Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 4, August 2024, pp. 263-272

DOI: https://doi.org/10.52436/1.jutif.2024.5.4.2176
p-ISSN: 2723-3863
e-ISSN: 2723-3871

TECHNOLOGY TREND OF DIGITAL IDENTITY: A BIBLIOMETRIC APPROACH

Tika Riskawati[1], Muhammad Suryanegara[*2]

[1,2]Graduate Program in Telecommunication Management, Department of Electrical Engineering, Universitas Indonesia, Indonesia
Email: [1]tikariskawati@gmail.com, [2]suryanegara@gmail.com

(Article received: May 30, 2024; Revision: June 12, 2024; published: August 01, 2024)

Abstract

The future of digital ecosystem requires various supporting technologies, one of which is digital identity. A necessary validation tool not only for individuals but also for organizational institutions which later will be used in digital economic activities. Indonesia as a country with large citizen urgently needs digital identity to protect the people and to upheld national security systems. However, we need to figure out the overall development of digital identity before adopting the technology. This article conducts a bibliometric analysis to investigate the future that digital identity holds. The investigations revealed that digital identity will eventually evolve to four technologies such as decentralized identity, verifiable credentials, self-sovereign identity, and metaverse. The findings will be a catalyst for the information technology and telecommunications industry to adopt digital identity technology.

Keywords: *bibliometric analysis, digital identity, metaverse, self-sovereign identity.*

ANALISIS TREN PERKEMBANGAN TEKNOLOGI DIGITAL IDENTITY

Abstrak

Pertumbuhan ekosistem digital membutuhkan berbagai teknologi pendukung, salah satunya yaitu teknologi *digital identity*. Teknologi tersebut menjadi diperlukan sebagai alat validasi tidak hanya bagi individu tetapi juga lembaga organisasi yang nantinya digunakan dalam kegiatan ekonomi digital. Indonesia sebagai salah satu negara dengan jumlah penduduk produktif tertinggi di dunia membutuhkan *digital identity* baik untuk melindungi masyarakat digital nasional maupun untuk menegakkan tindakan hukum digital tanah air. Namun, sebelum mengadopsi sebuah teknologi perlu adanya analisis mendalam untuk mengetahui tren masa depan teknologi tersebut. Penelitian ini menggunakan analisis bibliometrik untuk mengetahui arah perkembangan teknologi *digital identity*. Berdasarkan hasil penelitian, teknologi *digital identity* akan mengarah pada teknologi *decentralized identity*, *verifiable credentials*, *self-sovereign identity* dan *metaverse*. Keempat teknologi tersebut diprediksi akan banyak digunakan pada industri teknologi informasi dan elektronik untuk membangun Web3 dan *immersive reality*. Selain itu, *self-sovereign identity* dan *metaverse* diprediksi menjadi katalis industri telekomunikasi untuk mengadopsi teknologi *digital identity*.

Kata kunci: *analisis bibliometrik, digital identity, metaverse, self-sovreign identity.*

1. PENDAHULUAN

Saat dunia diwarnai dengan ketidakpastian geopolitik, konflik, perubahan iklim, pelemahan konsumsi, penurunan penjualan dan permasalahan lainnya, ekonomi kawasan Asia justru diprediksi akan tumbuh lebih baik daripada kawasan lain di dunia. Meskipun perekonomian Beijing dikatakan akan mendapat banyak tekanan, Vietnam dan Filipina diprediksi akan tumbuh dengan cemerlang. Sedangkan India dan Indonesia diperkirakan akan menampilkan pertumbuhan yang kuat di tahun 2024. Pertumbuhan tersebut diperoleh dari perluasan kerja sama dagang, investasi hijau, serta peningkatan produksi hasil digitalisasi berbagai sektor [1]. Transformasi digital yang masif dilaksanakan sejak masa pandemi Covid-19 menjadi katalis utama pertumbuhan ekonomi di Asia. Transformasi digital turut meningkatkan konektivitas sehingga memicu aktivitas ekonomi lebih efisien [2].

Indonesia sendiri diramalkan akan memiliki ekonomi digital terbesar di kawasan Asia Tenggara jika pemerintahnya konsisten dalam mendukung investasi digital, yakni fokus membangun infrastruktur digital dalam negeri, meningkatkan keahlian tenaga kerja, serta menyusun etika dan regulasi data [1]. Infrastruktur digital tidak lepas dari peran industri telekomunikasi yang turut membangun

ekosistem pendukung, seperti operator seluler, peralatan & perlengkapan, serta konten & layanan [3]. Berkat ekosistem pendukung tersebut konektivitas seluler mampu melahirkan inovasi digital yang berperan bagi transformasi digital pemerintah, swasta, dan masyarakat [4].

