BAB IV

PENYAJIAN DATA DAN PEMBAHASAN

A. Penyajian Data

Pencarian jurnal dilakukan dengan kata kunci blockchain *fraud*, *blockchain fraud prevention, blockchain fraud detection, fraud control, anti-fraud system, dan security model of blockchain*. Hasilnya, ditemukan 224 jurnal yang terindeks Scopus. Setelah screening, 83 jurnal dihapus, termasuk 35 jurnal duplikasi, 37 jurnal yang tidak memenuhi kriteria tahun publikasi (2019-2024), dan 27 jurnal yang tidak sesuai dengan Scopus tier (Q1, Q2, Q3).

Proses *screening* dilakukan terhadap 125 jurnal, di mana 67 jurnal dikeluarkan pada tahap ini. Pada tahap *eligibility*, sebanyak 58 jurnal diperiksa secara lengkap (*full-text*), namun 39 di antaranya tidak dapat diakses secara penuh. Setelah tahap *eligibility* selesai, penelitian berlanjut ke tahap *included*, menghasilkan 19 jurnal yang menjadi sampel untuk *review*. Gambaran tahapan ini dapat dilihat melalui diagram *PRISMA* yang disajikan pada tabel berikut

Tabel 4. 1 Tahapan Proses PRISMA

Tahap	Proses	Jumlah Jurnal
Identifikasi	Artikel yang ditemukan melalui pencarian di Scopus	224
	Artikel tambahan yang ditemukan melalui sumber lain	0
Total Identifikasi	Total artikel yang berhasil diidentifikasi	224
	Artikel yang dikeluarkan sebelum screening	83

	Artikel Terindikasi Duplikasi	35
	Tidak memenuhi kriteria tahun publikasi (2019-2024)	27
	Tidak memenuhi kriteria tier (Q1,Q2,Q3)	21
Screening	Artikel yang diseleksi	125
	Artikel yang dikeluarkan pada tahap screening	67
Eligibility	Artikel yang diperiksa teks lengkapnya (*full text)*	58
	Artikel yang tidak dapat diakses teks lengkapnya	39
	Artikel yang dibuang pada tahap eligibility	0
Include	Artikel yang masuk dalam review	19
	Artikel yang masuk dalam review dari sumber lain	1

Sumber: Hasil olah data WATASE UAKE

Berdasarkan diagram *PRISMA* yang telah dijelaskan, jurnal yang terpilih akan disajikan dalam tabel 4.1 berikut:

Tabel 4. 2 Analisis Jurnal

NO	Penulis	Judul	Nama Jurnal	Tahun	Hasil
1	Ahmed Abdelmoamen Ahmed, Oluwayemisi O. Alabi	Secure and Scalable *Blockchain*-Based Federated Learning for Cryptocurrency *Fraud* Detection: A Systematic Review	Al-Based Search	2024	- Peningkatan Deteksi Penipuan melalui *Blockchain federated Learning* (BCFL) - Meningkatkan Keamanan dan Privasi lewat integrasi teknik *Secure Multi-Party Computation* (SMPC) dan penggunakan teknologi canggih *Elliptic Curve Cryptography* (ECC)
2	Umar Islam, Abdullah Alshammari, Zaid Alzaid, Adeel Ahmed, Asima Abdullah, Saman Iftikhar, Shaikhan	Enhancing *Blockchain* Security Against Data Tampering: Leveraging Hybrid Model in Multimedia Forensics and Multi-Party Computation for Supply Chain Data Protection	Al-Based Search	2024	- Akurasi Deteksi Tinggi: Pendekatan hybrid LSTM-GRU dalam penelitian ini mencapai akurasi deteksi pemalsuan media sebesar 95%, menunjukkan peningkatan signifikan dibandingkan metode tradisional seperti SVM, KNN, dan Random Forest - Efisiensi Pemrosesan: Meskipun teknik privasi meningkatkan waktu pemrosesan, metode ini tetap efisien dengan waktu pelatihan 180 detik

	Bawazeer, dan Muhammad Izhar				dan inferensi 13.5 milidetik, menjadikannya layak untuk penggunaan praktis.
3	Khoa Tan-Vo, Khanh Pham, Phu Huynh, Mong-Thy Nguyen THI, Thu-Thuy Ta, Thu Nguyen, Tu-ANH Nguyen-Hoang, Ngoc-Thanh Dinh, dan Hong-Tri Nguyen	Optimizing Academic Certificate Management With *Blockchain* and Machine Learning: A Novel Approach Using Optimistic Rollups and *Fraud* Detection	Al-Based Search	2024	- Integrasi *blockchain* dengan Layer-2 (Optimistic Rollups) berhasil mengurangi biaya dan latensi transaksi hingga 61.92%, sekaligus meningkatkan skalabilitas dan keamanan dalam pengelolaan sertifikat akademik. - Dengan model machine learning XGBoost, sistem mencapai F1-score 99.42% dalam mendeteksi penipuan di jaringan Ethereum, memastikan integritas dan keamanan manajemen sertifikat.
4	Keundug Park dan heung-Youl Youm	Proposal of a Service Model for *Blockchain*-Based Security Tokens	Big data and Cognitive Computing	2024	- *Blockchain* berpotensi meningkatkan investasi dalam aset tokenisasi, baik berwujud maupun tidak. Penelitian ini mengusulkan model layanan token keamanan berbasis *blockchain* untuk memfasilitasi investasi, perdagangan, serta

					mengidentifikasi ancaman keamanan, kebutuhan privasi, dan kepatuhan regulasi, termasuk AML.
5	Baabdullah, Tahani; Alzahrani, Amani; Rawat, Danda B.; Liu, Chunmei	Efficiency of Federated Learning and *Blockchain* in Preserving Privacy and Enhancing the Performance of Credit Card *Fraud* Detection (CCFD) Systems	Future Internet	2024	- Integrasi *Federated Learning* (FL) dengan *blockchain* dapat meningkatkan kinerja dan akurasi dalam deteksi penipuan - Hasil menunjukkan efektivitas pendekatan dalam mendeteksi transaksi penipuan sambil menjaga privasi data - Blockhcain menyediakan penyimpanan desentralisasi yang aman, sehingga pembaruan model tidak dapat dimanipulasi
6	Wei, Sizheng; Lee, Suan	Financial Anti-*Fraud* Based on Dual-Channel Graph Attention Network	Journal of Theoretical and Applied Electronic Commerce Research	2024	- Hasil penelitian menunjukkan bahwa model GBDT-DGAN memiliki performa unggul dalam mendeteksi penipuan keuangan, dengan akurasi mencapai 93.82%, recall 89.5%, dan skor F1 81.66%. Model ini secara signifikan lebih efektif dibandingkan metode tradisional seperti GCN, BiLSTM, dan CNN, dengan peningkatan akurasi hingga 5.76%

7	Louati, Hassen; Louati, Ali; Almekhlafi, Abdulla; ElSaka, Maha; Alharbi, Meshal; Kariri, Elham; Altherwy, Youssef N	Adopting Artificial Intelligence to Strengthen Legal Safeguards in *Blockchain* Smart Contracts A Strategy to Mitigate *Fraud* and Enhance Digital Transaction Security	Journal of Theoretical and Applied Electronic Commerce Research	2024	- Model *Convolutional Neural Networks* (CNN) yang diusulkan memiliki kinerja unggul dalam mendeteksi aktivitas penipuan pada kontrak pintar *blockchain*, dengan tingkat kesalahan serendah 2.10 dan hanya 1.3 juta parameter.
8	Yakubu Bello Musa, Sabi'u Jamilu, Bhattarakosol Pattarasinee	*Blockchain*-based privacy and security model for transactional data in large *private* network	Scientific Reports	2023	- Model yang di usulkan mampu meningkatan Kecepatan Enkripsi hingga 17 kali dan Dekripsi hingga 4 kali dengan percepatan keskuruhan sebesar 16,5 di bandingkan model yang ada. - Model ini secara efektif menangkal ancaman keamanan seperti serangan man-in-the-middle dan replay dengan menggunakan sertifikat digital,

9	Jia Li	Dynamic financial and monetary security risk assessment based on information service security assessment model and *blockchain*	Scientific Reports	2023	- Peristiwa ketidakpastian di pasar forex dan saham secara signifikan mempengaruhi pengembalian Bitcoin, - Model penilaian keamanan informasi dan kepercayaan berbasis *blockchain* yang diusulkan efektif dalam mengelola risiko keamanan di pasar keuangan
10	Selvarajan, Shitharth; Srivastava, Gautam; Khadidos, Alaa O.; Khadidos, Adil O.; Baza, Mohamed; Alshehri, Ali; Lin, Jerry Chun-We	An artificial intelligence lightweight *blockchain* security model for security and privacy in IIoT system	Journal of Cloud Computing	2023	- Model keamanan yang diusulkan, yaitu *Artificial Intelligence-based Lightweight Blockchain Security Model* (AILBSM), menunjukkan kinerja yang signifikan dengan akurasi klasifikasi mencapai 99,8% dan kinerja deteksi mencapai 99,7%, jauh lebih baik dibandingkan metode konvensional.

