ANALISIS TEKNOLOGI BLOCKCHAIN PADA CYBERSECURITY DI BIDANG AKUNTANSI: SISTEMATIK LITERATUR REVIEW

ANALYSIS OF BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY IN THE FIELD OF ACCOUNTING: SYSTEMATIC LITERATURE REVIEW

Yulianissa Alvina
Universitas Andalas
2220532001_yulianissa@student.unand.ac.id

Wiska Sridayanti
Universitas Andalas
2220532006_wiska@student.unand.ac.id

Nabila Azzahra
Universitas Andalas
1910532042_nabila@student.unand.ac.id

Abstract

In the digital era, cybersecurity has become a primary focus due to increasingly complex threats. Blockchain technology, promising high levels of security, has garnered attention in the field of cybersecurity and opened up new opportunities in the world of accounting. However, the success of blockchain-based accounting practices also raises concerns related to overall security. This research utilizes a Systematic Literature Review (SLR) to understand the integration of blockchain in safeguarding data security, particularly in the context of accounting. The research findings indicate that the Internet of Things (IoT) is a primary focus within the theme of blockchain in cybersecurity, with a positive impact on the efficiency and accuracy of financial data management. However, vulnerabilities to Distributed Denial of Service (DDoS) and Sybil Attacks in blockchain technology underscore the need for innovation in developing more robust security solutions in the field of accounting. Therefore, the implications of this research are to support the development of proactive blockchain security solutions against dynamic cyber threats, ensuring the integrity of financial data and the sustainability of company operations in an increasingly advanced digital era.
Keywords: Blockchain, Cybersecurity, Accounting

Abstrak

Dalam era digital, keamanan *cybersecurity* menjadi fokus utama dengan ancaman yang semakin kompleks. Teknologi *blockchain*, yang menjanjikan tingkat keamanan tinggi, menarik perhatian di bidang *cybersecurity* dan membuka peluang baru di dunia akuntansi. Namun, keberhasilan praktik akuntansi berbasis *blockchain* juga menimbulkan kekhawatiran terkait keamanan secara keseluruhan. Penelitian ini menggunakan *Systematic Literature Review* (SLR) untuk memahami integrasi *blockchain* dalam menjaga keamanan data, terutama dalam konteks akuntansi. Hasil penelitian menunjukkan bahwa *internet of things* (IoT) menjadi fokus utama dalam

tema terkait *blockchai*n pada *cybersecurity,* dengan dampak positif pada efisiensi dan akurasi pengelolaan data keuangan. Namun, kerentanan terhadap *Distributed Denial of Service* (DDoS) dan *Sybil Attacks* dalam teknologi *blockchain* menunjukkan perlunya inovasi dalam mengembangkan solusi keamanan yang lebih tangguh dalam bidang akuntansi. Sehingga implikasi penelitian ini untuk mendukung pengembangan solusi keamanan *blockchain* yang proaktif terhadap ancaman siber yang dinamis, memastikan integritas data keuangan dan keberlanjutan operasional perusahaan di era digital yang semakin maju.
Kata kunci: *Blockchain, Cybersecurity*, Akuntansi

I. PENDAHULUAN

Dalam era digital yang semakin maju, keamanan *cybersecurity* menjadi fokus utama yang memerlukan perhatian khusus dari berbagai pihak, termasuk organisasi perusahaan, pemerintah, dan individu. Ancaman terhadap keamanan data dan informasi pribadi semakin kompleks, melibatkan berbagai jenis serangan seperti *malware, Distributed Denial of Service* (DDoS), serta pencurian identitas. Oleh karena itu, perlindungan terhadap data menjadi penting, dan solusi keamanan yang aman serta efektif diperlukan untuk melawan ancaman-ancaman ini.

Keamanan data dan informasi bukan hanya menjadi prioritas, melainkan juga menjadi landasan utama bagi keberlangsungan dan keberhasilan organisasi. Dalam menghadapi ancaman *cyber* yang semakin kompleks, teknologi *blockchain* menjadi solusi yang menjanjikan (Rifki Kautsar, 2023). Beberapa tahun terakhir, *blockchain* mendapatkan perhatian signifikan di bidang *cybersecurity* karena kemampuannya menyediakan tingkat keamanan yang tinggi untuk penyimpanan data dan transaksi. Taylor et al. (2020) menunjukkan bahwa teknologi *blockchain* terus berkembang dan mengalami perbaikan serta memberikan kontribusi pada keamanan dan efisiensi, terutama dalam aplikasi *cybersecurity*.

Kemajuan teknologi *blockchain* membuka peluang bagi profesi akuntansi untuk berkembang lebih jauh. Dalam evolusinya, praktik akuntansi berbasis *blockchain* menjadi pilihan yang menjanjikan di masa depan yang membentuk pondasi untuk sistem informasi bisnis yang inovatif (Demirkan et al., 2020). Karmańska (2021) menunjukkan bahwa adopsi *Internet of Things* (IoT) dapat meningkatkan analisis pelaporan dalam praktik akuntansi berbasis *blockchain*. Namun, seiring dengan keberhasilan praktik akuntansi berbasis *blockchain,* muncul kekhawatiran terkait *cybersecurity* secara keseluruhan.

Beberapa peneliti melakukan studi mengenai teknologi *blockchain* dan *cybersecurity* menggunakan *Systematic Literature Review (SLR)*. Taylor et al. (2020) memberikan fokus pada penggunaan teknologi *blockchain* sebagai pendukung aplikasi *cybersecurity*. Sedangkan, Prakash et al. (2022) menggali pengetahuan yang mungkin tidak dapat diakses secara efisien tanpa penggunaan komputasi. Namun, perhatian khusus diberikan pada penelitian yang menunjukkan risiko dan kelemahan di lingkungan digital, serta upaya penanggulangannya melalui penerapan teknologi *blockchain*. Meskipun demikian, *SLR* mengenai teknologi *blockchain* dan *cybersecurity* masih terbatas khususnya dalam praktik akuntansi.

Artikel ini menggunakan dua pertanyaan penelitian Taylor et al. (2020) dan menambahkan dua pertanyaan penelitian dari Prakash et al. (2022), yang ditunjukkan pada Tabel 1 berikut:

Tabel 1
Pertanyaan penelitian yang diajukan untuk penelitian ini.

Pertanyaan Penelitian	Deskripsi
RQ1	Apa aplikasi *blockchain* terbaru yang berfokus pada keamanan?
RQ2	Bagaimana *blockchain* digunakan untuk meningkatkan *Cybersecurity*?
RQ3	Apa jenis utama ancaman siber yang sangat rentan terhadap

Pertanyaan Penelitian	Deskripsi
	jaringan *blockchain?*
RQ4	Bagaimana kerentanan keamanan dan penelitian sebelumnya dapat berguna bagi penelitian selanjutnya dalam melindungi jaringan *blockchain* yang ada dan yang akan datang?