Hingga tahun 2023, jumlah masyarakat yang menggunakan layanan seluler mencapai 5,6 milyar jiwa atau 69% dari jumlah total populasi dunia. Jika tingkat pertumbuhan per tahun (CAGR) mencapai 1.7% selama 2023-2030, maka jumlah pelanggan layanan seluler diprediksi bertambah menjadi 6,3 milyar jiwa atau 74% dari jumlah total populasi dunia. Sedangkan untuk jumlah pelanggan konektivitas seluler (internet seluler) pada tahun 2023 mencapai 4,7 milyar jiwa atau 58% populasi dunia. Jika nilai CAGR 2023-2030 mencapai 2,3% maka jumlah pengguna layanan internet global mencapai 5,5 milyar jiwa atau 65% dari jumlah total populasi dunia [4]. Secara global, jumlah masyarakat yang belum menggunakan layanan seluler mencapai 31% atau 2,5 milyar jiwa, dan jumlah masyarakat yang belum terkoneksi dengan internet seluler mencapai 42% atau 3,4 milyar dari total populasi dunia.

Pertumbuhan pengguna layanan dan internet seluler berperan dalam peningkatan penggunaan *smartphone* [2]. Jumlah pengguna *smartphone* pada tahun 2023 di wilayah Asia Pasifik mencapai 78% [4], jumlah tersebut berpotensi bertambah dua kali lipat hingga 2030 [5]. Pesatnya peningkatan tersebut semakin menegaskan posisi *smartphone* sebagai perangkat elektronik paling dicintai manusia. Tidak hanya digunakan sebagai alat telekomunikasi, *smartphone* juga digunakan sebagai perangkat autentifikasi [6]. Berkat jumlah pengguna *smartphone* yang hampir mencapai angka lima milyar, fungsi autentifikasi menjadi nilai penting yang dimiliki *smartphone*. Autentifikasi melalui *smartphone* akan semakin luas digunakan, menggantikan dokumen yang digunakan sebagai alat identifikasi seperti SIM, paspor, KTP, hingga kunci tembaga. *Smartphone* berfungsi sebagai alat identifikasi terhadap pengguna itu sendiri, baik di dunia nyata maupun digital [7]. Tidak hanya berfungsi sebagai alat autentifikasi, *smartphone* sebagai perangkat digital juga memiliki identitas, yakni identitas digital. Selain manusia dan perangkat elektronik, identitas digital dimiliki oleh perangkat *Internet of Things*, organisasi ataupun entitas lainnya [8].

Identitas digital diperlukan untuk membuktikan legalitas sebuah entitas yang berperan sebagai representasi individu ataupun entitas di dunia digital [9]. Konsep identitas digital muncul sebagai salah satu solusi dari permasalahan yang muncul di era ekonomi digital, yakni pencurian identitas (*identity theft*), penyalahgunaan data pribadi (fraud), dan penipuan (*scams*). *Federal Trade Commission* (FTC) mencatat jumlah laporan kasus pencurian data sebanyak 1 juta laporan atau sekitar 19% dari total laporan yang masuk pada tahun 2023 [10]. Pencurian ataupun pemalsuan identitas tercatat sebagai kasus kejahatan tertinggi, dengan presentasi mencapai 90,38% di wilayah Afrika, Asia, dan Amerika Latin [11]. Kejahatan terjadi melalui berbagai platform, 62% aplikasi seluler, 58% toko daring & halaman internet, 41% modus *customer service*, 38% dilakukan secara tatap muka langsung [12].