11	Marjanovic, Jelena; Dalcekovic, Nikola; Sladic, Goran	*Blockchain*-based model for tracking compliance with security requirements	Computer Science and Information Systems	2023	- Model berbasis *blockchain* dengan IPFS dan Ethereum Ropsten untuk melacak kepatuhan keamanan dalam siklus hidup pengembangan perangkat lunak (SDL). Model ini melibatkan pemangku kepentingan seperti manajer proyek dan auditor, serta mendukung kepatuhan terhadap standar IEC 62443-4-1.
12	Mapa Mudiyanselage, Chalani; Perera, Pethigamage; Grandhi, Sriamannarayana	A *Blockchain*-Based Model for the Prevention of Superannuation *Fraud* A Study of Australian Super Funds	Applied Sciences	2023	- Penggunaan teknologi *blockchain* dapat meningkatkan transparansi dalam proses kontribusi superannuation. Dengan adanya sistem yang lebih transparan, deteksi penipuan seperti superannuation yang tidak dibayar dapat dilakukan lebih efektif, mengurangi ketergantungan pada keluhan karyawan dan audit internal
13	Mohammed, Mohammed A.; Boujelben,	A Novel Approach for *Fraud* Detection in *Blockchain*-Based Healthcare Networks	Future Internet	2023	- Penelitian menunjukkan bahwa algoritma Random Forest memiliki kinerja terbaik dalam mendeteksi penipuan dan serangan dalam konteks *blockchain*

	Manel; Abid, Mohamed	Using Machine Learning			- Sistem yang diusulkan, yang mengintegrasikan pembelajaran mesin dengan teknologi *blockchain*, berhasil meningkatkan keamanan dan keandalan aplikasi kesehatan berbasis *blockchain*
14	Kapadiya, Khyati; Patel, Usha; Gupta, Rajesh; Alshehri, Mohammad Dahman; Tanwar, Sudeep; Sharma, Gulshan; Bokoro, Pitshou N.	*Blockchain* and AI-Empowered Healthcare Insurance *Fraud* Detection an Analysis, Architecture, and 2022Future Prospects	IEEE Access	2022	- Penelitian ini mengusulkan arsitektur sistem deteksi penipuan asuransi kesehatan yang terdiri dari empat lapisan, yang mengintegrasikan teknologi *blockchain* dan kecerdasan buatan untuk meningkatkan transparansi dan kepercayaan antara penyedia layanan kesehatan dan pemegang polis
15	Pranto, Tahmid Hasan; Hasib, Kazi Tamzid Akhter Md.;	*Blockchain* and Machine Learning for *Fraud* Detection A Privacy-Preserving and	IEEE Access	2022	- Hasil penelitian ini menunjukkan bahwa integrasi teknologi *blockchain* dengan machine learning (ML) dapat secara efektif meningkatkan deteksi penipuan.

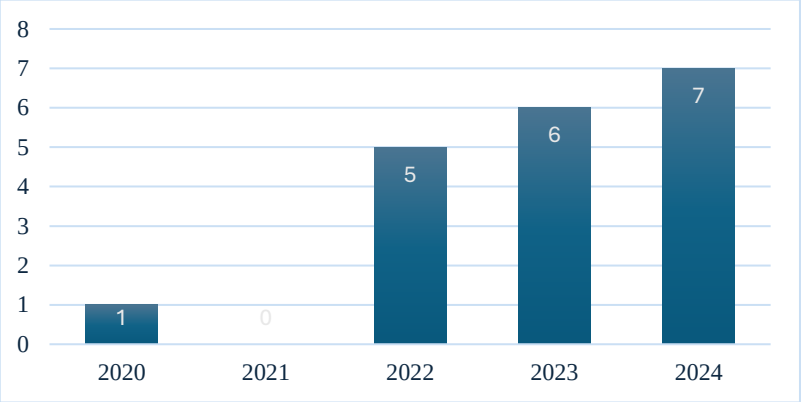
	Rahman, Tahsinur; Haque, Akm Bahalul; Islam, A. K. M. Najmul; Rahman, Rashedur M.	Adaptive Incentive Based Approach			- Alogaritme *Passive Aggressive Classifer* menunjukkan kinarja terbaik di antara model yang di uji dengan akurasi sebasar 93,7% serta skor *presisi-recall* dan F1 terbaik. - Studi ini memperkenalkan mekanisme insentif adaptif untuk mendorong partisipasi organisasi dalam memperbarui model pembelajaran mesin.
16	Lyu, Qiuyun; Li, Hao; Zhou, Renjie; Zhang, Jilin; Zhao, Nailiang; Liu, Yan	BCFDPS: A *Blockchain*-Based Click *Fraud* Detection and Prevention Scheme for *Online* Advertising	Security and Communication Networks	2022	- BCFDPS mampu mendeteksi setiap klik penipuan dengan probabilitas 100% dan Skema berbasis *blockchain* BCFDPS mampu deteksi penipuan klik dengan presisi 100% dan waktu verifikasi 7,87 ms, lebih efisien dibandingkan metode tradisional. - Skema ini melindungi privasi pengguna dan mengurangi biaya komunikasi dan penyimpanan, menjadikannya solusi unggul untuk pencegahan penipuan klik dalam periklanan *online*.
17	Bellagarda, Jagger; Abu-	Connect2NFT A Web-Based, *Blockchain*	Mathematics	2022	- Penelitian ini berhasil mengembangkan sebuah aplikasi yang mampu mengotentikasi

	Mahfouz, Adnan M.	Enabled NFT Application with the Aim of Reducing *Fraud* and Ensuring Authenticated Social, Non-Human Verified Digital Identity			kepemilikan NFT secara pribadi, aman, dan ekonomis. - Penelitian ini juga mengusulkan alur kerja teoritis yang mengintegrasikan NFT, IPFS (InterPlanetary File System), dan kredensial yang dapat diverifikasi untuk penyimpanan terdesentralisasi. - Penyimpanan Terdesentralisasi melalui IPFS dan Arweave menawarkan solusi untuk penyimpanan permanen
18	Ashfaq, Tehreem; Khalid, Rabiya; Yahaya, Adamu Sani; Aslam, Sheraz; Azar, Ahmad Taher; Alsafari, Safa; Hameed, Ibrahim A.	A Machine Learning and *Blockchain* Based Efficient *Fraud* Detection Mechanism	Sensors	2022	- Model pembelajaran mesin berbasis *blockchain* yang diusulkan berhasil mendeteksi transaksi penipuan pada jaringan Bitcoin dengan tingkat akurasi yang tinggi - Dengan menggunakan teknik seperti XGboost dan Random Forest model ini dapat mengklasifikasikan transaksi dengan lebih baik dan mengurangi jumlah entitas penipuan.

19	Tsoulias, Konstantinos; Palaiokrassas, Georgios; Fragkos, Georgios; Litke, Antonios; Varvarigou, Theodora A.	A Graph Model Based *Blockchain* Implementation for Increasing Performance and Security in Decentralized Ledger Systems	IEEE Access	2020	- Penerapan model graf dengan basis data Neo4j dapat meningkatkan kinerja dan keamanan *blockchain*. Mekanisme konsensus berbasis Casper yang mengintegrasikan PoW dan PoS, serta sistem validator dinamis, mempercepat konsensus, memperkuat analisis data, dan meningkatkan ketahanan terhadap serangan 51% dan Sybil

b. Data Jurnal Berdasarkan Tahun Publikasi

Grafik 4 1. Data Jurnal Berdasarkan Tahun Publikasi

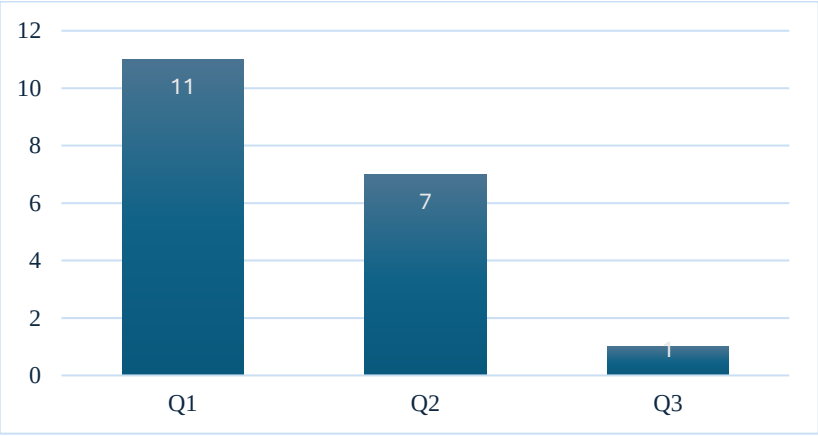


Sumber: Data diolah

Berdasarkan histogram, dari total 19 jurnal yang digunakan dalam penelitian ini, terdapat 1 jurnal yang dipublikasikan pada tahun 2020, 5 jurnal pada tahun 2022, 6 jurnal pada tahun 2023, dan 7 jurnal pada tahun 2024. Namun dalam penelitian ini, tidak terdapat jurnal yang dipublikasikan pada tahun 2021.

c. Data Jurnal Berdasarkan *Tier Scopus*

Grafik 4.2 Data Jurnal Berdasarkan *Tier Scopus*



Sumber: Data diolah

Berdasarkan histogram, dari total 19 jurnal yang digunakan dalam penelitian ini, terdapat 11 jurnal yang termasuk dalam kategori Q1, 7 jurnal dalam kategori Q2, dan 1 jurnal dalam kategori Q3.

d. Data Jurnal Berdasarkan Jenis Penelitian

Tabel 4. 3 Data Jurnal Berdasarkan Jenis Penelitian

No	Jenis Penelitian	Jumlah Jurnal
1.	Kualitatif	3
2.	Kuantitatif	13
3.	*Mixed Methods*	3
Total		19

Sumber: Data diolah

Berdasarkan data yang ditampilkan, terdapat 19 jurnal yang dianalisis dengan rincian 3 jurnal menggunakan pendekatan kualitatif, 13 jurnal menggunakan pendekatan kuantitatif, dan 3 jurnal menggunakan pendekatan *mixed methods*.

e. Data Jurnal Berdasarkan Objek Penelitian

Tabel 4. 4 Data Jurnal Berdasarkan Objek Penelitian

No	Topik Utama	Jumlah Jurnal
1.	Keamanan *Blockchain*	6
2.	Federated Learning *Blockchain*	2
3.	Deteksi Penipuan Blockchin	9
4.	*Blockchain* dalam Transaksi Keuangan	2
Total		19

Sumber: Data diolah

Dari 19 jurnal yang dianalisis, topik Deteksi Penipuan *Blockchain* paling banyak dibahas dengan 9 jurnal, diikuti oleh Keamanan *Blockchain* dengan 6 jurnal. Sedangkan, topik *Federated Learning Blockchain* dan *Blockchain* dalam Transaksi Keuangan masing-masing hanya memiliki 2 jurnal.