Melalui latar belakang tersebut, penelitian bertujuan untuk mengetahui bagaimana memberikan pemahaman yang jelas dan lengkap mengenai betapa pentingnya integrasi teknologi *blockchain* dalam menjaga keamanan data, khususnya dalam konteks dunia akuntansi, di tengah ancaman siber yang semakin kompleks.

II. OBJEK DAN METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan *Systematic Literature Review* (SLR). Penelitian ini menggunakan artikel yang relevan dengan objek penelitian yaitu ancaman serta kerentanan di dunia maya dalam aplikasi *blockchain*. Sebelum melakukan analisis, peneliti memulai dengan melakukan perancangan tinjauan dengan mengikuti tinjauan sistematis yang diusulkan oleh Snyder (2019) yaitu, untuk setiap langkah tinjauan literatur yang dilakukan, peneliti memastikan terlebih dahulu seperti apa informasi yang harus disertakan ke dalam tinjauan, jenis informasi seperti apa yang dibutuhkan untuk melakukan analisis secara spesifik, dan apakah nantinya kontribusi yang dihasilkan dari tinjauan ini akan dikomunikasikan dengan dengan jelas.

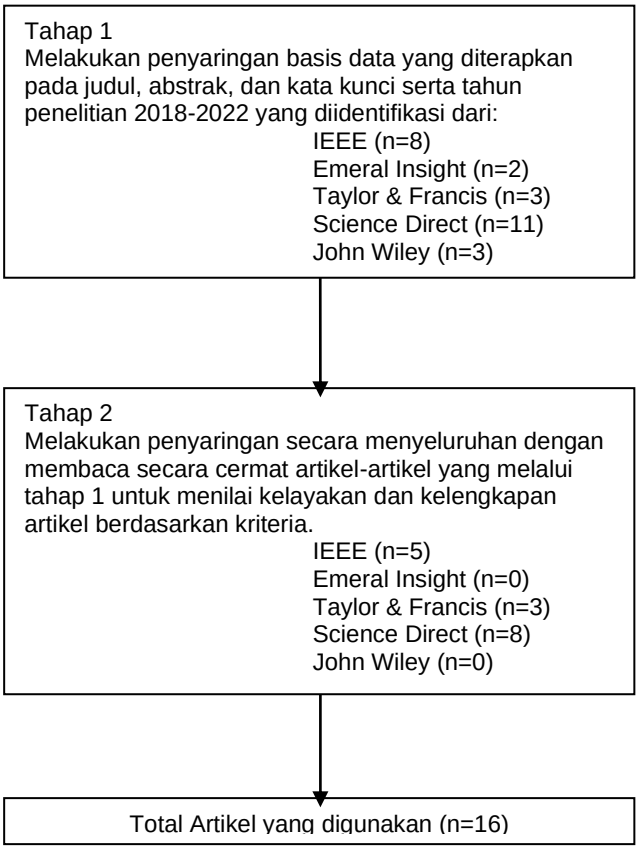
Untuk menjaga kedalaman penelitian, peneliti menggunakan strategi pencarian yang luas dan teliti untuk mengidentifikasi artikel yang relevan. Selain itu, peneliti melakukan evaluasi kritis terhadap metodologi dan temuan yang disajikan dalam setiap artikel yang dipilih, memastikan ketelitian analisis dalam memahami ancaman dan kerentanan di dunia maya dalam *blockchain*. Kemudian peneliti melakukan langkah-langkah tambahan seperti analisis tematik untuk mengidentifikasi pola dan tren dalam literatur yang dipilih. Peneliti juga mempertimbangkan publikasi dari berbagai sumber dan periode waktu untuk memastikan keragaman dan representasi yang seimbang. Selain itu, peneliti melakukan verifikasi silang antara penelitian untuk memperkuat keabsahan temuan. Dengan demikian, tinjauan ini menggambarkan pendekatan yang komprehensif dan mendalam dalam memahami ancaman dan kerentanan dalam konteks *lockchain*.

Peneliti kemudian menentukan kriteria pemilihan artikel. Seperti yang disarankan oleh Palmatier et al. (2018), bahwa didalam sebuah tinjauan literatur yang berkualitas harus terdapat kedalaman penelitian serta ketelitian analisis. Pencarian artikel dilakukan dengan menggunakan beberapa kata kunci seperti *"Research Article"* AND "*Blockchain*" *AND "Cybersecurity*" melalui berbagai *WebSite* jurnal online seperti *IEEE, Emerald Insight, Taylor & Francis, Sciencedirect, John Wiley*. *WebSite* jurnal online tersebut dipilih karena memiliki artikel yang sesuai dengan kriteria yang telah ditetapkan, maka dianggap memadai dengan menggunakan sumber-sumber tersebut. Artikel yang dipilih yaitu artikel yang terbit dari tahun 2018-2022 karena mengandung informasi yang lebih relevan dengan perembangan terbaru.

Tabel 2
Kriteria Pemilihan Artikel/Penelitian Terdahulu

No.	Kriteria Pemilihan Artikel
1	Artikel yang dipilih harus membahas tentang *Blockchain* dan *Cybersecurity*
2	Artikel terbit dalam jangka waktu lima tahun (2018-2022)
3	Artikel yang berbahasa Inggris
4	Artikel yang dipilih adalah jurnal memiliki metode penelitian yang

No.	Kriteria Pemilihan Artikel
	valid
5	Artikel yang dipakai berasal dari berbagai negara



Gambar 1.
Diagram Alur Pemilihan Artikel

Berdasarkan alur pemilihan artikel didapatkan total artikel yang digunakan untuk analisis sebanyak 16 artikel.

III. HASIL PENELITIAN DAN PEMBAHASAN

Analisis menyeluruh dilakukan terhadap artikel. Data kualitatif dan kuantitatif yang signifikan diekstraksi dan kemudian dirangkum secara komprehensif dalam Tabel 3 berikut.

