BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

2.1.1 *Blockchain*

Blockchain merupakan teknologi penyimpanan data terdistribusi yang terdiri atas rangkaian blok yang saling terhubung menggunakan algoritma kriptografi. Setiap blok memuat *hash* dari blok sebelumnya, data transaksi, dan *timestamp*, sehingga membentuk rantai data yang sulit diubah dan dipalsukan (Chandan et al., 2024).

Blockchain memiliki sejumlah fitur utama yang membedakannya dari sistem basis data konvensional. Karakteristik tersebut meliputi desentralisasi, transparansi, *immutability*, dan keamanan. Konsep desentralisasi mengacu pada distribusi *Blockchain* ke berbagai *node* dalam jaringan yang saling berkomunikasi untuk melakukan verifikasi transaksi, tanpa bergantung pada satu server pusat (Tripathi et al., 2023). Transparansi pada *Blockchain* memungkinkan seluruh peserta jaringan untuk melihat transaksi yang telah divalidasi. Setiap blok yang dimasukkan ke dalam rantai bersifat publik dan hanya dapat diubah melalui mekanisme konsensus mayoritas *node* (Tripathi et al., 2023). Menurut (Tripathi et al., 2023) fitur ini meningkatkan kepercayaan antar pengguna karena setiap transaksi terekam secara permanen dalam buku besar digital yang dapat diakses oleh siapa pun untuk keperluan verifikasi.

Karakteristik penting lainnya dari *Blockchain* adalah *immutability* atau sifat ketidakberubahan data. Setiap blok dalam *Blockchain* menyimpan *hash* dari blok sebelumnya, *timestamp*, serta data transaksi yang diamankan menggunakan

algoritma kriptografi. Sekecil apa pun perubahan pada data akan menyebabkan perubahan pada nilai *hash*, sehingga upaya manipulasi data dapat segera terdeteksi (Tripathi et al., 2023). Transaksi yang telah divalidasi tidak dapat diubah atau dihapus, sehingga sifat *immutability* menjadikan *Blockchain* aman dan tahan terhadap pemalsuan data.

(Tripathi et al., 2023) Mengklasifikasikan *Blockchain* ke dalam dua kategori utama, yaitu *public Blockchain* dan *private Blockchain*. *Public Blockchain* bersifat terbuka dan dapat diakses oleh siapa pun, seperti jaringan *Bitcoin* dan *Ethereum*. *Private Blockchain* bersifat tertutup dan hanya dapat diakses oleh entitas tertentu yang memiliki izin, serta umumnya digunakan dalam lingkungan korporasi untuk mendukung efisiensi operasional internal.

Blockchain dapat didefinisikan sebagai teknologi yang menggabungkan desentralisasi, transparansi, *immutability*, dan keamanan untuk membangun sistem penyimpanan data yang terdistribusi, aman, dan sulit dimanipulasi. Kombinasi keempat karakteristik tersebut menjadikan *Blockchain* relevan untuk berbagai aplikasi modern, termasuk verifikasi ijazah digital yang menuntut tingkat keandalan dan autentisitas data yang tinggi.

2.1.2 *Smart Contract*

Smart contract merupakan program digital yang dijalankan secara otomatis di atas jaringan *Blockchain* dan mengeksekusi perjanjian ketika kondisi tertentu terpenuhi (Baihaqsani et al., 2024). (Taherdoost, 2023) menjelaskan bahwa teknologi ini mengubah konsep kontrak konvensional dengan memasukkan logika pelaksanaan ke dalam kode yang berjalan secara terdesentralisasi, sehingga menghilangkan kebutuhan untuk bergantung pada pihak ketiga sebagai perantara.

Dalam praktiknya, *smart contract* dikembangkan pada platform *Blockchain*, seperti *Ethereum*, kemudian dideploy sehingga seluruh *node* dalam jaringan dapat mengeksekusi dan memverifikasi kode tersebut secara kolektif (Alshahrani et al., 2023).