f. Data Jurnal Berdasarkan Publikasi

Tabel 4. 5 Data Jurnal Berdasarkan Publikasi

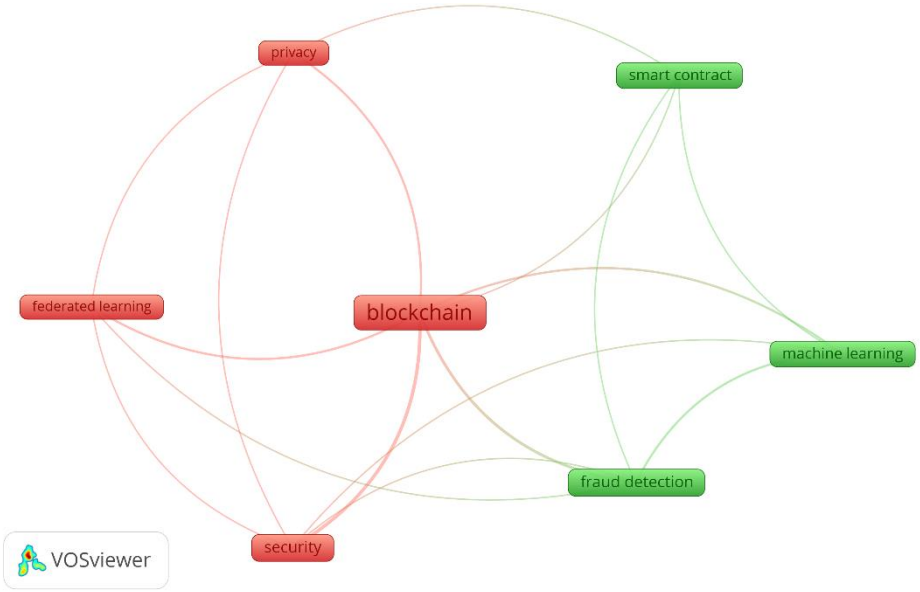
No	Jurnal Publikasi	Jumlah Jurnal
1.	IEEE Acces	6
2.	Big Data and Cognitive Computing	1
3.	Future Internet	2
4.	Journal of Theoretical and Applied Electronic Commerce Research	2
5.	Scientific Reports	2
6.	Journal of Cloud Computing	1
7.	Computer Science and Information Systems	1
8.	Applied Sciences	1
9.	Security and Communication Network	1
10.	Mathematics	1
11.	Sensors	1
Total		19

Dari 19 jurnal yang dianalisis, *IEEE Access* adalah jurnal yang paling sering dipilih, dengan 6 publikasi. Jurnal lainnya, seperti *Future Internet, Journal of Theoretical and Applied Electronic Commerce Research, dan Scientific Reports,* masing-masing memiliki 2 publikasi. Sementara itu, banyak jurnal lain seperti *Big Data and Cognitive Computing, Journal of*

Cloud Computing, dan lainnya hanya memiliki satu publikasi, menunjukkan bahwa topik-topik tersebut lebih spesifik atau kurang sering dibahas

g. Data berdasarkan *VOSviewer*

Gambar 4. 1 Data Berdasarkan VOSviewer



Berdasarkan visualisasi dari Vosviewer, yang menggunakan 19 jurnal sebagai data utama dalam penelitian ini, dengan garis yang menunjukkan hubungan antar topik pembahasan, topik *Blockchain* muncul sebagai topik terbesar dan memiliki hubungan erat dengan semua topik pembahasan lainnya. Pembahasan tentang *security* menjadi topik kedua, yang berhubungan dengan *fraud detection, federated learning, privacy, dan machine learning*. Pembahasan *fraud* detection menempati urutan ketiga, dengan hubungan erat dengan *federated learning, security, smart contract, dan machine learning*. Topik machine learning berada di urutan keempat, dengan hubungan dengan *smart contract, fraud detection, dan security*. Pembahasan *privacy* berada di urutan kelima, yang berhubungan dengan

smart contract, federated learning, dan security. Terakhir, federated learning berhubungan dengan *security, privacy, dan fraud detection.*

B. Analisis Data

1. Hubungan Blcokchain dapat mencegah *Fraud* Keuangan

a. Penerapan *Blockchain* Dalam Sektor Keuangan

Implementasi teknologi *blockchain* dalam sektor keuangan telah memperlihatkan potensi yang luar biasa. Studi oleh *Khoa Tan-Vo et al.* dan *Tahmid Hasan Pranto et al.* menyoroti bahwa *blockchain* memiliki peran signifikan di sektor ini, terutama sebagai sistem *anti-fraud*. Teknologi ini menawarkan platform yang aman, transparan, dan terdesentralisasi, yang secara khusus mendukung kebutuhan sektor keuangan. Penggunaan *blockchain* tidak hanya meningkatkan akurasi dan efisiensi dalam pelaporan keuangan tetapi juga mengurangi risiko kecurangan serta memperkuat transparansi dalam aktivitas keuangan.

Table analisis jurnal penerapan *blockchain* dalam sektor akuntansi dapat di lihat pada tabel 4.3 dibawah ini.

Tabel 4. 6 Jurnal Penerapan *Blockchain* Dalam Sektor Keuangan

Penulis	Judul
Tan-Vo, Khoa; Pham, Khanh; Huynh, Phu; Thi, Mong-Thy Nguyen; Ta, Thu-Thuy; Nguyen, Thu; Nguyen-Hoang, Tu-Anh; Dinh, Ngoc-Thanh; Nguyen, Hong-Tri	Optimizing Academic Certificate Management With *Blockchain* and Machine Learning: A Novel Approach Using Optimistic Rollups and *Fraud* Detection

Park, Keundug; Youm, Heung-Youl	Proposal of a Service Model for *Blockchain*-Based Security Tokens
Yakubu Bello Musa, Sabi'u Jamilu, Bhattarakosol Pattarasinee	*Blockchain*-based privacy and security model for transactional data in large *private* network
Kapadiya, Khyati; Patel, Usha; Gupta, Rajesh; Alshehri, Mohammad Dahman; Tanwar, Sudeep; Sharma, Gulshan; Bokoro, Pitshou N.	*Blockchain* and AI-Empowered Healthcare Insurance *Fraud* Detection an Analysis, Architecture, and 2022 Future Prospects
Pranto, Tahmid Hasan; Hasib, Kazi Tamzid Akhter Md.; Rahman, Tahsinur; Haque, Akm Bahalul; Islam, A. K. M. Najmul; Rahman, Rashedur M.	*Blockchain* and Machine Learning for *Fraud* Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach
Marjanovic, Jelena; Dalcekovic, Nikola; Sladic, Goran	*Blockchain*-Based Model For Tracking Compliance With Security Requirements
Tsoulias, Konstantinos; Palaiokrassas, Georgios; Fragkos, Georgios; Litke, Antonios; Varvarigou, Theodora A	A Graph Model Based *Blockchain* Implementation for Increasing Performance and Security in Decentralized Ledger Systems
Islam, Umar; Alshammari, Abdullah; Alzaid, Zaid; Ahmed, Adeel; Abdullah, Saima; Iftikhar, Saman;	Enhancing *Blockchain* Security Against Data Tampering: Leveraging Hybrid Model in Multimedia Forensics

Bawazeer, Shaikhan; Izhar, Muhammad	and Multi-Party Computation for Supply Chain Data Protection

Penerapan teknologi *blockchain* dalam sektor keuangan telah membawa perubahan signifikan dengan memberikan solusi inovatif untuk mendeteksi penipuan, meningkatkan keamanan, dan menciptakan transparansi dalam berbagai jenis transaksi. *Blockchain* menawarkan keunggulan berupa desentralisasi, transparansi, dan ketidakberubahan data, yang menjadikannya alat penting untuk mencegah berbagai bentuk kecurangan finansial. Dalam transaksi e-commerce dan jaringan Bitcoin, *blockchain* dapat mendeteksi penipuan dengan mengintegrasikan teknologi machine learning. Model deteksi berbasis *blockchain* memanfaatkan pola transaksi mencurigakan untuk pelatihan dan prediksi, sehingga meningkatkan akurasi klasifikasi transaksi secara signifikan (Tan-Vo et al., 2024).

Salah satu tantangan besar dalam transaksi digital adalah masalah double-spending, yaitu upaya untuk menggunakan aset digital yang sama dalam dua transaksi. *Blockchain* mengatasi masalah ini dengan mencatat setiap transaksi secara kronologis menggunakan cap waktu yang dilindungi oleh enkripsi kriptografi. Validasi transaksi dilakukan melalui mekanisme konsensus terdistribusi, memastikan bahwa semua node dalam jaringan menyetujui keabsahan transaksi baru. Teknologi ini juga memberikan solusi efektif dalam sektor asuransi. Misalnya, Roriz dan Pereira mengembangkan sistem *blockchain* yang dapat mendeteksi

penipuan dalam klaim asuransi kendaraan, seperti kasus *double-dipping*, di mana pelaku mencoba mengajukan klaim dari beberapa perusahaan asuransi untuk satu insiden yang sama (Pranto et al., 2022).

Lebih jauh, *blockchain* telah merevolusi perdagangan aset digital melalui tokenisasi, yaitu proses di mana aset fisik atau digital dikonversi menjadi token yang dapat diperdagangkan di jaringan *blockchain*. Hal ini tidak hanya memungkinkan perdagangan yang lebih mudah tetapi juga meningkatkan keamanan dan transparansi dalam transaksi aset seperti saham dan obligasi (Tsoulias et al., 2020). Dalam konteks ini, *blockchain* juga memfasilitasi penerbitan dan pengelolaan token keamanan, memungkinkan investasi lebih fleksibel dalam aset berwujud maupun tidak berwujud (Park & Youm, 2024). Teknologi ini membuka peluang besar bagi investor kecil untuk berpartisipasi dalam pasar yang sebelumnya tidak terjangkau.

Dalam hal privasi dan keamanan data transaksi, *blockchain* memberikan solusi unggul dengan enkripsi berbasis RSA dan penggunaan sertifikat digital untuk melindungi informasi keuangan dari akses yang tidak sah. Transparansi *blockchain* memastikan bahwa semua transaksi dicatat dan dapat diverifikasi oleh pihak-pihak terkait, menciptakan kepercayaan yang lebih tinggi di antara pemangku kepentingan (Yakubu et al., 2023). Selain itu, integrasi *blockchain* dengan algoritma pembelajaran mesin seperti Long Short-Term Memory (LSTM) dan Gated Recurrent Units (GRU) meningkatkan kemampuan

untuk mendeteksi pola dan anomali dalam data keuangan. Ini sangat membantu dalam mengidentifikasi aktivitas mencurigakan yang berpotensi merugikan (Islam et al., 2024)

Blockchain juga mendukung kepatuhan terhadap regulasi di sektor keuangan. Dengan ledger terdistribusi yang tidak dapat diubah, auditor dapat memverifikasi kepatuhan terhadap persyaratan keamanan dengan mudah, yang sangat penting untuk melindungi data sensitif dan mematuhi standar internasional (Marjanović et al., 2023). Tidak hanya itu, teknologi ini mengurangi kebutuhan akan perantara dalam transaksi keuangan, yang secara signifikan dapat menurunkan biaya dan meningkatkan efisiensi operasional (Kapadiya et al., 2022).