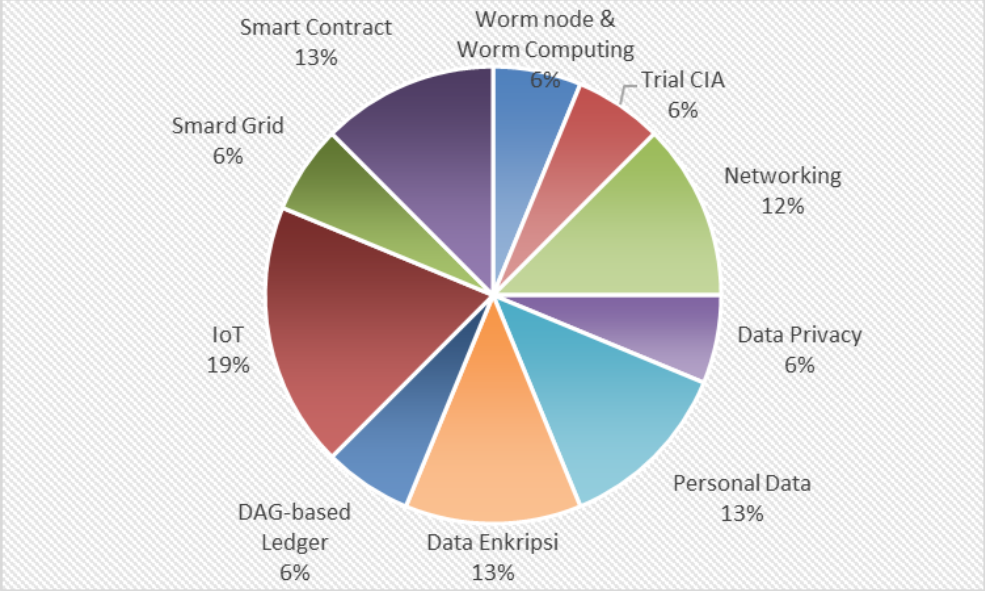
Tabel 3
Temuan Utama Dan Tema Studi Dasar

Primary Study	***Key Qualitative & Quantitative Data Reported***	***Focus/ Theme***

Primary Study	***Key Qualitative & Quantitative Data Reported***	***Focus/ Theme***
Badsha et al. (2020)	Mengusulkan privasi berbasis *blockchain* yang menjaga berbagi informasi *cybersecurity* menggunakan enkripsi ulang proxy dan enkripsi berbasis atribut (BloCyNfo-Share) dimana organisasi dapat mencapai kontrol akses yang lebih baik dengan mendelegasikan organisasi mana yang dapat memiliki akses ke organisasi tersebut.	Data Enkripsi
Wang et al. (2019)	Mengusulkan teknologi *blockchain* terbaru yang telah dimodifikasi berdasarkan metode Directed Acyclic Graph (DAG) yang terbukti dapat menghilangkan kebutuhan *node* pusat yang mana hal ini meningkatkan keamanan sistem.	*DAG-based Ledger*
Bansal et al. (2020)	Panduan mengenai arsitektur *blockchain* dan menjelaskan karakteristik, konsep, serta kebutuhan akan blockchain dalam hal keamanan dengan tujuan untuk mengimplementasikannya pada *Cyber Security, Cryptocurrency* dan *internet of things* (*IoT).* Menemukan ada kemajuan dalam *Cyber Security, Cryptocurrency* dan *IoT* yang diberikan oleh teknologi *blockchain*, karena memberikan data internet dan informasi yang aman, serta memberikan jaminan keamanan terhadap serangan siber.	*IoT*
Zhuang et al. (2021)	Menjelaskan beberapa jenis aplikasi yang dapat disusun pada lapisan DAPPS *blockchain*, yang memberikan bantuan dalam pembangunan kendali *smart grid* dengan keamanan melalui *cloud* dan otonomi.	*Smart Grid*
Zhao et al. (2018)	Merancang arsitektur baru yaitu Pub-Sub aman (SPS) yang berbeda dengan layanan pub-sub tradisional, dan Implementasi protokol yang dilakukan pada Ethereum kontrak pintar menggambarkan validitas SPS.	*Smart Contracts*
Abd El-Latif et al. (2021)	Merancang protokol *blockchain* terinspirasi kuantum diusulkan untuk menjaga privasi dan kerahasiaan dalam perangkat *internet of things* (IoT) *Smart Edge Utilities.*	*Enkripsi QIQW*
Varfolomeev et al. (2021)	Mekanisme untuk penerapan teknologi *blockchain* dalam *smart contracts* untuk meningkatkan keandalan, keamanan data, dan manfaat positif lainnya sebagai bagian dari berbagai layanan yang disediakan oleh lingkungan *smart city*.	*Smart Contracts*

Primary Study	***Key Qualitative & Quantitative Data Reported***	***Focus/ Theme***
Dehalwar et al. (2022)	Menjelaskan gambaran umum mengenai model identifikasi dan otentikasi perangkat *internet of things* (IoT) di *Smart Grid* dengan menggunakan teknologi *blockchain*.	*IoT*
Kotilevets et al. (2018)	Dengan menggabungkan *blockchain* dan grafik asiklik terarah, dimungkinkan untuk membuat jaringan yang menghilangkan kelemahan utama teknologi *blockchain* seperti kecepatan transaksi yang rendah dan masalah penskalaan.	*Networking*
Seenivasan et al. (2022)	Menyediakan model keamanan data yang memungkinkan penyimpanan data secara aman menggunakan *Fuzzy Logic.*	*Networking*
Shi et al. (2021)	Mengusulkan konsep *worm node* dan *worm computing* yang efektif dalam meningkatkan pemanfaatan sumber daya dan *cybersecurity*.	*Worm node & Worm Computing*
Suhail et al. (2022)	Mengusulkan kerangka kerja DT berbasis *blockchain* dengan *twins* terpercaya untuk mengamankan sistem *cyber* fisik (TTS-CPS). Ini membantu melacak entitas yang bertanggung jawab untuk menambahkan atau memperbarui aturan keselamatan dan keamanan (S&S) dan memastikan kepercayaan sumber penghasil data melalui ICM.	*Personal Data*
Warkentin & Orgeron (2020)	Menyajikan kerangka kerja *Trial Confidentiality, Availability, Integrity* (CIA) yang menyoroti peluan *blockchain* untuk mentransformasikan pemberian layanan publik. *Trial* CIA diintegrasikan dengan non reputasi untuk mengeksplorasi *blockchain* dan *e-government.*	*Trial CIA*
Demirkan et al. (2020)	Mempelajari penggunaan teknologi *blockchain* dan potensi teknologi *blockchain* dalam bisnis khususnya bidang akuntansi dan membahas isu terkait *cybersecurity*. *Blockchain* dapat mengintegrasikan dan menginterpretasikan *internet of things* (IoT), *Artificial Intelligence* (AI), dan teknologi baru lainnya sehingga memberikan layanan yang lebih berkualitas bagi masyarakat.	*Personal Data*

Primary Study	***Key Qualitative & Quantitative Data Reported***	***Focus/ Theme***
Dhar & Bose (2021)	Menggabungkan dua konsep *Zero Trust* dan *blockchain* untuk mengusulkan kerangka kerja holistik dalam mengamankan *internet of things* (IoT). Dimana *zero trust* ini menerapkan protokol dan kebijakan keamanan pada semua entitas jaringan, yang mana keamanan dalam jaringan IoT melibatkan data yang mengalir dari perangkat ini yang terletak di luar batas jaringan.	*IoT*
Woo (2020)	Menggunakan teknologi *blockchain* dengan metode *system dynamic* (SD) dalam meningkatkan integritas sistem pada *cybersecurity* pembangkit listrik tenaga nuklir.	*Data Privacy*



Gambar 2.
fokus atau tema terkait aplikasi *cybersecurity* menggunakan teknologi *blockchain*

Fokus masing-masing artikel dikelompokkan kedalam kategori yang lebih luas untuk memungkinkan klasifikasi tema studi utama yang disederhanakan. Studi memiliki fokus mengenai jaringan, penyimpanan terenkripsi, dan pencarian dikelompokkan ke dalam kategori penyimpanan dan berbagi data. Gambar 2 menunjukkan persentase tema berbeda dari 16 studi utama, yang membuat studi tersebut lolos penilaian kualitas untuk dimasukkan dalam analisis data.