Dalam penelitian ini, *smart contract* merupakan komponen penting dalam sistem verifikasi ijazah yang berfungsi untuk mencegah pemalsuan dokumen akademik. Dokumen ijazah dicatat, divalidasi, dan diverifikasi secara otomatis melalui logika yang tertanam dalam *smart contract* pada jaringan *Blockchain*. *Smart contract* memastikan bahwa data yang telah diunggah dan diverifikasi oleh institusi pendidikan tidak dapat diubah oleh pihak lain dengan menyimpan representasi *hash* dari dokumen tersebut. Proses ini memungkinkan pengguna melakukan verifikasi keaslian ijazah dengan memeriksa catatan transaksi pada *Blockchain* tanpa bergantung pada lembaga pusat, serta mendukung mekanisme pencabutan (*revocation*) apabila terjadi pembatalan status akademik (Leka & Selimi, 2021). *Smart contract* berperan sebagai komponen utama dalam menjamin integritas, transparansi, dan efisiensi sistem verifikasi ijazah.

2.1.3 Verifikasi Ijazah Digital

Verifikasi ijazah digital bertujuan untuk memastikan bahwa dokumen akademik yang ditunjukkan oleh pemiliknya merupakan dokumen asli yang dikeluarkan oleh institusi yang sah dan belum mengalami perubahan (Rustemi et al., 2023). Metode awal verifikasi digital umumnya hanya mencocokkan dokumen dengan basis data terpusat, yang rentan terhadap manipulasi serta menimbulkan ketergantungan pada otoritas penerbit, seperti direktorat pendidikan tinggi, dan

menjadi kurang efektif apabila basis data tersebut tidak dapat diakses oleh pihak ketiga (Rustemi et al., 2023).

Teknologi *Blockchain* telah diusulkan sebagai salah satu solusi untuk meningkatkan keandalan sistem verifikasi (Rustemi et al., 2023). Hasil survei literatur menunjukkan bahwa sistem berbasis *Blockchain* mampu menyediakan proses verifikasi yang lebih cepat, transparan, dan independen dari otoritas pusat, karena setiap kredensial akademik dicatat secara permanen dan diamankan secara kriptografis dalam jaringan terdesentralisasi.

Penggunaan teknologi *Blockchain* dalam verifikasi ijazah digital tidak hanya menjamin integritas data, tetapi juga meningkatkan efisiensi, keandalan, serta kepercayaan para pemangku kepentingan terhadap sistem verifikasi akademik yang bersifat terbuka dan terdokumentasi secara kriptografis.

2.1.4 Algoritma Konsensus *Blockchain*

Teknologi *Blockchain* menggunakan protokol yang dikenal sebagai mekanisme konsensus untuk memungkinkan seluruh peserta dalam jaringan terdistribusi mencapai kesepakatan mengenai status buku besar (*ledger*) tanpa bergantung pada otoritas sentral. Mekanisme ini berperan dalam mencegah konflik data, manipulasi, serta berbagai ancaman keamanan, seperti *double-spending* dan serangan lainny (Yakubu et al., 2024). Mekanisme konsensus memegang peran krusial dalam menjamin keamanan, desentralisasi, dan ketahanan jaringan, serta memengaruhi performa sistem, konsumsi energi, dan skalabilitas berbagai implementasi *Blockchain*, termasuk sistem verifikasi ijazah digital (Yakubu et al., 2024).

Mekanisme konsensus memegang peran krusial dalam menentukan karakteristik utama jaringan *Blockchain*, termasuk tingkat keamanan, desentralisasi, latensi transaksi, konsumsi energi, dan skalabilitas sistem. Berbagai studi menunjukkan bahwa tidak terdapat satu mekanisme konsensus yang unggul untuk seluruh konteks aplikasi, karena setiap mekanisme memiliki *trade-off* yang berbeda dan perlu disesuaikan dengan kebutuhan sistem yang dikembangkan (Jiayi Wang & Wang, 2025; Yakubu et al., 2024). Sistem non-finansial, seperti verifikasi ijazah digital, lebih menekankan aspek kecepatan verifikasi, finalitas hasil (*finality*), serta efisiensi operasional dibandingkan mekanisme ekonomi berbasis token yang umum diterapkan pada jaringan *Blockchain* publik.

