Penelitian

Adapun tujuan penelitian yang akan dicapai adalah sebagai berikut :

1. Mendeskripsikan desain protokol keamanan data berbasis blockchain untuk pengolahan data pengguna dalam aplikasi e-commerce.
2. Menganalisis kelebihan dan kekurangan penerapan teknologi blockchain

dalam meningkatkan keamanan data pengguna dalam aplikasi e-commerce.

1.4 Manfaat Penelitian

Adapun manfaat penelitian sebagai berikut:

1. Mengetahui desain protokol keamanan data berbasis blockchain untuk pengolahan data pengguna dalam aplikasi e-commerce.
2. Mengetahui kelebihan dan kekurangan penerapan teknologi blockchain dalam meningkatkan keamanan data pengguna dalam aplikasi e-commerce.

1.5 Ruang Lingkup Penelitian

Agar pembahasan dalam penelitian ini tidak meluas, maka dibuat batasan sebagai berikut:

1. Penelitian ini menggunakan blockchain sebagai metode penyelesaian masalah.
2. Penelitian ini menghasilkan desain protokol keamanan data berbasis blockchain.

1.6 Keterbaruan

- 1) Penelitian yang dilakukan oleh Azaria et al tahun 2016 tentang blockchain mulai berkembang menuju diversifikasi aplikasi di luar domain keuangan. Peneliti dan praktisi teknologi mulai mengeksplorasi potensi blockchain untuk digunakan dalam berbagai sektor, termasuk logistik, perawatan kesehatan, dan manajemen identitas digital. Blockchain digunakan untuk menjawab sebuah permasalahan mendasar dalam keamanan data, seperti keaslian, privasi, dan transparansi.
- 2) Penelitian dilanjutkan oleh mingxiao pada tahun 2027 yang memperkenalkan algoritma konsensus baru seperti Proof of Stake (PoS) dan Practical Byzantine Fault Tolerance (PBFT), yang lebih hemat energi dan lebih cocok untuk aplikasi di luar keuangan.
- 3) Penelitian yang dilakukan oleh Lit et al pada tahun 2018, pendekatan berbasis pembelajaran mesin (machine learning) dan analisis data besar (big data analytics) telah diterapkan untuk mendeteksi pola-pola anomali dalam transaksi blockchain, sehingga mampu meningkatkan deteksi dini terhadap potensi serangan siber .
- 4) Pada tahun 2019 hingga 2020, fokus penelitian bergeser pada peningkatan privasi

dan efisiensi blockchain, serta pemanfaatan analitik data yang lebih maju. Salah satu perkembangan signifikan adalah integrasi teknologi zero-knowledge proofs (ZKP), yang memungkinkan validasi transaksi tanpa mengungkapkan informasi sensitif yang di kemukakan oleh Ben-Sasson et al pada tahun Wang et al di tahun 2020.

- 5) Sejak tahun 2021 hingga saat ini, penelitian blockchain dan data science semakin berfokus pada integrasi dengan teknologi canggih lainnya, seperti kecerdasan buatan (AI), Internet of Things (IoT), dan komputasi awan. Blockchain digunakan sebagai kerangka kerja untuk mengelola data dalam sistem IoT, di mana keamanan komunikasi antar perangkat menjadi tantangan utama. Kombinasi blockchain dengan kontrak pintar (smart contracts) memungkinkan otomatisasi proses yang aman, seperti dalam pengelolaan rantai pasok atau sistem pembayaran lintas negara yang di kemukakan oleh Xu et al pada tahun 2022. Selain itu, data science memainkan peran penting dalam menganalisis data yang dihasilkan oleh perangkat IoT, membantu meningkatkan efisiensi operasional dan mendeteksi potensi ancaman keamanan.

Oleh karena itu, penelitian di bidang ini akan terus berkembang untuk menghadirkan solusi yang tidak hanya inovatif tetapi juga praktis dalam implementasi. Secara keseluruhan, penelitian terdahulu menunjukkan evolusi yang konsisten dalam mengatasi tantangan keamanan data melalui pendekatan berbasis blockchain dan data science. Mulai dari pengembangan algoritma konsensus yang lebih efisien hingga integrasi analitik data yang canggih, pendekatan ini terus menjadi solusi utama dalam menghadapi kebutuhan era digital. Referensi akademik dan studi kasus dalam berbagai bidang menegaskan bahwa kombinasi blockchain dan data science memiliki potensi besar untuk memberikan solusi keamanan yang andal, transparan, dan berbasis data, meskipun masih membutuhkan penelitian lebih lanjut untuk menjawab tantangan yang terus berkembang.