Tema-tema yang diidentifikasi dalam artikel-artikel utama menyoroti paling banyak dari seluruh penelitian mengenai teknologi *blockchain* dalam *cybersecurity* berkaitan dengan keamanan perangkat *internet of things* (IoT). Kemudian ada

beberapa tema umum yang dibahas dalam artikel ini terkait dengan Personal data, *Trial CIA, DAG-based Ledge, Smart Grid, Smart Contracts, Fuzzy Logic* dan *Worm node & Worm Computing.*

Penggunaan *internet of things* (IoT) dalam bidang akuntansi memberikan dampak yang signifikan terhadap efisiensi dan akurasi pengelolaan data keuangan. Salah satu aspek yang dapat dioptimalkan melalui IoT adalah pemantauan aset dan inventaris perusahaan. Dengan memanfaatkan sensor IoT, perusahaan dapat mengakses informasi *real-time* tentang lokasi dan kondisi aset mereka, memberikan data yang lebih akurat untuk mencatat nilai aset di neraca (Chen et al., 2019; Karmańska, 2021). Selain itu, IoT memungkinkan otomatisasi proses bisnis dengan pengumpulan data otomatis terkait transaksi keuangan atau aktivitas operasional (Hazar & Yilmaz, 2019). Dalam pengelolaan persediaan dan rantai pasokan, sensor IoT dapat memberikan informasi real-time untuk perencanaan persediaan yang lebih baik. Keamanan transaksi keuangan juga dapat ditingkatkan melalui integrasi *blockchain,* yang sering kali digunakan bersama dengan IoT. Teknologi ini memungkinkan penyimpanan data keuangan secara terdesentralisasi dan aman, mengurangi risiko peretasan atau manipulasi data. Selain itu, penggunaan IoT dalam memantau pemakaian aset fisik seperti mesin atau kendaraan dapat meningkatkan akurasi dalam menghitung penyusutan atau amortisasi. Penerapan IoT juga mendukung proses audit dan memastikan kepatuhan terhadap regulasi keuangan melalui pelacakan otomatis transaksi dan aktivitas bisnis. Dengan demikian, integrasi IoT dalam lingkungan akuntansi membantu perusahaan untuk mengoptimalkan proses, meningkatkan akurasi data, dan merespons perubahan dengan lebih cepat, mendukung peningkatan kinerja keuangan dan manajemen risiko.

3.1 RQ1: Apa aplikasi *blockchain* terbaru yang berfokus pada keamanan?

Tujuan tinjauan literatur sistematis ini ditekankan untuk fokus hanya pada aplikasi keamanan *cyber* dari *blockchain* bukan kepada aplikasi potensial atau yang sudah tersedia seperti contohnya, layanan kesehatan maupun logistik.

Selama dilakukannya proses untuk pemilihan artikel yang akan digunakan sebagai studi utama yang melibatkan pengidentifikasian artikel yang dianggap paling relevan, dan artikel yang menyajikan bagaimana *blockchain* digunakan dalam konteks keamanan siber secara akurat dan informatif, para peneliti/peneliti mencatat bahwa fokus utama dari beberapa studi yang telah dipilih ini terletak pada bagaimana peningkatan keamanan dan efisiensi dalam berbagai aspek teknologi informasi dan komunikasi, khususnya dalam konteks *internet of things (IoT), cybersecurity*, infrastruktur energi, sistem *cyber*-fisik, dan layanan publik, dapat dilakukan dengan melakukan pengembangan dan penerapan teknologi *blockchain* pada aspek-aspek yang telah disebutkan.

Peningkatan keamanan pada *internet of things* (IoT) memiliki peluang yang cukup besar jika dilihat secara keseluruhan, beberapa studi yang dipublikasikan kebanyakan mengaitkan *blockchain* dan *cybersecurity* dengan IoT. Hal ini disebabkan oleh semakin meningkatnya penggunaan atau penerapan IoT, seperti pada kendaraan otonom, pembangunan *smart city*, rumah pintar, bahkan hingga di bidang kesehatan (Bansal et al., 2020), sehingga dibutuhkan peningkatan keamanan dalam penggunaannya.

Berikut adalah beberapa studi terbaru yang menunjukkan bahwa aplikasi blockchain yang paling berfokus terhadap keamanan:

Data Enkripsi- fokus dengan penggunaan enkripsi ulang proksi, yang mengarah pada dapat dilakukannya pembatasan akses peminta dengan tidak membuat kuci *proxy* untuk re-enkripsi, dan pada perancangan *blockchain* menggunakan protokol

otentikasi dan enkripsi baru berdasarkan *quantum walk* (QIQW) yang dapat membantu *node* IoT (Abd El-Latif et al., 2021; Badsha et al., 2020).

DAG-based Ledger- fokus pada penciptaan platform bagi pengguna yang dilakukan oleh *DAG-based Ledger*. Ini juga meningkatkan keamanan siber, selain itu model ini juga aman, terdesentralisasi, dan transparan (Wang et al., 2019).

***internet of things* (IoT)**- fokus pada penggunaan teknologi *blockchain* di jaringan IoT, yang membuat pelacakan miliaran perangkat dapat dilakukan dan kegagalan sentral tidak akan menyebabkan kegagalan di seluruh sistem. Selain itu, disini juga terdapat model identifikasi dan otentikasi perangkat IoT di *Smart Grid* dengan menggunakan teknologi *blockchain* yang berfokus pada pencegah pencurian identitas dan penyamaran. Serta adanya aplikasi *blockchain* terbaru yang digunakan dalam perangkat IoT bernama *zero trust* (Bansal et al., 2020; Dehalwar et al., 2022; Dhar & Bose, 2021).

Smart Grid- penggunaan beberapa jenis aplikasi yang disusun pada lapisan *DAPPs blockchain* membantu pembangunan kendali *Smart Grid* dan melindungi keamanan jaringan ini (Zhuang et al., 2021).