Tabel 2.1 menyajikan perbandingan beberapa algoritma konsensus *Blockchain* yang umum digunakan serta relevansinya dalam konteks penerapan pada sistem verifikasi ijazah digital.

Tabel II.1 Algoritma Konsensus

Algoritma Konsensus	Karakteristik Singkat	Mengapa Dipilih ?
Proof of Work (PoW)	Kemanan tinggi, berbasis komputasi intensif	Digunakan sebagai referensi awal karena menjamin integritas data, namun memiliki latensi tinggi dan konsumsi energi besar sehingga kurang efisien untuk sistem verifikasi dokumen non-finansial
Proof of Stake (PoS)	Konsumsi energi lebih rendah, berbasis kepemilikan aset	Memberikan efisiensi lebih baik dibanding PoW dan cocok untuk jaringan publik berskala besar, namun tetap bergantung pada mekanisme ekonomi token

Delegated Proof of Stake (DPoS)	Validator dipilih oleh pemegang token, *throughput* tinggi	Mendukung transaksi cepat dan latensi rendah, tetapi melibatkan mekanisme voting berbasis token yang kurang relevan untuk lingkungan institusi pendidikan
Practical Byzantine Fault Tolerance (PBFT)	Konsensus cepat, toleran terhadap kegagalan Byzantine	Sangat sesuai untuk jaringan permissioned karena memberikan finalitas transaksi deterministik dan mendukung verifikasi *real-time*
Proof of Authority (PoA)	Validator berbasis identitas tepercaya	Cocok untuk sistem berbasis institusi dengan tingkat kepercayaan tinggi dan latensi rendah, namun memiliki tingkat desentralisasi terbatas
IBFT (Istanbul BFT)	Varian BFT dengan finalitas deterministik	Mendukung integrasi *smart contract* dengan proses verifikasi yang cepat dan konsisten pada jaringan permissioned

Mekanisme konsensus berbasis *Practical Byzantine Fault Tolerance* (PBFT) dan *Proof of Authority* (PoA) memiliki karakteristik yang sesuai untuk sistem verifikasi ijazah digital pada lingkungan jaringan tertutup (permissioned), terutama dalam aspek kecepatan verifikasi dan finalitas transaksi. Namun, penelitian ini menggunakan platform Ethereum yang menerapkan mekanisme konsensus Proof of Stake (PoS), sehingga pemilihan konsensus disesuaikan dengan karakteristik jaringan publik yang digunakan. Mekanisme PoS dipilih karena memberikan efisiensi, keamanan, dan dukungan terhadap implementasi *smart contract* dalam sistem terdesentralisasi.

2.1.5 Sistem Otentikasi Terdistribusi

Sistem autentikasi terdistribusi merupakan metode verifikasi identitas atau keaslian data yang tidak bergantung pada satu server pusat, melainkan dilakukan melalui jaringan yang terdiri atas banyak *node* yang saling berkoordinasi (Tripathi et al., 2023). Proses autentikasi pada sistem ini tidak dikendalikan oleh satu otoritas tunggal, sehingga mampu menghilangkan risiko terjadinya titik kegagalan tunggal (*single point of failure*).

Sistem autentikasi tradisional umumnya bergantung pada server pusat yang menyimpan basis data identitas. Ketergantungan tersebut menimbulkan sejumlah kerentanan, seperti risiko peretasan, manipulasi data, serta kegagalan layanan apabila terjadi gangguan pada server. Sistem autentikasi terdistribusi memungkinkan proses verifikasi data dilakukan secara kolektif oleh banyak pihak melalui mekanisme konsensus, sehingga meningkatkan ketahanan dan keandalan sistem (Tripathi et al., 2023).