Contoh penerapan teknologi *blockchain* adlaah Ripple, yang memungkinkan pembayaran internasional secara real-time dengan biaya lebih rendah dibandingkan metode tradisional. Saat ini, 15 dari 50 bank terbesar dunia telah bekerja sama dengan Ripple untuk mengembangkan platform berbasis *blockchain*. Bank sentral seperti Bank of England juga berkomitmen menggunakan *blockchain* untuk memperbarui infrastruktur basis data mereka, sementara Estonia memelopori penggunaan *blockchain* untuk identitas digital, pencatatan kesehatan, hingga potensi pengembangan pada pemungutan suara dan pengumpulan pajak (Raharjo, 2022).

Selain itu, dalam pengelolaan rantai pasok keuangan, *blockchain* menciptakan transparansi dan keterlacakan yang lebih baik. Walmart,

misalnya, menggunakan *blockchain* untuk melacak pengiriman makanan seperti daging babi dari China, mencatat setiap proses dari asal produk hingga distribusinya. Hal ini tidak hanya meminimalkan sengketa tetapi juga memungkinkan pembayaran lebih cepat kepada mitra di seluruh rantai pasok (Warburg et al., 2019b).

Di bidang akuntansi, *blockchain* menawarkan potensi besar melalui ledger (buku besar) yang tidak dapat diubah dan transparan. Ledger berbasis *blockchain* memungkinkan proses audit menjadi lebih efisien dan mengurangi potensi manipulasi data. Selain itu, transparansi data ini dapat mempermudah pelaporan kepada pemangku kepentingan eksternal, seperti pemerintah atau lembaga perpajakan. Dengan kemampuannya mencatat dan memverifikasi transaksi secara real-time, *blockchain* diyakini sebagai lompatan besar berikutnya dalam teknologi pembukuan, setelah sistem pembukuan berpasangan yang ditemukan pada era Renaisans (akhir abad pertengahan) (Raharjo, 2022; Warburg et al., 2019b).

Secara keseluruhan, *blockchain* membuka era baru di sektor keuangan dengan memberikan solusi yang lebih aman, efisien, dan transparan. Teknologi ini tidak hanya mendukung inovasi seperti smart contracts, yang mengotomatiskan proses transaksi, tetapi juga memperkuat sistem manajemen keuangan untuk mengatasi tantangan masa depan. Hal ini menjadikannya landasan penting untuk membangun kepercayaan dan stabilitas di tengah perkembangan teknologi finansial.

b. Penerapan *Blockchain* Dalam Mencegah dan Mendeteksi *Fraud* Keuangan

Teknologi *Blockchain* telah diidentifikasi sebagai solusi potensial untuk mencegah kecurangan keuangan. Dengan kemampuannya meningkatkan keamanan dan transparansi, *blockchain* membuatnya lebih sulit bagi pelaku penipuan atau *fraud* untuk memanipulasi data keuangan. Selain itu, teknologi ini juga mempermudah proses pelacakan dan deteksi jika terjadi kecurangan keuangan. Beberapa jurnal yang ada menekankan bahwa *blockchain* dapat memperkuat transparansi dan keamanan keuangan, sebagai berikut:

Tabel 4. 7 Jurnal Penerapan *Blockchain* Dalam Mencegah dan Mendeteksi *Fraud* Keuangan

Penulis	Judul
Ahmed, Ahmed Abdelmoamen; Alabi, Oluwayemisi O.	Secure and Scalable *Blockchain*-Based Federated Learning for Cryptocurrency *Fraud* Detection: A Systematic Review
Baabdullah, Tahani; Alzahrani, Amani; Rawat, Danda B.; Liu, Chunmei	Efficiency of Federated Learning and *Blockchain* in Preserving Privacy and Enhancing the Performance of Credit Card *Fraud* Detection (CCFD) Systems
Wei, Sizheng; Lee, Suan	Financial Anti-*Fraud* Based on Dual-Channel Graph Attention Network
Mapa Mudiyanselage, Chalani; Perera, Pethigamage; Grandhi, Sriamannarayana	A *Blockchain*-Based Model for the Prevention of Superannuation *Fraud*: A Study of Australian Super Funds

Pranto, Tahmid Hasan; Hasib, Kazi Tamzid Akhter Md.; Rahman, Tahsinur; Haque, Akm Bahalul; Islam, A. K. M. Najmul; Rahman, Rashedur M.	*Blockchain* and Machine Learning for *Fraud* Detection A Privacy-Preserving and Adaptive Incentive-Based Approach
Mohammed, Mohammed A.; Boujelben, Manel; Abid, Mohamed	A Novel Approach for *Fraud* Detection in *Blockchain*-Based Healthcare Networks Using Machine Learning
Lyu, Qiuyun; Li, Hao; Zhou, Renjie; Zhang, Jilin; Zhao, Nailiang; Liu, Yan	BCFDPS: A *Blockchain*-Based Click *Fraud* Detection and Prevention Scheme for *Online* Advertising
Bellagarda, Jagger; Abu-Mahfouz, Adnan M.	Connect2NFT A Web-Based, *Blockchain* Enabled NFT Application with the Aim of Reducing *Fraud* and Ensuring Authenticated Social, Non-Human Verified Digital Identity
Ashfaq, Tehreem; Khalid, Rabiya; Yahaya, Adamu Sani; Aslam, Sheraz; Azar, Ahmad Taher; Alsafari, Safa; Hameed, Ibrahim A.	A Machine Learning and *Blockchain* Based Efficient *Fraud* Detection Mechanism

Penerapan teknologi *blockchain* dalam sektor keuangan telah membuka peluang baru dalam pencegahan dan deteksi penipuan. Dengan sifatnya yang desentralisasi, transparan, dan tidak dapat diubah,

blockchain menawarkan keamanan tambahan yang signifikan. Teknologi ini memungkinkan analisis data transaksi secara real-time untuk mendeteksi pola mencurigakan yang dapat mengindikasikan aktivitas penipuan, seperti double spending dan transaksi yang mencurigakan (Ahmed & Alabi, 2024).

Integrasi *blockchain* dengan machine learning lebih lanjut meningkatkan efisiensi deteksi penipuan. Algoritma machine learning dapat digunakan untuk mengidentifikasi pola transaksi yang abnormal, termasuk akun palsu atau transaksi bernilai besar yang mencurigakan (Lyu et al., 2022). Kemampuan ini membuat *blockchain* menjadi lebih cerdas dan proaktif dalam melindungi integritas transaksi keuangan.

Selain itu, federated learning (FL), yang terintegrasi dengan *blockchain*, menawarkan solusi inovatif untuk menjaga privasi data sambil meningkatkan akurasi model deteksi penipuan. FL memungkinkan pelatihan model tanpa mengorbankan privasi data pengguna, yang memberikan keamanan lebih pada sistem anti-penipuan terdistribusi (Mapa Mudiyanselage et al., 2023).

Dalam konteks periklanan *online*, *blockchain* juga terbukti efektif dalam mencegah click *fraud*. Penipuan ini, di mana klik palsu digunakan untuk meningkatkan biaya iklan secara tidak sah, dapat diminimalkan dengan transparansi yang ditawarkan oleh *blockchain*. Dengan mencatat setiap klik pada jaringan yang terdesentralisasi, pengiklan dapat dengan

mudah mengidentifikasi aktivitas mencurigakan, melindungi anggaran iklan mereka dari manipulasi (Pranto et al., 2022).

Tidak hanya itu, *blockchain* juga memiliki potensi besar dalam pengelolaan identitas digital. Dengan menawarkan sistem yang aman dan transparan, teknologi ini memastikan keaslian dan privasi identitas digital pengguna. Aplikasi *blockchain* dalam pengamanan identitas digital meluas ke berbagai sektor seperti pendidikan, kesehatan, dan keuangan, memberikan solusi yang lebih kuat terhadap ancaman manipulasi data (Bellagarda & Abu-Mahfouz, 2022)

Dalam sistem pelaporan pelanggaran atau whistleblowing, *blockchain* memainkan peran penting dengan melindungi identitas pelapor melalui penggunaan identitas digital anonim. Hal ini menciptakan lingkungan yang lebih aman bagi pelapor untuk melaporkan pelanggaran tanpa rasa takut terhadap pembalasan atau intimidasi (Wei & Lee, 2024)

Penerapan algoritma Graph Neural Network (GNN) dalam *blockchain* semakin memperkuat kemampuannya untuk mendeteksi penipuan. GNN memungkinkan sistem untuk memetakan hubungan kompleks dalam data, mengidentifikasi anomali, dan mendeteksi aktivitas mencurigakan yang mungkin mengindikasikan adanya penipuan. Pendekatan ini meningkatkan kemampuan *blockchain* untuk memberikan perlindungan tambahan terhadap ancaman keamanan (Pranto et al., 2022)

Selain itu, kolaborasi *blockchain* dengan machine learning memungkinkan sistem memberikan peringatan dini terhadap aktivitas mencurigakan. Hal ini memungkinkan organisasi untuk segera mengambil tindakan pencegahan sebelum potensi kerugian berkembang menjadi masalah besar (Ahmed & Alabi, 2024). Dengan fitur ini, *blockchain* tidak hanya meningkatkan efisiensi dan keamanan tetapi juga membangun kepercayaan antara pengguna dan penyedia layanan (Lyu et al., 2022)

c. Tantangan dan Hambatan Penerapan *Blockchain* dalam Sektor Keuangan

Meskipun teknologi ini menawarkan berbagai potensi, penerapan *blockchain* juga dihadapkan pada sejumlah kendala dan tantangan. Berikut ini adalah tabel analisis jurnal yang mengidentifikasi berbagai hambatan dan tantangan yang dihadapi dalam penerapan *blockchain*.