Data Pribadi/*Personal Data*- fokus pada kerahasiaan dan keandalan terhadap data data, anonimitas pelanggan serta keadilan pembayaran antara penerbit dan pelanggan, serta aplikasi *blockchain* terbaru yang menggunakan *digital twins* (DT) (Demirkan et al., 2020; Suhail et al., 2022).

Smart Contract- fokus pada penerapan teknologi *blockchain* dalam *Smart contract* yang mengarah pada pembatalan peran yang mempunyai keterkaitan dengan *broker real estate* atau pihak ketiga mana pun dan mencapai transparansi yang besar untuk proses di semua tahapannya, serta pembahasan topik2 yang berkaitan dengan teknologi *blockchain* seperti *big data* (Varfolomeev et al., 2021; Zhao et al., 2018).

Networking- *networking* dengan konteksnya yang berada dalam *blockchain,* fokusnya disini adalah mengarah kepada membuat jaringan untuk mengatasi masalah seperti kecepatan transaksi yang rendah agar dapat ditingkatkan dan masalah penskalaan dan pada implementasi logika fuzzy dalam analisis tingkat kepercayaan data yang memasuki jaringan *blockchain* (Seenivasan et al., 2022; Kotilevets et al., 2018).

Worm* node & Worm Computing- adalah sebuah *blockchain* terbaru yang fokusnya terarah pada keamanan dengan menggunakan *Worm node & worm computing* (Shi et al., 2021).

Trial Confidentiality, Availability, Integrity (CIA)- adalah aplikasi blockchain terbaru yang menyoroti peluang *blockchain* untuk mentransformasikan pemberian layanan publik (Warkentin & Orgeron, 2020).

Data Privasi- ini merupakan aplikasi *blockchain* terbaru yang digunakan dalam *cybersecurity* untuk melakukan pembuatan algoritma dengan metode *system dynamic* (SD) (Woo, 2020).

3.2 RQ2: Bagaimana blockchain digunakan untuk meningkatkan *Cybersecurity*?

Blockchain dan teknologi terkait hanya mendukung upaya yang telah dilakukan sebelumnya untuk mengamankan jaringan, komunikasi dan data. *Blockchain* menggunakan enkripsi dan hashing untuk menyimpan catatan yang tidak dapat diubah dan banyak solusi *cybersecurity* yang ada juga menggunakan teknologi yang sangat mirip. Rata-rata tindakan keamanan yang ada bergantung pada satu otoritas terpercaya untuk memverifikasi informasi atau menyimpan data terenkripsi. Sehingga membuat sistem rentan terhadap serangan dan banyak pelaku kejahatan dapat memfokuskan upaya mereka pada satu target untuk melakukan serangan penolakan layanan, menyuntikkan informasi berbahaya dan memeras data melalui pencurian atau pemerasan.

Blockchain memiliki keunggulan dibandingkan langkah-langkah keamanan saat ini karena *blockchain* yang sebenarnya terdesentralisasi dan tidak memerlukan otoritas atau kepercayaan dari masing-masing anggota grup atau jaringan. Sistem ini tidak memerlukan kepercayaan karena setiap *node*, atau anggota, memiliki salinan lengkap dari semua informasi historis yang tersedia dan hanya dengan mencapai konsensus mayoritas maka akan lebih banyak data yang ditambahkan ke rantai informasi sebelumnya. Banyak anggota dalam kelompok yang memiliki akses terhadap informasi yang sama akan mampu mengamankan kelompok tersebut jauh lebih baik daripada kelompok yang dibentuk. dari seorang pemimpin dan sekelompok anggota yang bergantung pada pemimpin tersebut untuk mendapatkan informasi, terutama ketika pelaku kejahatan bisa datang dalam bentuk anggota kelompok atau bahkan sebagai pemimpin itu sendiri.

Berdasarkan aplikasi *blockchain* yang paling berfokus pada keamanan yang diidentifikasi di RQ1, peneliti membahas bagaimana *blockchain* diterapkan untuk meningkatkan keamanan cyber di *internet of things (*IoT), Penyimpanan dan berbagi data, keamanan jaringan, data pengguna pribadi.

***internet of things (*IoT)**- metode *blockchain* (seperti *Zero trust*) diterapkan untuk menerapkan protokol dan kebijakan keamanan pada semua entitas jaringan, yang mana keamanan dalam jaringan IoT melibatkan data yang mengalir dari perangkat ini yang terletak di luar batas jaringan. Bansal et al. (2020) dan Dhar & Bose (2021) melakukannya untuk memberikan data internet dan informasi yang aman, serta memberikan jaminan keamanan terhadap serangan siber. Sedangkan, dalam penelitian Dehalwar et al. (2022) dan Zhuang et al. (2021), *blockchain* digunakan untuk mengumpulkan, menyimpan, mentransfer hingga eksekusi kontrol data di *smart grid* untuk meningkatkan keamanan dan transparansi di antara semua pemangku kepentingan.

Penyimpanan dan pembagian data - baik buku besar terdistribusi publik maupun swasta digunakan untuk menghilangkan satu sumber kegagalan dalam ekosistem penyimpanan tertentu, sehingga melindungi datanya dari gangguan. Artinya, *blockchain* membantu memastikan bahwa data yang disimpan di cloud tetap tahan terhadap perubahan yang tidak sah, daftar hash memungkinkan pencarian data yang dapat dipertahankan dan disimpan dengan aman, dan pertukaran data dapat diverifikasi sama dari pengiriman hingga penerimaan (Abd El-Latif et al., 2021; Badsha et al., 2020). Singkatnya, *blockchain* meningkatkan penyimpanan data dan keamanan privasi berbagi dengan menciptakan jaringan terdesentralisasi yang menggunakan enkripsi sisi klien di mana pemilik data akan memiliki kendali penuh atas data mereka yang dapat dilacak.

Keamanan Jaringan - sebagian besar pekerjaan dalam kategori ini menggunakan *blockchain* untuk membuat jaringan, meningkatkan kecepatan transaksi, mengukur

dan menganalisis tingkat kepercayaan data yang diunggah menggunakan *fuzzy logic* (Kotilevets et al., 2018; Seenivasan et al., 2022). Dalam penelitian tersebut perlindungan jaringan yang mendukung *blockchain* menggunakan grafik *directed acyclic* dan *fuzzy logic*. Peneliti menggunakan *blockchain* yang menggabungkan keduanya untuk membuat jaringan yang menghilangkan kelemahan *blockchain* agar mengatasi masalah jaringan pada *blockchain*.