2.1.6 *Decentralized Identifier* (DID)

Decentralized Identifier (DID) merupakan konsep identitas digital terdesentralisasi yang memungkinkan suatu entitas memiliki identitas unik yang dapat diverifikasi secara kriptografis tanpa bergantung pada otoritas pusat. Konsep DID dirancang untuk memberikan kontrol identitas kepada pemiliknya serta mengurangi ketergantungan pada sistem identitas terpusat yang rentan terhadap manipulasi dan kegagalan tunggal (Schardong & Custódio, 2022).

Sistem identitas berbasis DID menggunakan pasangan kunci kriptografis, sementara dokumen DID disimpan atau direferensikan pada sistem terdistribusi, seperti *Blockchain*. Pendekatan ini memungkinkan proses verifikasi identitas

dilakukan secara *peer-to-peer* dan keabsahannya dapat diuji secara kriptografis berdasarkan standar terbuka (Schardong & Custódio, 2022).

Berbagai penelitian menunjukkan bahwa implementasi *Decentralized* Identifier (DID) dalam sistem verifikasi akademik masih menghadapi sejumlah tantangan, terutama terkait integrasi dengan *smart contract* dan pengelolaan siklus hidup kredensial, seperti pembatalan atau pencabutan ijazah (*revocation*). Kondisi tersebut menunjukkan perlunya perancangan sistem yang mampu mengintegrasikan DID secara operasional dalam alur verifikasi yang bersifat *end-to-end* (Schardong & Custódio, 2022).

2.1.7 *Revocation* dalam Kredensial Digital

Revocation merupakan mekanisme penting dalam siklus hidup kredensial digital untuk memastikan status validitas kredensial secara berkelanjutan. Sejumlah sistem verifikasi ijazah digital masih terbatas pada pembuktian penerbitan dokumen dan belum menyediakan mekanisme *revocation* yang bersifat operasional, sehingga status kredensial, baik valid maupun tidak valid, tidak selalu dapat dipastikan secara *real-time* (Rustemi et al., 2023). Integrasi mekanisme *revocation* berbasis *Blockchain* dan *smart contract* memungkinkan pembaruan status kredensial dilakukan secara transparan dan dapat diverifikasi oleh pihak ketiga tanpa ketergantungan pada institusi penerbit (Schardong & Custódio, 2022).

2.1.8 Ethereum

Ethereum merupakan platform *Blockchain* publik bersifat *open-source* yang dirancang untuk mendukung eksekusi *smart contract* dan pengembangan *Decentralized Applications* (DApps). Ethereum memperluas konsep *Blockchain* dari sekadar pencatatan transaksi nilai menjadi platform komputasi umum yang

mendukung logika bisnis terprogram (Kistaubayev et al., 2023). Secara arsitektural, Ethereum bekerja sebagai mesin *state* terdistribusi yang mengikuti fungsi transisi *state* deterministik, di mana setiap *node* dalam jaringan menjalankan *Ethereum Virtual Machine* (EVM) secara serempak untuk memvalidasi transaksi dan mempertahankan *state* global yang konsisten.

Komponen inti Ethereum mencakup EVM sebagai mesin eksekusi *bytecode* yang bersifat *sandboxed* pada setiap *node*, mekanisme *gas* sebagai satuan biaya komputasi yang mencegah eksekusi tak terbatas, serta model akun berbasis dua jenis entitas, yaitu *Externally Owned Accounts* (EOA) yang dikendalikan pengguna dan *Contract Accounts* yang dikendalikan kode *smart contract*. Sejak *The Merge* pada September 2022, Ethereum beralih dari mekanisme konsensus *Proof of Work* ke *Proof of Stake* (PoS) melalui protokol Casper FFG dan LMD-GHOST, yang menurunkan konsumsi energi jaringan hingga 99,98% sekaligus mempertahankan jaminan keamanan kriptografis yang kuat (Kapengut & Mizrach, 2023).