Tabel 4. 8 Analisis Jurnal Tantangan dan hambatan yang dihadapi dalam penerapan *blockchain* dalam sektor akuntansi

Penulis	Judul
Louati, Hassen; Louati, Ali; Almekhlafi, Abdulla; ElSaka, Maha; Alharbi, Meshal; Kariri, Elham; Altherwy, Youssef N.	Adopting Artificial Intelligence to Strengthen Legal Safeguards in *Blockchain* Smart Contracts: A Strategy to Mitigate *Fraud* and Enhance Digital Transaction Security

Marjanovic, Jelena; Dalcekovic, Nikola; Sladic, Goran	*Blockchain*-based model for tracking compliance with security requirements
Li, Jia	Dynamic financial and monetary security risk assessment based on information service security assessment model and *blockchain*
Selvarajan, Shitharth; Srivastava, Gautam; Khadidos, Alaa O.; Khadidos, Adil O.; Baza, Mohamed; Alshehri, Ali; Lin, Jerry Chun-We	An artificial intelligence lightweight *blockchain* security model for security and privacy in IIoT system
Yakubu Bello Musa, Sabi'u Jamilu, Bhattarakosol Pattarasinee	*Blockchain*-based privacy and security model for transactional data in large *private* network
Lyu, Qiuyun; Li, Hao; Zhou, Renjie; Zhang, Jilin; Zhao, Nailiang; Liu, Yan	BCFDPS: A *Blockchain*-Based Click *Fraud* Detection and Prevention Scheme for *Online* Advertising

Blockchain menghadapi berbagai tantangan dan hambatan signifikan dalam penerapannya di berbagai sektor, termasuk periklanan *online*, keuangan, dan jaringan IoT. Dalam konteks deteksi dan pencegahan klik palsu pada periklanan *online*, tantangan utama meliputi biaya komunikasi yang tinggi antar *blockchain*, keterbatasan throughput,

serta tantangan dalam menjaga keamanan data yang diproses di luar *blockchain* (Lyu et al., 2022).

Pada sektor keuangan, penerapan *blockchain* dihadapkan pada masalah skalabilitas, asimetri informasi, dan tantangan regulasi hukum(Li, 2023). Selain itu, penerapan *blockchain* dalam sistem IoT menghadapi hambatan dalam memastikan privasi data dan efisiensi enkripsi serta dekripsi, terutama pada jaringan besar dengan kompleksitas tinggi (Yakubu et al., 2023). Untuk mengoptimalkan keamanan kontrak pintar dan mencegah penipuan, integrasi AI seperti *Convolutional Neural Networks* (CNNs) menawarkan solusi efektif namun menuntut optimalisasi arsitektur teknis dan kerangka hukum (Louati et al., 2024).

Hambatan interoperabilitas antar jaringan *blockchain* juga menjadi masalah dalam mengintegrasikan data pada skala global, terutama pada aplikasi seperti pengelolaan dana pensiun (Mapa Mudiyanselage et al., 2023). *Blockchain* dalam IIoT menyoroti kebutuhan akan model keamanan ringan berbasis AI untuk memastikan privasi dan keamanan, terutama dalam lingkungan dengan serangan siber tingkat tinggi (Selvarajan et al., 2023)

C. Pembahasan Analisis Data

1. Penerapan *Blockchain* Dalam Mencegah dan Mendeteksi *Fraud* Keuangan

Financial *fraud* merupakan isu serius yang dihadapi oleh berbagai pihak atau organisasi. Tindakan *fraud* ini dapat mencakup manipulasi laporan

keuangan, penggelapan aset, korupsi, hingga penipuan investasi melalui *Ponzi schemes*. Dampak dari financial *fraud* tidak hanya terbatas pada kerugian finansial tetapi juga dapat merusak reputasi dan mengurangi tingkat kepercayaan para *stakeholders*.

Blockchain adalah teknologi inovatif yang mengusung konsep desentralisasi, transparansi, dan sifatnya yang tidak dapat diubah (*immutable*), sehingga menawarkan tingkat keamanan yang luar biasa dan dianggap mampu mengurangi risiko *financial fraud*. Teknologi ini bekerja melalui sebuah *decentralized digital ledger* yang mencatat setiap transaksi secara kronologis, transparan, dan permanen. Dengan sistem *distributed ledger*, *blockchain* menghadirkan solusi baru yang mendukung transparansi, akurasi, keamanan, pelacakan, efisiensi, kecepatan, serta kemampuan untuk melakukan verifikasi data secara otomatis.

Distributed ledger (DLT) adalah salah satu elemen inti dalam teknologi *blockchain* yang memberikan keamanan, transparansi, dan keandalan tinggi, sehingga menjadi solusi yang sangat efektif dalam pencegahan dan deteksi *fraud* keuangan. *Distributed ledger* adalah buku besar digital yang terdistribusi di seluruh node dalam jaringan, di mana semua peserta memiliki salinan yang identik. Sistem ini memastikan bahwa setiap transaksi yang dicatat bersifat permanen, tidak dapat diubah, dan mudah diaudit (Mapa Mudiyanselage et al., 2023).

Secara teknis, *blockchain* mencegah penipuan melalui beberapa mekanisme utama.

a) Penyimpanan data yang terdesentralisasi

Data yang disimpan secara desentralisasi merupakan salah satu keunggulan utama *blockchain* dalam mencegah manipulasi data. Teknologi ini beroperasi sebagai buku besar terdistribusi, di mana setiap node dalam jaringan menyimpan salinan lengkap dari seluruh data transaksi. Desain ini memastikan bahwa tidak ada satu entitas pun yang memiliki kendali penuh atas data, sehingga menciptakan sistem yang lebih aman dan transparan. Untuk dapat memanipulasi data, seorang pelaku harus menguasai mayoritas node dalam jaringan secara bersamaan, yang merupakan tugas sangat sulit dan hampir mustahil dilakukan karena skala dan struktur jaringan *blockchain* (Baabdullah et al., 2024; Mapa Mudiyanselage et al., 2023)

b) Transparansi dan ketertelusuran

Transparansi merupakan elemen kunci dalam keunggulan *blockchain* untuk mencegah dan mendeteksi *fraud*. Dalam sistem *blockchain*, setiap transaksi yang tercatat tersimpan dalam buku besar yang dapat diakses secara terbuka oleh seluruh peserta jaringan. Transparansi ini memungkinkan semua pihak untuk melacak dan memverifikasi seluruh riwayat transaksi dengan akurat, sehingga mempermudah deteksi terhadap upaya penipuan atau aktivitas mencurigakan (Mohammed et al., 2023). Keunggulan ini mengurangi risiko manipulasi data secara tersembunyi karena semua perubahan atau transaksi baru dapat dilihat oleh seluruh peserta jaringan. Dengan sistem

ini, *blockchain* menciptakan lingkungan di mana integritas data terjaga dan tindakan manipulatif menjadi sulit untuk dilakukan tanpa terdeteksi (Baabdullah et al., 2024).

c) Keamanan dan Ketidakberubahan

Blockchain didukung oleh penerapan teknik kriptografi yang canggih, menjadikannya salah satu teknologi yang paling andal dalam mencegah manipulasi data. Setiap blok dalam *blockchain* terhubung dengan blok sebelumnya melalui hash kriptografi, menciptakan struktur data yang saling terkait. Mekanisme ini memastikan bahwa data dalam satu blok tidak dapat diubah tanpa memengaruhi semua blok berikutnya dalam rantai. Untuk melakukan perubahan semacam itu, pelaku membutuhkan konsensus dari mayoritas jaringan, yang secara praktis sangat sulit dicapai. Proses ini memberikan lapisan keamanan tambahan yang melindungi data dari upaya manipulasi (Mapa Mudiyanselage et al., 2023).

Keunggulan dari *blockchain* adalah mekanisme konsensus yang digunakan untuk memvalidasi transaksi. Sebelum transaksi dicatat dalam *blockchain*, mayoritas node harus menyetujui validitasnya. Mekanisme ini secara efektif mencegah tindakan seperti pengeluaran ganda, di mana aset digital yang sama digunakan lebih dari sekali.

d) Penerapan kontrak cerdas *(smart contracts)*

Memungkinkan otomatisasi proses verifikasi dan pelaksanaan transaksi. Kontrak cerdas ini dapat diprogram untuk mendeteksi pola

anomali atau aktivitas mencurigakan, sehingga meningkatkan efisiensi sekaligus mengurangi kesalahan manusia dalam mendeteksi penipuan (Pranto et al., 2022).

Smart contract adalah protokol komputer yang berjalan secara otomatis ketika kondisi tertentu terpenuhi, sehingga memungkinkan proses transaksi yang efisien, aman, dan transparan (Mapa Mudiyanselage et al., 2023). Dalam pencegahan *fraud*, *smart contract* berfungsi untuk mengotomatisasi proses verifikasi dan pelaksanaan transaksi, seperti memastikan bahwa pembayaran hanya dilakukan jika semua persyaratan yang telah ditentukan terpenuhi. Dengan otomatisasi ini, risiko kesalahan manual atau manipulasi oleh pihak ketiga dapat diminimalkan (Pranto et al., 2022). Selain itu, teknologi *blockchain* yang mendukung smart contract memungkinkan deteksi pola anomali atau aktivitas mencurigakan dalam transaksi keuangan secara real-time, mengurangi peluang terjadinya penipuan dan meningkatkan efisiensi sistem (Ashfaq et al., 2022).

Desentralisasi juga menjadi fondasi utama yang menunjukkan keunggulan dari teknologi *blockchain*. Pada *blockchain network*, kendali atas data tidak berada di tangan satu pihak saja, sehingga meminimalkan kemungkinan manipulasi oleh otoritas yang bersifat terpusat (Ashfaq et al., 2022). Transparansi jaringan memungkinkan semua pihak untuk memverifikasi keabsahan transaksi langsung dari buku besar publik, sehingga peluang terjadinya *fraud* semakin kecil. Selain itu, sifat anti-rusak dari data dalam *blockchain* memberikan perlindungan ekstra terhadap manipulasi

karena setiap perubahan membutuhkan persetujuan mayoritas jaringan (Lyu et al., 2022).

Penerapan *blockchain* untuk mencegah dan mendeteksi *fraud* keuangan melibatkan penggunaan teknologi terdesentralisasi, transparan dan *immutable* untuk menjaga integritas data transaksi. Setiap transaksi direkam dalam *blocks* yang saling terhubung secara kronologis, menjadikannya sulit untuk diubah tanpa terdeteksi. Struktur ini memastikan integritas data, karena modifikasi apa pun memerlukan konsensus dari mayoritas *nodes* dalam jaringan. Selain itu, integrasi *blockchain* dengan algoritma pembelajaran mesin memungkinkan analisis pola serta deteksi anomali yang mengindikasikan aktivitas penipuan. Melalui analisis data transaksi secara otomatis dan mendalam, sistem ini dapat mendeteksi transaksi mencurigakan dan memverifikasi keabsahannya sebelum diproses, sehingga meningkatkan keamanan dan keandalan sistem keuangan berbasis *blockchain* (Mohammed et al., 2023).