Menghadapi permasalahan tersebut, negara-negara di Afrika fokus membangun sistem verifikasi identitas digital, mempelajari dampak perkembangan teknologi (*Artificial Intelligence* & *Machine Learning*), mengantisipasi dampak terhadap konsumen dan bisnis, serta menyusun rencana komprehensif sebagai upaya mitigasi & preventif terhadap ancaman penipuan digital masa depan [13]. Uni Eropa menyusun regulasi *eIDAS1* [9] dan *eIDAS2* untuk mendukung pengembangan identitas digital dan autentikasi demi masa depan ekonomi digital negara-negara kawasan Uni Eropa [14]. Pemerintah Australia menyusun *the Digital ID Bill 2024* untuk memperkuat dasar hukum identitas digital bagi otoritas Australia, serta memperkuat keamanan dan perlindungan konsumen [15]. Melihat keseriusan negara-negara dalam menyusun regulasi terkait *digital identity* menimbulkan pertanyaan tentang seberapa penting *digital identity* di masa depan. Kemana arah tren teknologi *digital identity* akan berkembang jika dilihat dari sudut penelitian (*research*). Oleh karena itu, penelitian ini mencoba melakukan analisis tren masa depan dari teknologi *digital identity* menggunakan pendekatan bibliometrik.

2. METODE PENELITIAN

Penelitian dilakukan dengan pendekatan bibliometrik untuk menganalisis tren penelitian saat ini dari *digital identity*. Analisis bibliometrik digunakan untuk mengeksplorasi tren penelitian *digital identity*, menemukan arah penelitian dan perkembangan konsep *digital identiy*, mengidentifikasi kebutuhan masa depan sebelum mengadopsi konsep *digital identity* [16].

Gambar 1. Alur Penelitian

Alur penelitian yang tertera pada Gambar 1 merupakan rangkaian proses penelitian dari awal hingga selesai. Mencakup studi literatur, pengambilan data *lens.org*, analisis bibliometrik,

hasil analisis, yang kemudian diakhiri dengan tahap pengambilan kesimpulan & saran.

Proses penelitian dimulai dengan studi literatur terhadap berbagai sumber seperti artikel jurnal, prosiding, laporan konsultan, laporan perusahaan keamanan, laporan lembaga dan berbagai dokumen *whitepaper* lainnya. Tujuan studi literatur yaitu menemukan kata kunci atau *keywords* yang digunakan untuk merujuk pada teknologi *digital identity*.

Tabel 1. Hasil Pencarian Terminologi

Terminologi	Referensi	Jumlah
Digital *Identity*	[8][9][12][13][17]-[28]	16
Digital *Identities*	[2][6][14][29]-[39]	14
Digital *ID*	[8][9][14][40]-[49]	13
Total Referensi		43

Tabel 1. adalah hasil studi terhadap 47 literatur terkait menunjukkan bahwa kata kunci atau terminologi yang paling banyak digunakan untuk merujuk pada teknologi identitas digital yaitu *Digital Identity* (18 referensi), *Digital Identities* (16 referensi), dan *Digital ID* (13 referensi). Temuan tersebut kemudian digunakan sebagai input pada database *Lens.org* untuk mengambil data bibliometrik terkait teknologi identitas digital.

Proses pengambilan data dimulai dengan memasukan ketiga kata kunci pada menu pencarian Lens.org. Kata kunci yakni *Digital Identity*, *Digital Identities*, *Digital ID*, pencarian mencakup data Judul, Abstrak, Keyword, *Field of Study*. Hasil pencarian kemudian dibatasi hanya untuk publikasi yang terbit hingga 31 Desember 2023, dan hanya mengambil publikasi tipe artikel jurnal & artikel prosiding. Hasilnya adalah 1,176 publikasi yang kemudian diekstraksi dari database *lens.org* oleh penulis.

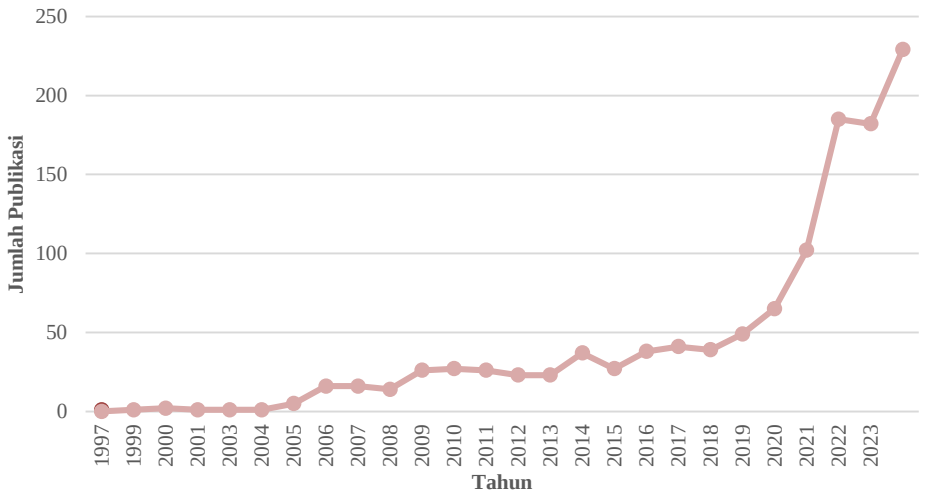
Data yang telah diterima oleh penulis kemudian dianalisis dengan menggunakan aplikasi VOSviewer sebagai aplikasi yang biasa digunakan dalam analisis bibliometrik [16][48]-[52].