Ethereum menjadi platform yang paling relevan untuk sistem verifikasi ijazah digital karena beberapa alasan. Pertama, *smart contract* yang bersifat *Turing-complete* memungkinkan implementasi logika penerbitan, verifikasi, dan pencabutan ijazah secara otomatis. Kedua, standar DID berbasis Ethereum (did:ethr) mendukung model identitas terdesentralisasi sesuai spesifikasi W3C. Ketiga, ekosistem pengembangan yang matang mencakup Solidity, Remix IDE, Hardhat, serta jaringan pengujian seperti Sepolia *Testnet* yang memungkinkan simulasi sistem secara terkontrol tanpa biaya transaksi nyata (Kistaubayev et al., 2023).

2.1.9 *Decentralized Applications* (DApps)

Decentralized Applications (DApps) merupakan perangkat lunak yang logika bisnisnya dieksekusi pada jaringan *peer-to-peer* terdistribusi berbasis *Blockchain*, dan bukan pada *server* terpusat milik satu entitas (Zheng dkk., 2023). Sebuah aplikasi dikategorikan sebagai DApp apabila memenuhi empat karakteristik fundamental, yaitu bersifat *open source*, terdesentralisasi, memanfaatkan mekanisme insentif berbasis *token* kriptografis, serta memvalidasi transaksi melalui protokol konsensus sehingga seluruh *node* memiliki salinan *ledger* yang identic (Zheng dkk., 2023). Motivasi utama pengembangan DApps adalah menghilangkan ketergantungan pada otoritas pusat yang menjadi *single point of failure* dalam sistem tradisional.

Arsitektur DApp secara umum diorganisasi dalam tiga lapisan yang saling melengkapi. Lapisan pertama adalah *frontend* berbasis antarmuka pengguna yang dibangun menggunakan *framework* seperti React.js, terhubung ke jaringan *Blockchain* melalui pustaka Ethers.js atau Web3.js dan *wallet* MetaMask. Lapisan kedua adalah *smart contract* yang mengenkode aturan bisnis dan bersifat *immutable* serta dieksekusi secara deterministik oleh setiap *node*. Lapisan ketiga adalah *Blockchain backend* sebagai *distributed ledger* tempat transaksi dikonfirmasi melalui mekanisme konsensus, yang dapat dilengkapi dengan penyimpanan data *off-chain* seperti IPFS untuk menangani data berukuran besar secara efisien (Lai et al., 2023) Dalam konteks verifikasi ijazah digital, DApps memberikan solusi fundamental terhadap keterbatasan sistem terpusat. Sifat *immutability* kriptografis menjamin data ijazah tidak dapat dimanipulasi setelah dicatat, sementara arsitektur *trustless* memungkinkan verifikasi dilakukan secara langsung tanpa perantara.

2.1.10 *InterPlanetary File System* (IPFS)

InterPlanetary File System (IPFS) merupakan protokol jaringan *peer-to-peer* terdistribusi untuk menyimpan, mengalamatkan, dan mengirimkan berkas dalam ruang penyimpanan global yang terdesentralisasi (Trautwein et al., 2022) Berbeda dengan HTTP yang mengambil data berdasarkan lokasi server (URL/IP), IPFS menggunakan paradigma *content addressing* di mana setiap berkas diidentifikasi berdasarkan isi kontennya melalui nilai *hash* kriptografis yang disebut *Content Identifier* (CID). Setiap berkas di-*hash* menggunakan SHA-256 sehingga perubahan sekecil apa pun pada isi berkas akan menghasilkan CID yang berbeda, yang menjamin integritas data secara *by design(Trautwein et al., 2022).*