Blockchain memainkan peranan penting dalam sektor keuangan dengan menawarkan peningkatan transparansi dan kepercayaan, pengurangan biaya transaksi, percepatan proses, serta peningkatan keamanan data dan transaksi. Selain itu, teknologi ini mampu mencegah dan mendeteksi penipuan, memfasilitasi inklusi keuangan, memungkinkan implementasi *smart contracts*, mengelola aset digital dan tokenisasi, mengoptimalkan kepatuhan terhadap regulasi, serta mengurangi risiko sistemik. Dengan mengintegrasikan aspek transparansi, keamanan, desentralisasi, dan privasi, *blockchain* menyediakan

fondasi kokoh untuk menciptakan sistem anti-penipuan yang lebih efisien dan terpercaya.

Dalam konteks pencegahan *fraud* keuangan, *blockchain* membangun lingkungan transaksi yang aman dan dapat dipercaya. Salah satu keunggulan utamanya adalah kemampuan untuk memverifikasi identitas dan validitas transaksi secara kolektif melalui konsensus mayoritas node dalam jaringan. Proses ini membuat manipulasi data hampir mustahil dilakukan tanpa terdeteksi(Pranto et al., 2022). Misalnya, dalam sektor asuransi, *blockchain* efektif mencegah praktik penipuan seperti *double-dipping* di mana satu klaim diajukan lebih dari sekali untuk kejadian yang sama karena setiap transaksi terekam secara permanen dan tidak dapat diubah.

Beberapa studi yang telah dikumpulkan oleh peneliti mendukung pernyataan ini, seperti penelitian yang dilakukan oleh (Mapa Mudiyanselage et al., 2023) yang menunjukkan bahwa *blockchain* dapat memastikan kontribusi pemberi kerja tercatat dengan benar dan diverifikasi oleh karyawan maupun otoritas seperti *Australian Taxation Office* (ATO), sehingga membantu mendeteksi kontribusi yang belum dibayarkan dan memungkinkan tindakan korektif. Dalam konteks pengelolaan dana, smart contract memastikan transfer dana hanya terjadi jika kondisi tertentu terpenuhi, seperti dalam pengelolaan dana pensiun, yang secara signifikan mengurangi risiko kecurangan dan meningkatkan efisiensi. Selain itu, desentralisasi *blockchain* mendorong pengambilan keputusan yang lebih terdistribusi, sehingga perusahaan dapat mengadopsi struktur organisasi yang lebih datar, meningkatkan responsivitas

terhadap perubahan, serta mendorong inovasi di berbagai tingkat organisasi (Bellagarda & Abu-Mahfouz, 2022). Penggunaan kredensial yang dapat diverifikasi juga memperkuat keaslian identitas dan transaksi, meningkatkan kepercayaan dan keamanan dalam operasional bisnis.

Penerapan teknologi *blockchain* dalam sektor keuangan telah membuka peluang baru dalam pencegahan dan deteksi penipuan. Dengan sifatnya yang desentralisasi, transparan, dan tidak dapat diubah (*immutable*), *blockchain* menawarkan tingkat keamanan tambahan yang signifikan. Teknologi ini memungkinkan analisis data transaksi secara real-time untuk mengidentifikasi pola mencurigakan, seperti *double spending* dan aktivitas transaksi yang tidak biasa, yang dapat mengindikasikan potensi penipuan. Penelitian oleh Ahmed & Alabi, (2024) mendukung hal ini dengan menyatakan bahwa kemampuan *blockchain* dalam menganalisis data *secara real-time* memungkinkan deteksi dini terhadap pola-pola mencurigakan, sehingga dapat mencegah terjadinya *fraud* keuangan.

Blockchain berperan penting dalam mencegah dan mendeteksi *fraud* keuangan melalui penerapan mekanisme desentralisasi. Mekanisme ini memungkinkan data transaksi disimpan di berbagai node dalam jaringan, sehingga tidak terpusat pada satu server atau otoritas tunggal. Keunggulan utama desentralisasi adalah mengurangi risiko titik kegagalan tunggal (*single point of failure*) yang sering menjadi celah dalam sistem sentralisasi (Mapa Mudiyanselage et al., 2023).

Berbeda dengan mekanisme sentralisasi yang umum digunakan, di mana seluruh data dikendalikan oleh satu entitas atau server, mekanisme *desentralisasi blockchain* memastikan bahwa setiap transaksi divalidasi oleh konsensus jaringan. Hal ini membuat data lebih aman dari risiko manipulasi, peretasan, atau kesalahan manusia. Selain itu, sifat transparan dari *blockchain* memungkinkan semua pihak terkait untuk memverifikasi transaksi secara langsung, mengurangi peluang terjadinya penipuan atau penyembunyian data. Berikut table yang menunjukkan perbedaan antara sistem sentralisasi dan desentralisasi (Bashir, 2023; Singhal et al., 2018):

Tabel 4. 9 Perbedaan Sistem Sentralisasi dan Desentralisasi

Aspek	Sistem Sentralisasi	Sistem Desentralisasi
Kepercayaan	Bergantung pada satu entitas atau pihak ketiga untuk pengelolaan dan pengawasan data.	Tidak memerlukan kepercayaan terhadap pihak ketiga; kepercayaan dibangun secara otomatis.
Keamanan	Rentan terhadap serangan karena memiliki satu titik kegagalan utama (*single point of failure*).	Lebih tahan terhadap serangan karena data tersebar di berbagai node
Privasi	Privasi sering terancam, termasuk potensi penyalahgunaan atau penjualan data pengguna.	Privasi lebih terlindungi karena data didistribusikan dan sulit diakses tanpa izin.
Biaya dan Waktu	Memerlukan biaya tinggi untuk infrastruktur, pemeliharaan, dan proses transaksi lambat.	Biaya lebih rendah karena eliminasi perantara, dan transaksi lebih cepat.
Verivikasi Transaksi	Bergantung pada satu entitas untuk memverifikasi transaksi, sehingga lebih rentan terhadap kesalahan atau manipulasi.	Verifikasi lebih mudah, cepat, dan asli karena menggunakan konsensus di jaringan.

Trasparansi	Transparansi terbatas karena akses data dikontrol oleh entitas pusat.	Transparansi tinggi karena data tersedia di seluruh jaringan dan dapat dilihat oleh semua node.
Sifat Sistem	Terpusat, rentan terhadap modifikasi atau manipulasi data oleh pihak yang berwenang.	Terdesentralisasi, tidak dapat diubah, sehingga lebih andal untuk pencatatan data permanen.

Tabel tersebut menunjukkan perbedaan yang signifikan antara sistem sentralisasi dan desentralisasi, khususnya dalam konteks sistem anti-*fraud*. Sistem desentralisasi terbukti lebih efektif dalam meminimalkan kemungkinan terjadinya *fraud* keuangan, seperti korupsi, manipulasi aset, dan kecurangan dalam laporan keuangan.

Blockchain merupakan teknologi yang dapat digunakan untuk memantau pola transaksi keuangan melalui penyimpanan data dalam blok-blok yang saling terhubung menggunakan hash kriptografi. Mekanisme ini memastikan keamanan dan integritas data secara menyeluruh. Dengan teknik kriptografi seperti *Secure Multi-Party Computation* (SMPC), keamanan dalam pertukaran data dapat lebih dijamin. Ketika digabungkan dengan teknologi *blockchain* dan *federated learning* (FL), terbentuk kerangka kerja yang kuat untuk mencegah dan mendeteksi penipuan keuangan sambil tetap menjaga privasi serta keamanan data. *Blockchain* juga mendukung pengembangan sistem peringatan dini yang efektif dalam mencegah penipuan. Dengan kemampuan mencatat setiap transaksi secara transparan dan permanen, sistem ini dapat menganalisis data secara *real-time* untuk mendeteksi pola atau anomali mencurigakan yang menjadi indikasi aktivitas penipuan (Ahmed & Alabi, 2024).

Blockchain memanfaatkan *consensus mechanisms* seperti *Proof of Work (PoW) atau Proof of Stake (PoS)* untuk memverifikasi transaksi. Proses ini memastikan bahwa hanya transaksi yang valid dapat tercatat dalam jaringan, sehingga mengurangi kemungkinan terjadinya kecurangan secara drastis. (Baabdullah et al., 2024). Selain itu, dengan memanfaatkan algoritma analisis data canggih, *blockchain* mampu mengenali pola transaksi yang tidak wajar, yang mungkin menandakan adanya aktivitas penipuan. Kemampuan deteksi dini ini memungkinkan respons cepat terhadap ancaman, sehingga dapat mencegah potensi kerugian yang lebih besar (Bellagarda & Abu-Mahfouz, 2022).

Blockchain juga memungkinkan pengembangan sistem peringatan dini yang efektif untuk mencegah *fraud*. Dengan mencatat setiap transaksi secara transparan dan permanen, teknologi ini memungkinkan analisis data secara real-time untuk mendeteksi pola atau anomali yang mencurigakan (Ahmed & Alabi, 2024). Saat ini, teknologi canggih semakin banyak digunakan untuk mendeteksi pola dan anomali dalam data transaksi. Salah satu pendekatan yang efektif adalah penggunaan *Graph Neural Network* (GNN), yang dirancang untuk mengidentifikasi hubungan kompleks dalam jaringan keuangan yang sangat besar. GNN bekerja dengan menggabungkan informasi dari node-node tetangga dan menyebarkan fitur melalui lapisan-lapisan jaringan. Pendekatan ini memungkinkan model untuk mengenali perilaku yang tidak biasa dan potensi penipuan, yang dapat beradaptasi dengan bentuk penipuan yang terus berkembang. Dengan kemampuan analisis yang mendalam terhadap pola

transaksi, GNN memberikan solusi yang lebih inovatif dibandingkan metode deteksi tradisional yang sering bergantung pada data historis atau informasi pribadi (Wei & Lee, 2024).

