BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dokumen merupakan aset yang memiliki nilai penting serta berperan sebagai sumber informasi yang dibutuhkan oleh berbagai pihak baik individu, instansi, organisasi, maupun negara[1]. Dokumen elektronik muncul sebagai komponen dari layanan publik yang berperan menggantikan dokumen berbasis kertas dengan karakteristik yang lebih fleksibel, mudah diakses melalui pencarian, efisien dalam pemanfaatan ruang penyimpanan, mendukung pengarsipan digital, dan memfasilitasi proses pemindahan dokumen[2]. Pada saat pertukaran dokumen secara digital, sering terjadi perubahan, pemalsuan, dan manipulasi data selama proses pengiriman dokumen dari si pengirim ke si penerima baik karena serangan pihak ketiga maupun karena kelemahan pada sistem penyimpanan yang terpusat[3].

Di era digital yang terus maju, teknologi *blockchain* hadir sebagai solusi inovatif yang menawarkan sistem pencatatan terdistribusi dengan tingkat keamanan, transparansi, dan integritas data yang tinggi[4]. Dalam penerapannya, algoritma tanda tangan digital berperan penting dalam menjamin keaslian identitas pengirim dan memastikan integritas dokumen yang dikirimkan. Setiap dokumen yang akan disimpan ke dalam *blockchain* terlebih dahulu diberi tanda tangan digital yang bersifat unik untuk membuktikan bahwa dokumen tersebut benar berasal dari pemilik yang sah[5]. Salah satu algoritma tanda tangan digital modern yang efisien dan aman adalah EdDSA (*Edwards-curve Digital Signature Algorithm*). Algoritma ini menggunakan kurva eliptik (*Edwards Curve*) dan memanfaatkan transformasi Fiat–Shamir untuk menghasilkan tanda tangan deterministik yang tahan terhadap pemalsuan pesan dan serangan substitusi kunci[6].

Dalam Teknologi *blockchain*, terdapat sebuah mekanisme konsensus yang digunakan untuk mencapai kesepakatan bersama antar node di dalam jaringan. *Proof of Work* (PoW) merupakan salah satu mekanisme konsensus dalam sistem *blockchain* dengan melibatkan perhitungan matematis yang kompleks sebagai bentuk pembuktian kerja komputasi, dimana proses tersebut dilakukan oleh pengguna yang berperan sebagai *miner* untuk memastikan keabsahan dan integritas data sebelum dicatat ke

dalam blok baru[7]. Beberapa penelitian sebelumnya telah menerapkan mekanisme *Proof of Work* (PoW) dalam berbagai implementasi sistem berbasis *blockchain* untuk menjamin integritas dan keabsahan data. Sebagai contoh, penelitian yang dilakukan oleh Annisya dan Emy Haryatmi[8] menunjukkan bahwa *penerapan Proof-of-Work* (PoW) mampu menjaga keaslian data transaksi pada rantai pasok produk dengan menciptakan catatan yang sulit dimanipulasi secara sepihak. Sementara itu, penelitian yang dilakukan oleh Putra dkk[9] menegaskan bahwa penerapan mekanisme *Proof-of-Work* (PoW) pada sistem berbasis *blockchain* mampu meningkatkan keamanan dan integritas data dalam lingkungan pemerintahan, khususnya pada sistem pelatihan kerja di Dinas Tenaga Kerja Kota Surakarta. Meskipun penerapan mekanisme *Proof-of-Work* (PoW) pada *blockchain* telah banyak digunakan, namun masih terbatas penelitian yang mengintegrasikannya dengan algoritma tanda tangan digital modern EdDSA.

Dari permasalahan yang telah dijelaskan, tim peneliti berupaya mengisi celah penelitian yang ada dengan mengangkat judul **"Penerapan Algoritma EdDSA Dalam Menjamin Keamanan dan Keaslian Dokumen Elektronik Berbasis Konsensus *Proof of Work*."** Melalui kombinasi antara algoritma tanda tangan digital EdDSA dan mekanisme konsensus *Proof-of-Work*, sistem yang dikembangkan diharapkan mampu menjaga keaslian, integritas, dan keamanan dokumen elektronik mulai dari proses pengiriman hingga penyimpanan di jaringan *blockchain*. Dengan demikian, penerima dokumen dapat memverifikasi keabsahan dokumen secara kriptografis dan memastikan bahwa dokumen yang diterima tidak mengalami perubahan dan manipulasi selama proses transmisi data berlangsung.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang yang telah diuraikan, penelitian ini akan menjawab beberapa permasalahan yang timbul mengenai penerapan algoritma EdDSA pada dokumen elektronik berbasis konsensus *Proof of Work*. Permasalahan pertama yang muncul yaitu mengukur sejauh mana tingkat efektivitas penggunaan algoritma tanda tangan digital EdDSA pada dokumen elektronik untuk menjamin keamanan dan keaslian dokumen elektronik selama proses transmisi berlangsung. Permasalahan kedua adalah bagaimana penerapan mekanisme konsensus *Proof of Work* berperan

dalam menjaga keamanan dan penyimpanan dokumen elektronik di jaringan *blockhain*.