Secara arsitektural, IPFS mensintesis beberapa teknologi terdahulu. Pertama, *Distributed Hash Table* (DHT) berbasis Kademlia digunakan untuk *peer routing* dan *content routing*, di mana setiap CID direplikasi pada 20 *node* terdekat untuk menjamin ketersediaan. Kedua, struktur data *Merkle Directed Acyclic Graph* (Merkle DAG) digunakan untuk merepresentasikan berkas dalam bentuk blok-blok terverifikasi yang saling terhubung, sehingga mendukung *deduplication* otomatis dan verifikasi integritas secara efisien. Ketiga, protokol *BitSwap* menangani pertukaran blok antar *peer* secara efisien dengan strategi *tit-for-tat* untuk mencegah *free-riding (Trautwein et al., 2022)*

Dalam sistem verifikasi ijazah berbasis *Blockchain*, IPFS berperan sebagai lapisan penyimpanan dokumen *off-chain* untuk mengatasi keterbatasan biaya penyimpanan di jaringan Ethereum. Sistem hanya menyimpan *CID* IPFS berukuran kurang dari 50 *byte* di dalam *smart contract*, sehingga biaya *gas* dapat ditekan secara signifikan. Pendekatan ini menghasilkan jaminan integritas ganda: dokumen

bersifat *immutable* melalui *content addressing* IPFS, sekaligus *CID*-nya tercatat permanen di *Blockchain* sehingga perubahan sekecil apa pun pada dokumen ijazah akan langsung terdeteksi. (Sultana et al., 2023).

2.2 State-of-the-Art

Penelitian terkini dalam bidang verifikasi ijazah digital berbasis *Blockchain* menunjukkan fokus yang kuat pada peningkatan keamanan, transparansi, dan kepercayaan terhadap proses validasi kredensial akademik. *State of the Art* pada Tabel 2.2 merangkum berbagai pendekatan yang memanfaatkan *Blockchain* dan *smart contract* untuk mengatasi keterbatasan sistem verifikasi tradisional.

Tabel II.2 *State-of-the-Art* (SOTA)

No	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
1	*Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation*	Memiliki arsitektur sistem yang jelas serta mampu mengatasi pemalsuan sertifikat digital.	Menggunakan MD5 yang kurang aman dan tidak disertai evaluasi performa.	Diperlukan penggunaan algoritma kriptografi yang lebih kuat serta evaluasi kinerja sistem.
2	*Electronic document authenticity verification of diploma and transcript using smart contract on ethereum Blockchain*	Sistem bersifat transparan dan proses verifikasi berbasis file lebih praktis.	Pengujian terbatas dan belum membahas aspek biaya serta keamanan.	Diperlukan pengujian dalam skala besar serta analisis performa dan keamanan.
3	*Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications*	Sistem terdesentralisasi dengan verifikasi *QR Code* yang cepat dan biaya implementasi rendah.	Pengujian hanya pada test network dan belum ada evaluasi.	Perlu pengujian skala besar dan analisis performa.

No	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
4	*Blockchain-Based E-Certificate System: Secure and Transparent Credential Management*	Menjamin keamanan dan integritas data dengan verifikasi otomatis berbasis *smart contract* serta telah diimplementasikan.	Skala terbatas dan biaya operasional tinggi.	Perlu optimasi performa dan skalabilitas.
5	*DIAR: A Blockchain-Based System for Generation and Verification of Academic Diplomas*	Arsitektur sistem lengkap serta mempertimbangkan integrasi AI.integrasi AI dan keamanan lanjutan.	Masih konseptual dan belum diuji secara nyata.	Perlu implementasi dan validasi sistem.
6	*Development of Blockchain-Based Academic Credential Verification System*	Meningkatkan efisiensi dan keamanan dengan verifikasi QR Code serta evaluasi performa.	Error rate tinggi, pengujian terbatas, dan integrasi belum optimal.	Perlu peningkatan keandalan, pengujian skala besar, dan optimasi sistem.
7	Implementasi Teknologi *Smart contract*s untuk Sistem Ijazah Digital di Politeknik Negeri Samarinda	Verifikasi sertifikat cepat, transparan, dan terdesentralisasi dengan implementasi sistem nyata.	Pengujian terbatas pada fungsional, belum ada analisis performa dan keamanan.	Perlu optimasi biaya dan fleksibilitas data
8	*Decentralized Academic Certificate Issuance and*	Sistem aman dan transparan dengan verifikasi cepat serta	Masih menggunakan MD5, belum ada evaluasi performa dan scalability secara mendalam.	Perlu penguatan kriptografi, evaluasi