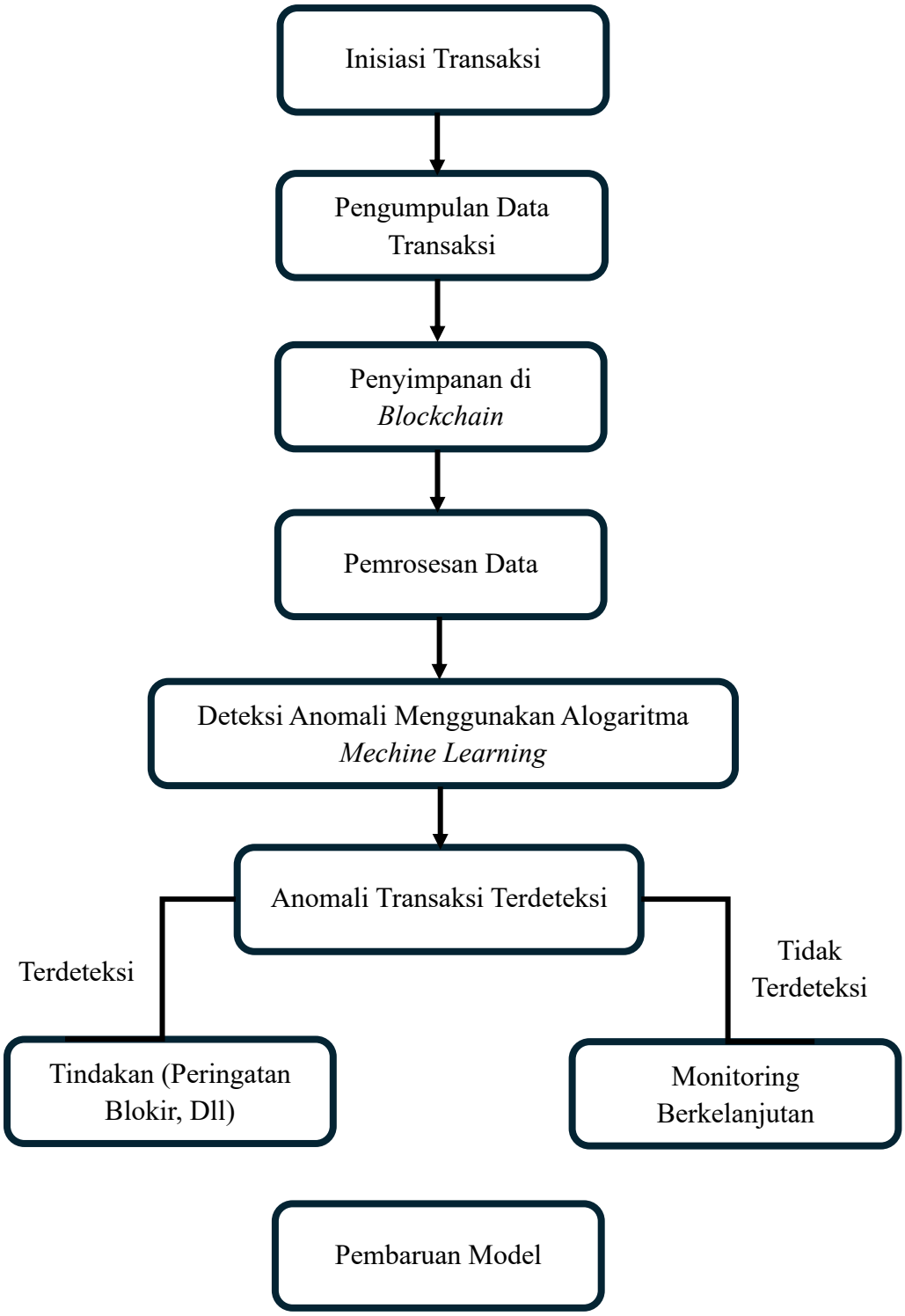
Dalam hal deteksi *fraud* keuangan, *blockchain* menawarkan kemampuan untuk memverifikasi transaksi secara real-time. Teknologi ini memungkinkan sistem untuk dengan cepat mendeteksi pola transaksi yang mencurigakan dan memberikan peringatan dini terkait potensi penipuan. Selain itu, semua transaksi yang tercatat secara permanen dalam *blockchain* dapat dilacak dan diaudit dengan mudah (Bellagarda & Abu-Mahfouz, 2022). Kemampuan ini mempermudah identifikasi aktivitas yang tidak biasa atau mencurigakan, yang sering menjadi indikator awal adanya kecurangan. Analisis pola transaksi juga menjadi fitur utama dalam mendeteksi potensi *fraud* (Lyu et al., 2022)

Penggunaan *Federated Learning* (FL) memberikan pendekatan inovatif dalam pelatihan model pembelajaran mesin secara kolaboratif tanpa membagikan data pribadi, yang membantu menjaga privasi data (Ahmed & Alabi, 2024). Dengan FL, model dapat dilatih secara lokal di berbagai node, seperti di bank, tanpa perlu berbagi data mentah. Pendekatan ini memungkinkan model global untuk mendeteksi anomali atau aktivitas mencurigakan lebih efektif karena dapat mempelajari pola transaksi yang lebih luas tanpa melanggar kerahasiaan informasi (Baabdullah et al., 2024). Selain itu, teknologi pembelajaran mesin (*machine learning*) dan pembelajaran mendalam (*deep learning*) memainkan peran penting dalam mendeteksi penipuan dengan lebih akurat dan andal. Pembelajaran mendalam sangat

efisien dalam mengenali pola transaksi yang rumit, jauh lebih efektif dibandingkan dengan teknik konvensional (Wei & Lee, 2024).

Algoritma pembelajaran mesin dapat mengidentifikasi pola penipuan yang kompleks, memberikan keunggulan dibandingkan sistem tradisional yang sering kali memiliki keterbatasan dalam hal akses data lintas organisasi(Pranto et al., 2022). Berikut adalah penjelasan mengenai langkah-langkah penggunaan *blockchain* dan algoritma pembelajaran mesin untuk mendeteksi anomali dalam sistem keuangan:

Langkah deteksi Anomali



Berikut penjabaran narasi dari gambar diatas:

a. Pengumpulan Data Transaksi

Data transaksi dikumpulkan dari berbagai sumber seperti bank atau aplikasi pembayaran untuk memastikan data yang lengkap dan akurat.

b. Penyimpanan di *Blockchain*

Setelah data terkumpul, data tersebut disimpan di *blockchain*. *Blockchain* bertindak seperti buku catatan digital yang aman dan tidak bisa diubah, memastikan data tetap aman dan dapat dipercaya.

c. Pemrosesan Data

Data yang sudah disimpan di *blockchain* kemudian diproses untuk memastikan kualitasnya baik dan siap digunakan untuk analisis lebih lanjut.

d. Penetapan Alogaritma *Machine Learning*

Setelah data siap, algoritma pembelajaran mesin digunakan untuk menganalisis pola transaksi, baik yang normal maupun yang tidak biasa. Algoritma ini belajar dari data sebelumnya untuk memahami transaksi yang normal.

e. Deteksi Anomali

Algoritma yang sudah dilatih digunakan untuk mendeteksi anomali atau transaksi yang mencurigakan, seperti transaksi besar yang terjadi di luar jam kerja normal.

f. Tindakan saat Anomali Terdeteksi

Jika ada transaksi yang mencurigakan, sistem akan memberi peringatan kepada pihak terkait atau langsung memblokir transaksi tersebut agar tidak terjadi kerugian lebih lanjut.

g. Pembaruan Model

Model pembelajaran mesin akan terus diperbarui dengan data baru agar lebih akurat dalam mendeteksi anomali dan bisa mengikuti pola penipuan yang baru.

Teknologi *machine learning* sangat cocok dipadukan dengan *blockchain* untuk mendeteksi penipuan secara lebih efektif, memperkuat integritas sistem keuangan. *Blockchain*, dengan sifatnya yang transparan, permanen, dan tidak dapat diubah (immutability), menyediakan fondasi yang kuat untuk membangun sistem keuangan yang lebih aman dan bebas dari penipuan (Pranto et al., 2022). Integrasi ini juga memungkinkan deteksi penipuan keuangan secara *real-time*, di mana *blockchain* mencatat transaksi dan algoritma pembelajaran mesin seperti *XGBoost* serta *Random Forest* menganalisis pola transaksi untuk mendeteksi anomali atau aktivitas mencurigakan. *XGBoost*, algoritma boosting yang efisien, dan *Random Forest*, metode gabungan yang menggabungkan beberapa pohon keputusan, meningkatkan akurasi dalam mendeteksi penipuan (Ashfaq et al., 2022)

Contoh penerapan *blockchain* pada sektor keuangan antara lain seperti dalam pelacakan asal-usul aset (provenance). Misalnya, dalam industri seni atau properti, *blockchain* digunakan untuk mencatat dan memberikan label unik pada aset agar asal-usulnya dapat diverifikasi oleh pihak lain. Hal ini

mencegah pemalsuan dan memastikan keaslian aset. *blockchain* awalnya dikembangkan untuk menghilangkan peran bank dalam transaksi, dan kini teknologi ini digunakan dalam berbagai layanan keuangan, seperti transfer antarbank, pembayaran lintas negara, dan perdagangan saham. Keuntungan utama *blockchain* adalah proses yang lebih cepat, aman, efisien, dan transparan, dengan penghematan biaya yang signifikan. Di bidang pemasaran, *blockchain* dapat mengurangi penipuan dan pemborosan dalam rantai pasokan media digital, dengan memberikan transparansi yang lebih besar mengenai aliran dana dan iklan. Proyek seperti AminoPay dan Basic Attention Token sedang mengembangkan aplikasi *blockchain* untuk mempercepat pembayaran dan merestrukturisasi aliran konten antara pengiklan dan pencipta (Warburg et al., 2019b).

Blockchain juga dapat memastikan bahwa kontribusi yang dilakukan oleh pemberi kerja tercatat dengan benar dan dapat diverifikasi oleh karyawan serta otoritas terkait, seperti *Australian Taxation Office* (ATO). Teknologi ini dapat membantu mendeteksi kontribusi yang belum dibayarkan, memungkinkan karyawan dan otoritas untuk mengambil tindakan yang tepat (Mapa Mudiyanselage et al., 2023).

Kesimpulannya, *blockchain* memiliki potensi besar dalam mencegah kecurangan melalui transparansi dan keamanan data. Dengan mencatat semua transaksi secara terbuka dan tidak dapat diubah, teknologi ini mengurangi risiko penipuan. Selain itu, penggunaan alogaritma kriptografi yang kuat

memastikan data terlindungi dan sulit dimanipulasi tanpa terdeteksi, menjadikannya solusi efektif untuk menangani *financial fraud*i..