3. HASIL DAN PEMBAHASAN

3.1. Pertumbuhan Publikasi

Berdasarkan hasil pengolahan data publikasi, diperoleh informasi bahwa publikasi pertama yang menyebutkan terminologi Digital ID yaitu jurnal akuntansi karya Richard J. Koreto yang terbit pada tahun 1997. Hingga tahun 2023, jumlah publikasi tipe jurnal dan prosiding telah mencapai 1,176.

Gambar 2 menunjukkan pertumbuhan jumlah publikasi hingga tahun 2004 tidak mengalami kenaikan berarti karena jumlah publikasi hanya 1. Mulai tahun 2005, jumlah publikasi secara bertahap semakin naik, tapi tren pertumbuhannya cenderung fluktuatif, bahkan hingga tahun 2017 jumlah publikasi masih di bawah angka 364. Pertumbuhan signifikan terjadi mulai tahun 2019 hingga tahun 2022 dengan jumlah publikasi mencapai 534 publikasi. Meskipun terjadi penurunan jumlah pada tahun 2022, jumlah publikasi pada tahun 2023 sebanyak 229 publikasi, sehingga total jumlah publikasi mulai 1997 s.d 2023 sebanyak 1,176 publikasi. Pertumbuhan jumlah penelitian *digital identity* merupakan dampak dari pesatnya transformasi digital di seluruh dunia pada masa pandemi Covid-19 [2][5]. Pada masa tersebut interaksi digital dan layanan elektronik menjadi bagian penting dalam kehidupan manusia [9]. Namun, masa tersebut menimbulkan permasalahan baru seperti penipuan transaksi digital [11][13], *identity fraud* [12], *biometric fraud* [13], serta ancaman siber [15] lainnya. Oleh karena itu, kebutuhan akan sebuah sistem teknologi yang dapat mengidentifikasi dan menjamin status hukum entitas menjadi penting, yakni *digital identity* [8][9][15].

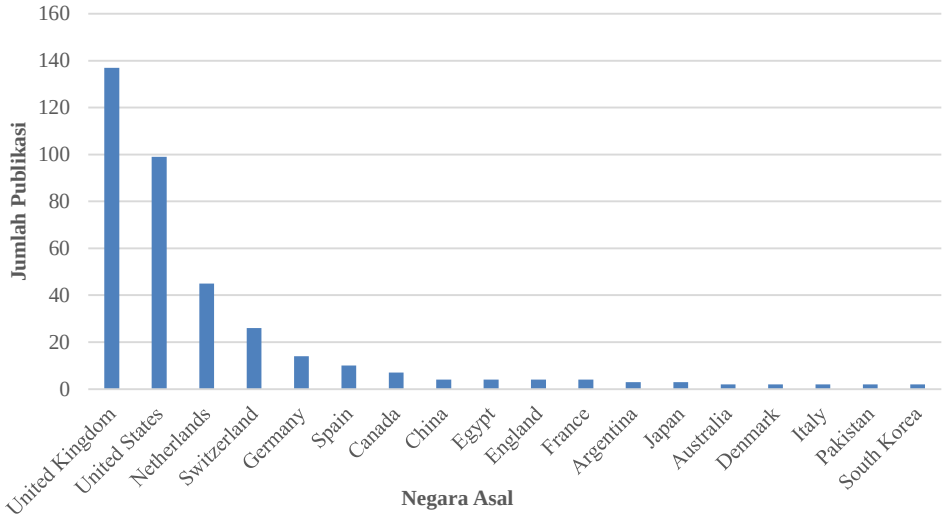


Gambar 2. Grafik Pertumbuhan Publikasi

3.2. Negara Asal Publikasi

Hasil pengolahan data menunjukkan bahwa negara yang memiliki lebih dari satu publikasi, yaitu Inggris raya, Amerika Serikat, Belanda, Swiss, Jerman, Spanyol, Kanada, Cina, Mesir, Inggris, Perancis, Argentina, Jepang, Australia, Denmark,