No	Judul Penelitian	Kelebihan	Kekurangan	Gap Penelitian
	Verification Using Blockchain Technology	mengurangi pemalsuan sertifikat.		performa, dan pengujian skala besar.
9	*Implementation of Diploma and Transcript Verification System on the Ethereum Blockchain Network*	Meningkatkan keamanan dan transparansi dengan verifikasi QR Code serta implementasi sistem berbasis web.	Biaya gas fee tinggi, data tidak dapat diubah, dan masih menggunakan data eksperimen.	Perlu optimasi biaya, fleksibilitas data, dan pengujian pada lingkungan nyata.
10	*A BLOCKCHAIN-BASED DIGITAL EDUCATIONAL CERTIFICATE VERIFICATION SYSTEM*	Sistem aman, transparan, dan mendukung verifikasi cepat serta fitur revocation.	Evaluasi terbatas (10 pengguna), maintainability rendah, dan ketergantungan pada platform.	Perlu peningkatan evaluasi skala besar, maintainability, dan independensi sistem.

Blockchain menjadi solusi efektif dalam meningkatkan keamanan dan transparansi proses verifikasi ijazah digital. Berbagai penelitian memanfaatkan *Blockchain*, *smart contract*, *hash*ing kriptografis, dan QR Code untuk menjamin integritas dokumen akademik serta mencegah pemalsuan. Hasil penelitian tersebut menunjukkan bahwa *Blockchain* mampu meningkatkan keandalan dan efisiensi verifikasi ijazah oleh pihak ketiga.

Analisis terhadap penelitian pada Tabel 2.2 menunjukkan bahwa sebagian besar penelitian masih berfokus pada aspek verifikasi integritas dokumen melalui pencocokan *hash* dan pemanfaatan QR Code. Pendekatan tersebut hanya memastikan bahwa dokumen tidak mengalami perubahan, tetapi belum mampu menjamin keabsahan identitas pihak penerbit dokumen. Ketiadaan mekanisme

verifikasi identitas penerbit secara terdesentralisasi menyebabkan sistem masih memiliki celah dalam memastikan validitas sumber dokumen.

Selain itu, proses verifikasi masih dilakukan secara parsial dan belum mengintegrasikan verifikasi integritas dokumen, identitas penerbit, dan status dokumen dalam satu sistem terpadu. Kondisi ini menyebabkan proses verifikasi belum efisien dan belum memberikan jaminan keabsahan secara menyeluruh. Penelitian ini mengusulkan sistem verifikasi ijazah berbasis *Blockchain* dan *smart contract* yang terintegrasi dengan *Decentralized* Identifier (DID) dan mekanisme revocation *on-chain* untuk mendukung proses verifikasi yang lebih aman, efisien, dan terpadu

2.3 Matriks Penelitian

Matriks penelitian yang disajikan dalam Tabel 2.3 menggambarkan pemetaan penelitian-penelitian terkait sistem verifikasi ijazah berbasis *Blockchain* yang telah dilakukan. Matriks ini memuat informasi mengenai penulis dan judul penelitian, jenis *Blockchain* yang digunakan, cakupan penerapan *smart contract*, pemanfaatan identitas penerbit berbasis *Decentralized Identifier* (DID), ketersediaan mekanisme *revocation*, aspek keamanan, mekanisme konsensus, serta tingkat implementasi sistem. Penyajian matriks ini bertujuan untuk memudahkan perbandingan pendekatan yang digunakan, sekaligus mengidentifikasi celah penelitian yang belum sepenuhnya terakomodasi dalam studi-studi sebelumnya.