Implementasi teknologi blockchain dalam sektor keuangan memiliki potensi luar biasa untuk mengatasi enam elemen utama dalam Fraud Hexagon: Pressure (tekanan), Capability (kapabilitas), Opportunity (peluang), Rationalization (rasionalisasi), Arrogance (ego), dan Collusion (kolusi). Dengan sifatnya yang transparan, terdesentralisasi, dan tidak dapat diubah (immutable), blockchain mampu menciptakan sistem keuangan yang lebih aman, terpercaya, dan tahan terhadap risiko kecurangan.

a. Mengurangi Peluang (*Opportunity)*

   Blockchain mencatat setiap transaksi secara permanen di jaringan ledger yang tersebar di banyak node, sehingga meminimalkan risiko manipulasi data. Dengan pengawasan yang real-time dan audit otomatis, peluang untuk melakukan kecurangan menjadi jauh lebih kecil.

b. Mencegah Kolusi (*Collusion)*

   Mekanisme konsensus dalam blockchain membutuhkan persetujuan dari berbagai pihak di jaringan untuk memvalidasi transaksi, membuat kolusi antara individu atau kelompok menjadi hampir tidak mungkin dilakukan tanpa deteksi.

c. Mengatasi Tekanan (*Pressure)*

   Tekanan dapat diminimalkan dengan transparansi yang ditawarkan blockchain. Pengelolaan risiko keuangan yang lebih baik, seperti smart

contracts untuk otomatisasi pembayaran dan kepatuhan, membantu individu dan organisasi mengelola tekanan finansial dengan cara yang sah.

d. Meningkatkan akuntabilitas untuk mengurangi Rasionalisasi *(Rationalization)*

Karena blockchain menciptakan jejak audit yang tak terhapuskan, individu sulit membenarkan tindakan curang. Transparansi ini memastikan bahwa setiap langkah terekam dengan jelas, sehingga mempersempit ruang untuk rasionalisasi.

e. Membatasi Penyalahgunaan Kapabilitas (*Capability*)

Sistem blockchain dirancang dengan enkripsi kuat dan kontrol akses yang ketat. Bahkan individu dengan keahlian teknis tinggi tidak dapat mengeksploitasi sistem tanpa meninggalkan jejak yang mudah dilacak.

f. Mengontrol Ego dan Arogansi (*Arrogance)*

Blockchain menghilangkan ketergantungan pada otoritas terpusat, sehingga mengurangi dominasi individu yang merasa berada di atas hukum. Sistem berbasis smart contracts menjalankan aturan secara otomatis tanpa intervensi manusia, memastikan bahwa semua pihak diperlakukan setara.

Berdasarkan temuan penelitian ini, dapat disimpulkan bahwa *blockchain* memiliki potensi besar dalam mencegah *financial fraud* melalui platform yang aman, transparan, dan terdesentralisasi, serta fitur-fitur seperti

perlindungan anti-penipuan dan peningkatan efisiensi rantai pasokan. Namun, penelitian lebih lanjut sangat diperlukan untuk memperdalam pemahaman dan memaksimalkan manfaat *blockchain* dalam pencegahan kecurangan di sektor keuangan.

2. Tantangan dan Hambatan Penerapan *Blockchain* dalam Sektor Keuangan

Analisis terhadap artikel-artikel tersebut mengungkapkan bahwa teknologi *blockchain* memiliki potensi signifikan untuk merevolusi sistem anti-*fraud*, terutama dalam aspek keamanan, transparansi, ketidakberubahan data, dan efisiensi transaksi serta penyimpanan dokumen keuangan. Sebagian besar penelitian menyoroti manfaat *blockchain* di sektor keuangan, seperti peningkatan klasifikasi transaksi, pengurangan risiko, dan efisiensi dalam manajemen keuangan.

Tantangan dalam penerapan *blockchain* mencakup masalah skalabilitas, biaya implementasi dan operasional, kerangka hukum dan regulasi, serta integrasi dengan sistem yang telah ada.

a) Skalabilitas

Salah satu tantangan utama dalam adopsi teknologi *blockchain* adalah skalabilitas, terutama pada *blockchain* publik, yang sering kali kesulitan dalam menangani volume transaksi besar secara efisien. Seiring dengan semakin banyaknya pengguna yang bergabung dalam jaringan blockchain, kecepatan dan efisiensi jaringan dapat menurun karena tuntutan

pemrosesan dan penyimpanan data yang sangat besar, seperti yang terlihat pada Bitcoin dan Ethereum (Mapa Mudiyanselage et al., 2023; Tan-Vo et al., 2024). Keterbatasan ini muncul karena faktor-faktor seperti ukuran blok, waktu blok, dan mekanisme konsensus, yang dapat menyebabkan kemacetan dan memperlambat waktu pemrosesan transaksi (Tan-Vo et al., 2024). Masalah ini dapat memengaruhi kinerja sistem deteksi *fraud* yang efektif. Skalabilitas merupakan tantangan utama dalam implementasi *blockchain*, terutama pada *blockchain* publik, yang seringkali kesulitan memproses volume transaksi besar secara efisien. Dalam bidang akuntansi, di mana transaksi bisa sangat banyak, masalah ini dapat mengakibatkan keterlambatan dan biaya operasional yang lebih tinggi, seperti yang dibahas oleh Warburg et al., (2019).

b) Pengembangan Kerangka Hukum

Pentingnya pengembangan kerangka hukum yang tepat sangat besar untuk mendukung adopsi *blockchain*. Ketidakjelasan regulasi dapat menimbulkan ketidakpastian dan menghambat implementasi teknologi ini. Regulasi yang lemah dapat menghalangi inovasi serta menurunkan kepercayaan pelaku industri untuk beralih ke sistem *blockchain* hal tersebut juga di bahas oleh Warburg et al., (2019).

Aset berbasis *blockchain* menghadapi tantangan regulasi dan kesulitan dalam integrasi dengan sistem yang ada. Pemerintah dan bank seringkali enggan untuk beralih, mengingat biaya dan skala yang diperlukan untuk mengganti sistem lama. Kecuali jika *blockchain* dapat

membuktikan adanya penghematan biaya atau manfaat yang signifikan, sulit bagi institusi besar seperti pemerintah atau bank untuk mengadopsinya dalam waktu dekat. (Raharjo, 2022).

c) Integrasi dengan Teknologi yang ada

Menggabungkan teknologi *blockchain* dengan sistem informasi keuangan yang ada adalah tantangan besar. Banyak sistem akuntansi yang beroperasi dengan infrastruktur dan standar yang berbeda, memerlukan penyesuaian rumit agar kompatibel dan dapat berinteroperasi dengan baik. Terdapat berbagai *hambatan* dalam adopsi teknologi *blockchain*, baik dari segi organisasi maupun teknis.

Kususnya pada sistem anti *fraud* di indonesia dimana pada umumnya menggunakan sistem wisthlee blower dan pelaporan serta sistem deteksi dengan auditing secara berkala. Harus di integrasikan dengan sistem berbasis blockchain, pastinya hal tersebut tidaklah mudah dan berlu waktu yang lama untuk bisa mengoprasikan secara penuh.

Di Indonesia, sebagian besar sistem anti-*fraud* masih mengandalkan mekanisme pelaporan melalui *whistleblower* dan audit berkala sebagai metode deteksi. Mengadopsi teknologi *blockchain* untuk menggantikan atau melengkapi sistem yang sudah ada bukanlah hal yang sederhana. Integrasi tersebut memerlukan waktu yang cukup panjang untuk memastikan bahwa sistem baru dapat berfungsi secara optimal dan efisien. Tantangan ini mencakup penyesuaian infrastruktur, pelatihan sumber daya manusia, serta perubahan budaya organisasi dalam beradaptasi dengan

teknologi yang lebih canggih. Sebagai hasilnya, meskipun *blockchain* menawarkan potensi besar dalam hal keamanan dan transparansi, transisi menuju penggunaannya dalam sistem anti-*fraud* memerlukan perencanaan dan implementasi yang matang

d) Biaya Operasional

Penerapan teknologi *blockchain* membutuhkan investasi besar dalam hal infrastruktur, perangkat keras, dan perangkat lunak. Selain itu, biaya operasional yang terus-menerus juga dapat menjadi kendala, terutama bagi perusahaan kecil yang terbatas dalam hal sumber daya finansial.

Beberapa hambatan yang dihadapi dalam penerapan *blockchain* yaitu seperti kurangnya pemahaman mengenai blockchain dan serangan 51%.

a) Kurangnya Pemahaman mengenai Blockchain

Hambatan terbesar hanyalah masih kurangnya pengetahuan tentang *blockchain* dan kasus penggunaannya karena perkembangannya baru-baru ini. Sebagian besar pers populer telah mengelilingi pertumbuhan mata uang kripto khususnya *bitcoin* dan ini telah menghambat adopsi umum *blockchain* untuk penggunaan lain. Seperti yang di telah di ungkapkan oleh Raharjo, (2022), penggunaan *blockchain* yang paling umum dikenal adalah bitcoin, dan pada saat ini Perusahaan yang mengembangkan system *blockchain* mencoba untuk menjauhkan hubungan antara *bitcoin* dan *blockchain*

b) Serangan 51%

Blockchain dirancang untuk mengikuti model pemerintahan demokratis dan menghadapi masalah yang sama seperti yang dihadapi oleh demokrasi dunia nyata. Serangan 51% adalah sebuah ancaman serius dalam dunia *blockchain* di mana sebuah entitas atau kelompok berhasil menguasai lebih dari 50% kekuatan komputasi (hash rate) dalam suatu jaringan *blockchain*. Dengan mengendalikan lebih dari setengah kekuatan komputasi ini, pelaku serangan dapat memanipulasi jaringan dengan cara membatalkan transaksi yang sudah terjadi, menggandakan koin (double spending), atau bahkan menghentikan transaksi baru (Vyas Nick et al., 2022). Ini seperti memiliki suara terbanyak dalam sebuah pemungutan suara, sehingga dapat mengubah hasil akhir sesuai kehendak pelaku

Dengan penelitian lebih lanjut dan penanganan terhadap tantangan serta hambatan yang ada, penerapan blockchain dalam akuntansi dapat memberikan manfaat yang signifikan bagi perusahaan dan profesional akuntansi yang mencari manajemen keuangan yang lebih aman dan efisien. Implementasi blockchain juga berpotensi untuk mengatasi berbagai kendala dan tantangan di sektor keuangan.