1.3 Tujuan dan Manfaat

1.3.1 Tujuan

Tujuan dari penelitian ini antara lain:

1. Mengimplementasikan algoritma tanda tangan digital EdDSA pada sistem berbasis *blockchain* untuk pengamanan dokumen elektronik secara terdistribusi.
2. Menganalisis kemampuan algoritma EdDSA dalam menjamin keaslian integritas dokumen elektronik melalui proses penandatanganan dan verifikasi digital.
3. Mengevaluasi penerapan mekanisme konsensus *Proof of Work* dalam proses validasi dan penyimpanan dokumen pada jaringan *blockchain.*

1.3.2 Manfaat

Manfaat dari penelitian ini antara lain:

1. Memberikan kontribusi terhadap pengembangan sistem di bidang keamanan data digital dan teknologi *blockchain*, khususnya dalam penerapan algoritma tanda tangan digital EdDSA untuk menjamin keamanan dan keaslian dokumen elektronik.
2. Meningkatkan kepercayaan pengguna terhadap dokumen elektronik yang terhindar dari risiko manipulasi maupun penyalahgunaan identitas. Hal ini dikarenakan teknologi *blockchain* bekerja dengan mekanisme *peer-to-peer* (P2P) yang bersifat terdesentralisasi.
3. Menjadi dasar pengembangan aplikasi sistem keamanan dokumen elektronik yang efisien, terdesentralisasi, dan tahan terhadap serangan oleh pihak ketiga.

1.4 Batasan Masalah

Pada penelitian yang dilakukan, penelitian ini memiliki beberapa batasan masalah sebagai berikut:

1. Penelitian ini secara khusus berfokus pada penerapan teknologi *blockchain* untuk menjaga keamanan dan keaslian dokumen elektronik, tidak mencakup

pembahasan mengenai jenis dokumen lain yang berbentuk non-elektronik atau fisik.

2. Pengembangan sistem blockchain hanya dilakukan sebatas simulasi pada jaringan lokal di satu komputer menggunakan empat node yang berjalan secara bersamaan pada port yang berbeda.
3. Sistem tidak membahas mekanisme reward atau insentif ekonomi bagi node yang berhasil memenangkan proses mining, karena fokus penelitian adalah pada demonstrasi mekanisme konsensus dan keamanan data, bukan pada aspek ekonomi jaringan blockchain
4. Sistem hanya mendukung penyimpanan satu dokumen per blok, berbeda dengan implementasi blockchain pada umumnya yang dapat menampung banyak transaksi dalam satu blok.
5. Penelitian yang dilakukan akan menggunakan algoritma tanda tangan digital EdDSA (*Edwards-curve Digital Signature Algorithm*) tanpa melakukan integrasi atau penggabungan dengan algoritma tanda tangan digital lainnya, seperti ECDSA, RSA, maupun DSA.
6. Pendistribusian dokumen elektronik pada jaringan *blockchain* menggunakan konsensus terdistribusi *Proof of Work.*

1.5 Keterbaruan

1. Menurut Moumita Das, Xingyu Tao, Yuhan Liu, Jack C.P Cheng (2022) dalam penelitian yang berjudul "*A Blockchain-based Integrated Document Management Framework for Construction Applications".* Penelitian ini mengembangkan sistem dengan teknologi *blockchain* terdesentralisasi untuk memfasilitasi keamanan dalam memanajemen proyek AEC. Penggunaan smart contract berbasis *blockchain* dikembangkan untuk mendukung manajemen dokumen pada proyek AEC seperti alur kerja persetujuan dokumen yang dapat disesuaikan, manajemen versi dan pencatatan siklus hidup dokumen yang dicatat secara permanen melalui penerapan teknologi *blockchain* terdistribusi[10].
2. Menurut Cheysha Restu Nabila, Rissal Efendi (2024) dalam penelitian yang berjudul "*Integrasi Blockchain dan Keamanan Data untuk Meningkatkan Efisiensi dan Transparansi Sistem Logistik Global".* Penelitian ini

menggunakan pendekatan tinjauan literatur dengan menganalisis studi-studi relevan tentang penerapan *blockchain* dan keamanan data dalam logistik global. Hasil penelitian ini menunjukkan bahwa integrasi *blockchain* dalam sistem logistik global dapat memfasilitasi rantai pasok yang lebih efisien dan transparansi, validasi real-time, dan pemantauan aktivitas logistik yang lebih baik. Keamanan data yang terinkripsi dapat mengurangi risiko keamanan dan penipuan serta memberikan perlindungan lebih baik terhadap serangan siber dan manipulasi data[11].

3. Menurut Juniar hutagalung, Puji Sari Ramadhan, Sarah Juliana Sihombing (2023) dalam penelitian yang berjudul "*Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) Pada Digital Signature*". Penelitian ini menggunakan metode Secure Hash Algorithm (SHA-256) dan River Shamir Adleman (RSA). Dengan menggunakan sistem otentikasi berbasis web, pengguna dapat memastikan bahwa dokumen yang telah ditandatangani atau dibubuhi dengan kode QR membantu menjaga keaslian dokumen agar orang lain tidak dapat menyalinnya. Untuk mencegah pemalsuan surat, integritas data, dan keabsahan data, isi dokumen dilindungi sandi menggunakan algoritma kriptografi SHA-256 dan RSA[12].
4. Menurut Andi, Charles Juliandy, Robert, dan Octora Pribadi (2022) dalam penelitian berjudul "*Securing Medical Records of Covid-19 Patients using Elliptic Curve Digital Signature Algorithm (ECDSA) in Blockchain*". Penelitian ini mengusulkan model baru yang memadukan teknologi *blockchain* dan tanda tangan digital ECDSA berbasis konsensus *Proof of Work* (PoW) untuk meningkatkan keamanan rekam medis pasien COVID-19. Penelitian ini menunjukkan bahwa ECDSA efektif melindungi rekam medis dari akses tidak sah, sementara itu *blockchain* berhasil mencegah perubahan atau manipulasi data karena sifatnya yang tidak dapat diubah[13]