Data pengguna pribadi – dibandingkan dengan kategori lainnya, penerapan *blockchain* untuk meningkatkan privasi data kurang dibahas dalam literatur. Alasannya mungkin karena sifat *blockchain* yang tidak dapat diubah (seperti setiap orang memiliki salinan buku besar), sehingga sulit digunakan untuk tujuan privasi, khususnya dalam perlindungan data. Dalam pendekatan Woo (2020), saat ini, preferensi perangkat pengguna pada umumnya dienkripsi dan disimpan di *blockchain* untuk hanya diambil oleh pengguna tersebut. Selain itu menggunakan metode *system dynamic (*SD) yang dilakukan dengan perhitungan berbasis *random sampling.*

3.3 RQ3: Apa jenis utama ancaman siber yang sangat rentan terhadap jaringan *blockchain*?

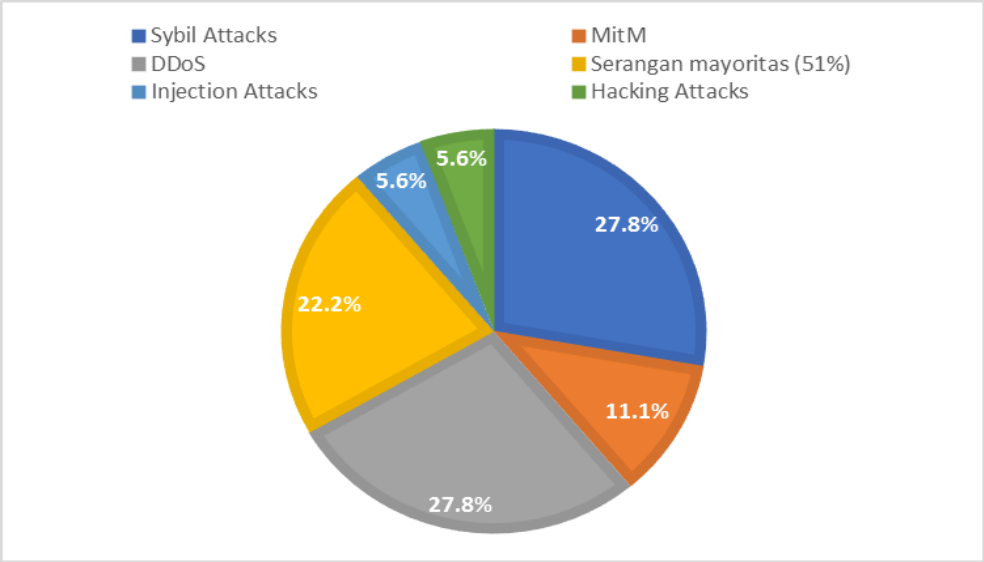
Jaringan *blockchain* sebagai fondasi teknologi terdesentralisasi, menghadapi berbagai jenis ancaman siber yang dapat membahayakan integritas, keamanan, dan kinerjanya. Dalam rentang 5 tahun terakhir terdapat beberapa jenis utama *cybersecurity* yang sangat rentan terhadap jaringan *blockchain* mencakup *Distributed Denial of Service* (DDoS), *Sybil Attacks*, Serangan mayoritas (51%), *Man-in-the-Middle* (MitM), dan Injection Attacks yang ditunjukkan pada gambar 3.

DDoS dan *Sybil Attacks* menempati posisi utama yaitu mencapai 27.8% (Dehalwar et al., 2022; Demirkan et al., 2020; Kotilevets et al., 2018; Seenivasan et al., 2022; Shi et al., 2021; Suhail et al., 2022; Wang et al., 2019; Warkentin & Orgeron, 2020; Zhuang et al., 2021). Serangan DDoS mengancam jaringan *blockchain* dengan mengalirkan lalu lintas data yang luar biasa besar, menciptakan kekacauan dan menyebabkan ketidakstabilan jaringan. Kegagalan akses yang diakibatkan oleh serangan ini dapat merugikan operasional normal dan merusak kepercayaan pengguna. Sedangkan, *Sybil Attacks* melibatkan penciptaan identitas palsu atau node palsu dalam jaringan. Penyerang mencoba memanipulasi konsensus atau membuat keputusan yang merugikan bagi jaringan dengan mengendalikan sejumlah besar identitas palsu. Dengan cara ini, integritas dan keamanan konsensus dalam jaringan dapat terancam.

Selanjutnya, serangan mayoritas (51%) mencapai 22.2% (Dhar & Bose, 2021; Kotilevets et al., 2018; Varfolomeev et al., 2021; Zhao et al., 2018). Serangan mayoritas (51%) terjadi ketika satu entitas atau kelompok entitas memegang lebih dari 50% daya komputasi total dalam jaringan *blockchain*. Dengan kontrol mayoritas, penyerang dapat mengendalikan konsensus, memodifikasi transaksi, dan bahkan menciptakan rantai ganda, mengancam keandalan dan integritas jaringan. Lebih lanjut, MitM *Attacks* mencapai 11.1%, serangan yang dilakukan dengan mengekspos kelemahan dalam komunikasi antara pihak yang berkomunikasi (Abd El-Latif et al., 2021; Bansal et al., 2020). Dalam konteks *blockchain*, penyerang dapat mencoba mencuri informasi sensitif atau memanipulasi data selama proses transmisi, mengancam keamanan data yang dipertukarkan.

Injection Attacks, dan *Hacking Attacks* berada pada urutan terakhir yaitu mencapai 5.6% (Badsha et al., 2020; Woo, 2020). *Injection Attacks*, seperti SQL *injection*, mengarah pada upaya penyerang untuk menyisipkan kode berbahaya ke dalam transaksi atau *query blockchain.* Dengan memanfaatkan celah ini, penyerang dapat mencuri data atau mengubah logika eksekusi *blockchain*. Sementara, *Hacking*

Attacks mencakup berbagai teknik untuk meretas sistem keamanan jaringan *blockchain*, dapat mencuri informasi atau merusak integritas data.



Gambar 3.
Jumlah kumulatif dari kerentanan blockchain yang berbeda

Berdasarkan hasil penelitian, ancaman siber terbesar terhadap jaringan *blockchain*, yaitu *Distributed Denial of Service* (DDoS) *attacks* dan *Sybil attacks*. Ancaman tersebut memiliki dampak signifikan terhadap keamanan dan integritas data keuangan dalam konteks akuntansi karena keduanya mengancam fondasi fundamental dari jaringan *blockchain* yang digunakan dalam sistem akuntansi. Perlindungan terhadap ancaman DDoS dan *Sybil attacks* menjadi esensial dalam merancang mekanisme keamanan yang kokoh, menjaga integritas data keuangan, dan memastikan keberlanjutan proses akuntansi dalam lingkungan yang semakin kompleks dan rentan terhadap serangan siber. Sehingga pemahaman mendalam diperlukan dalam merancang mekanisme keamanan dan mitigasi risiko yang dapat diintegrasikan ke dalam sistem akuntansi berbasis *blockchain.*

3.4 RQ4: Bagaimana kerentanan keamanan dan penelitian sebelumnya dapat berguna bagi penelitian selanjutnya dalam melindungi jaringan *blockchain* yang ada dan yang akan datang?