Italia, Pakistan, dan Korea Selatan. Mesir menjadi negara satu-satunya dari Benua Afrika yang memiliki 4 publikasi. Benua Australia memiliki 2 publikasi. Sedangkan dari Benua Asia (Cina, Jepang, Pakistan, Korea Selatan) memiliki 11 publikasi. Benua Amerika (Amerika Serikat, Kanada, Argentina, Brazil) memiliki 110 publikasi. Benua Eropa memiliki jumlah publikasi paling banyak yaitu 241. Negara lainnya hanya memiliki satu publikasi perihal *Digital Identity*.



Gambar 3. Jumlah Publikasi Berdasarkan Negara Asal

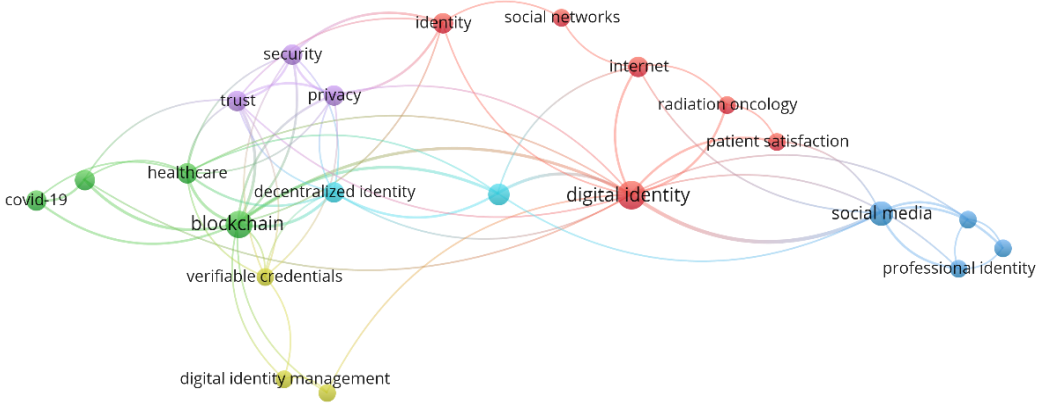
Gambar 3 menunjukkan bahwa Inggris Raya merupakan negara dengan jumlah publikasi paling tinggi, artinya penelitian *digital identity* di negara tersebut lebih maju, sehingga negara-negara lain di dunia dapat belajar dari penelitian yang telah dilakukan oleh Inggris Raya.

3.3. Analisis Peta Jaring

Hasil analisis bibliometrik menggunakan aplikasi VOSviewer menghasilkan peta jaring yang menghubungkan seluruh *keywords* dalam data bibliometrik. Proses analisis dimulai dengan menerapkan batas minimum perulangan terhadap *keywords*. Batas tersebut menentukan jumlah *keywords* yang ada pada peta jaring. Pada penelitian [16], jumlah batas perulangan yang digunakan adalah 2, batas tersebut menghasilkan 4 *cluster* data. Penelitian [19] menggunakan batas minimum 5 yang menghasilkan 2 *cluster* data. Penelitian [50], batas minimum yang diambil adalah 4 yang kemudian menghasilkan 8 *cluster* data. Penelitian [51] menggunakan batas minimum 2 dan menghasilkan 7 *cluster* data. Penelitian [52] menggunakan batas minimum 4 dan menghasilkan 5 *cluster* data.

Penelitian [53] menggunakan batas minimum 5 yang menghasilkan 4 *cluster* data. Sedangkan penelitian [54] menggunakan batas minimum 6 yang menghasilkan 4 *cluster* data. Berdasarkan penelitian [16][50]-[54], tidak ada aturan baku dalam menentukan batas minimum. Peneliti dapat menggunakan batas minimum minimal 1, 2, 4, 5, 6 ataupun jumlah lain yang menghasilkan jumlah *cluster* tidak lebih dari 8.

Penelitian ini menggunakan batas minimum 2, yang menghasilkan 6 *cluster* sesuai dengan Gambar 4. Dari 237 *keywords* pada data bibliometrik, *keywords* yang memiliki *co-occurrence* 2 sebanyak 22 *keywords*, dan terbagi dalam 6 *cluster*. Setiap *cluster* memiliki representasi warna yang sama pada Gambar 4.