Tabel II.3 Matriks Penelitian

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
1	(Chaniago et al., 2021)	*Electronic document authenticity verification of diploma and transcript using smart contract on ethereum Blockchain*	*Public*	✓	-	-	✓	PoW	Implementasi
2	(Djajadi et al., 2023)	*Blockchain-Based E-Certificate Verification and Validation Automation Architecture to Avoid Counterfeiting of Digital Assets in Order to Accelerate Digital Transformation*	*Public*	✓	-	-	✓	PoS	Prototipe

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
3	(Gangwar, 2024)	*Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications*	*Public*	✓	-	-	✓	PoS	*Testnet*
4	(Chotijah et al., 2024)	*Blockchain-Based E-Certificate System: Secure and Transparent Credential Management*	*Private*	✓	-	-	-	PBFT	Implementasi

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
5	(Rustemi et al., 2024)	*DIAR: a Blockchain-based system for generation and verification of academic diplomas*	*Public*	✓	-	✓	✓	PoS	Konseptual
6	(Noshi & Yuan Xu, 2024)	*Development of Blockchain-Based Academic Credential Verification System*	*Public*	✓	-	-	✓	PoS	Prototipe

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
7	(Putri et al., 2024)	*Implementation of Diploma and Transcript Verification System on the Ethereum Blockchain Network*	*Public*	✓	-	-	✓	PoW	Implementasi
8	(Ifeyemi et al., 2024)	*A Blockchain-Based Digital Educational Certificate Verification System*	*Public*	✓	-	✓	✓	PoS	Implementasi

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
9	(Fikri et al., 2025)	*Implementasi Teknologi Smart contracts Untuk Sistem Ijazah Digital Di Politeknik Negeri Samarinda*	*Public*	✓	-	-	✓	PoW	Implementasi
10	(Dr. Rashmi H C et al., 2025)	*Decentralized Academic Certificate Issuance and Verification Using Blockchain Technology*	*Public*	✓	-	-	✓	PoS	Prototipe

No	Penulis	Judul	*Blockchain*	Ruang Lingkup				Konsensus	Implementasi
				Smart contract	Issuer Identity (DID – W3C)	Revocation Mechanism	Keamanan		
11	Penelitian ini	Implementasi *Blockchain* Berbasis *Smart contract* Untuk Sistem Verifikasi IjazahTerdistribusi Dengan Pendekatan *Decentralized Identifier*	*Public*	✓	✓	✓	✓	PoS	Implementasi

Analisis terhadap matriks penelitian pada Tabel 2.3 menunjukkan bahwa sebagian besar penelitian masih berfokus pada pembuktian integritas dokumen melalui pemanfaatan *Blockchain* dan *smart contract*, tanpa mengintegrasikan penjaminan identitas penerbit secara terdesentralisasi. Sebagian penelitian juga belum mengimplementasikan mekanisme *revocation* secara operasional, sehingga sistem belum mampu menangani perubahan status validitas ijazah secara dinamis.

Penelitian ini mengusulkan sistem verifikasi ijazah terdistribusi yang mengintegrasikan *Decentralized Identifier* (DID) sebagai mekanisme verifikasi identitas penerbit serta menerapkan mekanisme *revocation on-chain* dalam satu sistem terpadu. Implementasi

sistem menggunakan *Blockchain* publik berbasis *Ethereum* dengan mekanisme konsensus *Proof of Stake* (PoS), sehingga mampu mendukung proses verifikasi yang efisien, aman, dan andal.