Kerentanan keamanan yang teridentifikasi dalam jenis utama *cybersecurity* terhadap jaringan *blockchain* memberikan wawasan yang berharga untuk arah penelitian masa depan guna meningkatkan keamanan dan keandalan jaringan *blockchain* yang ada dan yang akan datang. Setiap jenis serangan memiliki implikasi yang unik dan dapat memberikan panduan untuk fokus penelitian yang lebih mendalam.

Kerentanan terhadap *Distributed Denial of Service* (DDoS) *attacks* pada jaringan *blockchain* sebesar 27.8% menjadi fokus utama dalam penelitian *cybersecurity*. Penelitian mendatang dapat difokuskan menjadi tiga bagian. Pertama, pada pemantauan sistem transmisi daya terdistribusi, terutama pada implementasi *blockchain* dengan fungsionalitas *smart contract* yang diimplementasikan secara terdistribusi (Zhuang et al., 2021). Ini bertujuan untuk memperkuat keamanan dan kinerja sistem distribusi daya, menciptakan ekosistem yang lebih andal. Kedua, identifikasi teknik kecerdasan buatan terbaik dalam otomatisasi keamanan

penyimpanan *cloud* menjadi penting, dengan penerapan strategi replikasi yang menjanjikan untuk meningkatkan waktu pengambilan data dan ketangguhan operasional (Seenivasan et al., 2022). Ketiga, konsep *worm node* dan *worm computing* memberikan arah inovatif, dengan penelitian yang berfokus pada pengurangan konsumsi daya komputasi, optimalisasi sumber daya perangkat keras bersama, dan penerapan strategi pertahanan diri terhadap peristiwa berbahaya (Shi et al., 2021).

Kerentanan terhadap *Sybil attacks*, juga memiliki persentase 27.8%, menunjukkan pentingnya penelitian lebih lanjut untuk meningkatkan keamanan sistem. Fokus penelitian masa depan dapat terarah pada pemantauan sistem transmisi daya terdistribusi dengan implementasi *blockchain* dan *smart contracts* yang terdistribusi secara otomatis, meningkatkan efisiensi dan keandalan sistem distribusi daya (Zhuang et al., 2021). Kerentanan ini juga memicu eksplorasi pembangunan mekanisme toleransi terhadap masalah, termasuk identifikasi dan respons terhadap insiden, peningkatan ketahanan sistem, serta integrasi kontrak pintar untuk respons otomatis terhadap peristiwa berdasarkan kondisi keamanan (Suhail et al., 2022). Selain itu, kerentanan terhadap *Sybil attacks* menciptakan peluang untuk mengubah pemberian layanan publik melalui keamanan *blockchain* dan mengintegrasikan *Trial Confidentiality, Availability, Integrity* (CIA) dengan non-reputasi untuk penelitian potensi penggunaan *blockchain* dalam *e-government* (Warkentin & Orgeron, 2020). Hal ini membentuk landasan kuat untuk membangun sistem yang aman dan dapat diandalkan, menjadikan *blockchain* solusi unggul dalam mengatasi tantangan keamanan jaringan yang semakin kompleks.

Kerentanan terhadap serangan mayoritas (51%), sebesar 22.2%, menunjukkan perlunya menjaga desentralisasi dalam jaringan. Dalam menjawab tantangan ini, konsep *zero trust* pada *internet of things (*IoT) dalam jaringan *blockchain* menonjol sebagai solusi potensial (Dhar & Bose, 2021). Oleh karena itu, penelitian mendatang dapat mengeksplorasi integrasi antara *zero trust* dan teknologi *blockchain* untuk memperkuat keamanan Infrastruktur Siber (IS). Kombinasi ini memiliki potensi untuk memberikan lapisan pertahanan tambahan, meningkatkan ketahanan jaringan *blockchain* terhadap serangan 51%.

Kerentanan terhadap MitM *attacks* sebesar 11.1% menunjukkan terdapatnya peluang penelitian masa depan dengan fokus pada eksperimen berskala besar terhadap *blockchain* dengan memanfaatkan prinsip kuantum sebagai sumber inspirasi, dengan pertimbangan khusus terhadap penerapannya pada sektor kesehatan atau domain lain (Abd El-Latif et al., 2021). Eksplorasi ini dapat membuka jalan bagi pengembangan mekanisme keamanan baru yang tahan terhadap serangan MitM.

Kerentanan terhadap *Injection attacks*, dan *Hacking attacks* masing-masing sebesar 5.6%, bahwa perlindungan terhadap integritas data dan keamanan transmisi adalah aspek kritis. Penelitian masa depan dapat diarahkan pada eksplorasi kriptografi berbasis homomorfik sebagai metode analisis yang dapat membangun pertahanan siber proaktif, yang tidak hanya cepat dalam mendeteksi serangan tetapi juga aman terhadap berbagai teknik *injection attacks*, dan *hacking attacks* (Badsha et al., 2020).

Penelitian masa depan dapat memanfaatkan temuan dari penelitian sebelumnya untuk memberikan kontribusi penting dalam menghadapi tantangan *cybersecurity* dalam konteks akuntansi. Dengan memahami kelemahan dan kerentanan yang teridentifikasi, peneliti dapat merancang solusi keamanan yang lebih baik, terutama terkait dengan integritas data keuangan dan pengelolaan informasi akuntansi. Pengembangan mekanisme mitigasi yang kuat akan mendukung keamanan transaksi dan rekam jejak keuangan perusahaan, menciptakan landasan yang kokoh untuk implementasi teknologi *blockchain* yang aman dan dapat diandalkan dalam praktik akuntansi. Sehingga diharapkan dapat memberikan kontribusi signifikan dalam menjaga integritas dan keamanan data keuangan perusahaan, sekaligus

memperkuat kepercayaan dalam penerapan teknologi *blockchai*n di dunia akuntansi yang terus berkembang.

IV. KESIMPULAN DAN SARAN

Tinjauan literatur ini bertujuan untuk mengetahui bagaimana memberikan pemahaman yang jelas dan lengkap mengenai pentingnya integrasi teknologi *blockchain* dalam menjaga keamanan data, khususnya dalam konteks dunia akuntansi, di tengah ancaman siber yang semakin kompleks. Hasil penelitian menunjukkan bahwa fokus atau tema terkait teknologi *blockchain* pada c*ybersecurity* yang paling banyak digunakan adalah *internet of things (*IoT). Hal ini dikarenakan penggunaan IoT dalam akuntansi memberikan dampak positif melalui efisiensi dan akurasi pengelolaan data keuangan. Melalui sensor IoT, perusahaan dapat memantau aset secara *real-time*, meningkatkan pencatatan nilai aset. Otomatisasi proses bisnis dan integrasi *blockchain* meningkatkan efisiensi operasional dan keamanan transaksi. Sensor IoT juga mendukung perencanaan persediaan, manajemen aset fisik, dan kepatuhan regulasi sehingga memberikan kontribusi signifikan pada optimasi proses, akurasi data, dan respons cepat terhadap perubahan. Disisi lain, teknologi *blockchain* dalam *cybersecurity* menunjukkan kerentanan yang paling besar pada *Distributed Denial of Service* (DDOs) dan *Sybil Attact.* Serangan ini memiliki dampak langsung pada keamanan dan integritas data keuangan dalam akuntansi. Sehingga, implikasi selanjutnya diperlukan integrasi temuan kerentanan keamanan pada penelitian sebelumnya dengan inovasi baru untuk mengembangkan solusi keamanan *blockchain* yang lebih tangguh dan proaktif terhadap evolusi ancaman siber yang dinamis dalam akuntansi.

V. DAFTAR PUSTAKA

Abd El-Latif, A. A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S. E., & Peng, J. (2021). *Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities.* Information Processing & Management, 58(4), 102549. https://doi.org/10.1016/j.ipm.2021.102549

Badsha, S., Vakilinia, I., & Sengupta, S. (2020). *BloCyNfo-Share: Blockchain based Cybersecurity Information Sharing with Fine Grained Access Control.* In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 317–323.

Bansal, P., Panchal, R., Bassi, S., & Kumar, A. (2020). *Blockchain for Cybersecurity: A Comprehensive Survey*. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 260–265. https://doi.org/10.1109/CSNT48778.2020.9115738

Chen, T., Barbarossa, S., Wang, X., Giannakis, G. B., & Zhang, Z. L. (2019). *Learning and Management for Internet of Things: Accounting for Adaptivity and Scalability*. Proceedings of the IEEE, 107(4), 778–796. https://doi.org/10.1109/JPROC.2019.2896243

Dehalwar, V., Kolhe, M. L., Deoli, S., & Jhariya, M. K. (2022). *Blockchain-based trust management and authentication of devices in smart grid.* Cleaner Engineering and Technology, 8, 100481. https://doi.org/10.1016/j.clet.2022.100481

Demirkan, S., Demirkan, I., & McKee, A. (2020). *Blockchain technology in the future of business cyber security and accounting.* Journal of Management Analytics, 7(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

Dhar, S., & Bose, I. (2021). *Securing IoT Devices Using Zero Trust and Blockchain.* Journal of Organizational Computing and Electronic Commerce, 31(1), 18–34. https://doi.org/10.1080/10919392.2020.1831870

Hazar, H. B., & Yilmaz, N. K. (2019). *Analyzing technology acceptance for internet of things (Iot) among accounting and finance students*. Pressacademia, 8(4), 198–208. https://doi.org/10.17261/pressacademia.2019.1163

Karmańska, A. (2021). *Internet of Things in the Accounting Field Benefits And Challenges.* Operations Research and Decisions, 31(3), 23–39. https://doi.org/10.37190/ord210302

Kotilevets, I. D., Ivanova, I. A., Romanov, I. O., Magomedov, S. G., Nikonov, V. V., & Pavelev, S. A. (2018). *Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions.* IFAC-PapersOnLine, 51(30), 693–696. https://doi.org/10.1016/j.ifacol.2018.11.213

Palmatier, R. W., Houston, M. B., & Hulland, J. (2018). *Review articles: purpose, process, and structure*. In Journal of the Academy of Marketing Science,46 (1). https://doi.org/10.1007/s11747-017-0563-4

Prakash, R., Anoop, V. S., & Asharaf, S. (2022). *Blockchain technology for cybersecurity: A text mining literature analysis.* In International Journal of Information Management Data Insights, 2(2). https://doi.org/10.1016/j.jjimei.2022.100112

Rifki Kautsar, M. (2023). *Teknologi Blockchain dalam Cybersecurity*. https://www.researchgate.net/publication/370074689

Seenivasan, M., Krishnasamy, V., & Muppudathi, S. S. (2022). *Data division using Fuzzy Logic and Blockchain for data security in cyber space.* Procedia Computer Science, 215, 452–460. https://doi.org/10.1016/j.procs.2022.12.047

Shi, L., Li, X., Gao, Z., Duan, P., Liu, N., & Chen, H. (2021). *Worm computing: A blockchain-based resource sharing and cybersecurity framework.* Journal of Network and Computer Applications, 185, 103081. https://doi.org/10.1016/j.jnca.2021.103081

Snyder, H. (2019). *Literature review as a research methodology: An overview and guidelines.* Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Suhail, S., Malik, S. U. R., Jurdak, R., Hussain, R., Matulevičius, R., & Svetinovic, D. (2022). *Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins.* Computers in Industry, 141, 103699. https://doi.org/10.1016/j.compind.2022.103699

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). *A systematic literature review of blockchain cyber security.* In Digital Communications and Networks, 6(2), 147–156). https://doi.org/10.1016/j.dcan.2019.01.005

Varfolomeev, A. A., Alfarhani, L. H., & Oleiwi, Z. Ch. (2021). *Secure-reliable smart contract applications based blockchain technology in smart cities environment*.

Procedia Computer Science, 186, 669–676. https://doi.org/10.1016/j.procs.2021.04.188

Wang, B., Dabbaghjamanesh, M., Kavousi-Fard, A., & Mehraeen, S. (2019). *Cybersecurity Enhancement of Power Trading within the Networked Microgrids Based on Blockchain and Directed Acyclic Graph Approach*. IEEE Transactions on Industry Applications, 55(6), 7300–7309. https://doi.org/10.1109/TIA.2019.2919820

Warkentin, M., & Orgeron, C. (2020). *Using the security triad to assess blockchain technology in public sector applications*. International Journal of Information Management, 52, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Woo, T. H. (2020). *Cybersecurity analysis using the blockchain algorithm in nuclear power plants to enhance safe operations*. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 1–11. https://doi.org/10.1080/15567036.2020.1826011

Zhao, Y., Li, Y., Mu, Q., Yang, B., & Yu, Y. (2018). *Secure Pub-Sub: Blockchain-Based Fair Payment with Reputation for Reliable Cyber Physical Systems*. IEEE Access, 6, 12295–12303. https://doi.org/10.1109/ACCESS.2018.2799205

Zhuang, P., Zamir, T., & Liang, H. (2021). *Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey*. IEEE Transactions on Industrial Informatics, 17(1), 3–19. https://doi.org/10.1109/TII.2020.2998479