Gambar 4. Peta Jaring Analisis Keyword Co-Occurrence

Cluster satu, dengan representasi warna merah terdiri dari 6 *keywords* (*digital identity*, *identity*, *internet*, *patient satisfaction*, *radiation oncology*, dan *social networks*). *Cluster* pertama merupakan kumpulan penelitian perihal *digital identity* serta penerapannya di dunia digital, yakni internet, dan sektor kesehatan dan jejaring sosial.

Cluster dua, direpresentasikan warna hijau, terdiri dari 4 *keywords* (*Blockchain*, *covid-19*, *healthcare*, *self-sovereign identity*). *Keyword* utama pada *cluster* ini yaitu teknologi *blockchain* yang merupakan teknologi dasar pada *digital identity*. *Blockchain* berkembang semenjak pandemi Covid-19 yang kemudian digunakan dalam membangun aplikasi kesehatan. *Blockchain* kemudian berkembang menjadi *self-spvereign identity*.

Cluster tiga, direpresentasikan warna biru dongker, terdiri dari 4 *keywords* (*digital professionalism*, *professional identity*, *professionalism*, *social media*). *Cluster* ini menjabarkan *digital identity* sebagai representasi entitas di dunia digital, serta mengedepankan aspek profesionalisme.

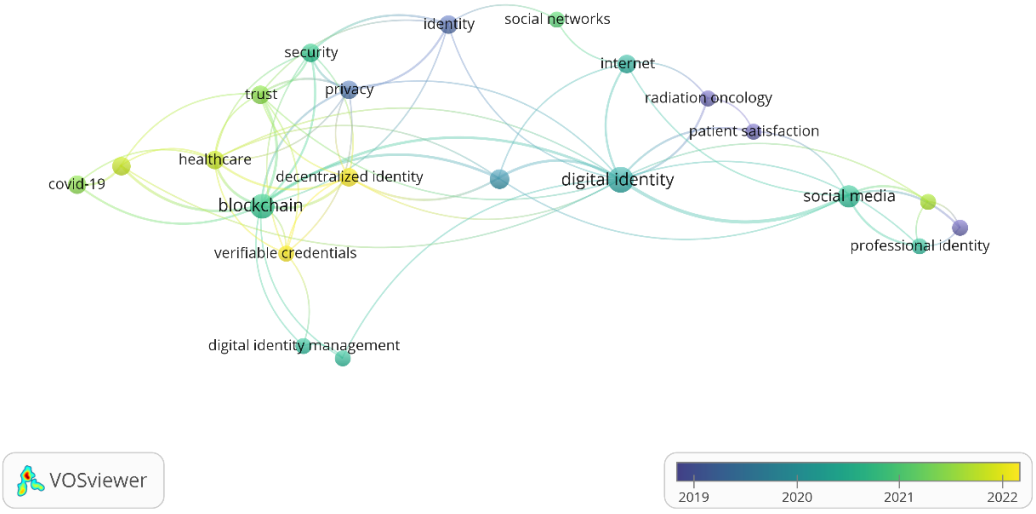
Cluster empat, direpresentasikan dengan warna kuning, terdiri dari 3 *keywords* (*digital identity management*, *machine learning*, *verifiable credentials*) merupakan kelompok kata kunci yang fokus pada manajemen *digital identity*, khususnya perihal pembagian peran dan autorisasi terhadap entitas.

Cluster lima, direpresentasikan warna ungu terdiri dari 3 *keywords* (*privacy*, *security*, *trust*). Kelompok ini merupakan kumpulan *keywords* yang berkaitan dengan ancaman terhadap *digital identity*. Selain ancaman, *cluster* lima merupakan *keywords* yang akan melahirkan banyak inovasi khususnya di bidang keamanan dan kepercayaan *digital identity*.

Cluster enam, direpresentasikan oleh warna biru muda, terdiri dari 2 *keywords* yakni *decentralized identity* dan *identity management*. Kedua *keywords* tersebut berkaitan dengan kepemilikan data *digital identity* atau *ownership*.

3.4. Analisis Peta Overlay

Selain membuat peta jaring, VOSviewer juga menghasilkan peta visualisasi *overlay* yang menggunakan sistem warna untuk merepresentasikan *keywords* dengan *novelty* atau penelitian paling terkini. *Novelty* pada peta overlay direpresentasikan oleh warna kuning, artinya *keywords* dengan warna tersebut merupakan topik yang baru dan menjadi 'hot topic' pada perkembangan *digital identity*.



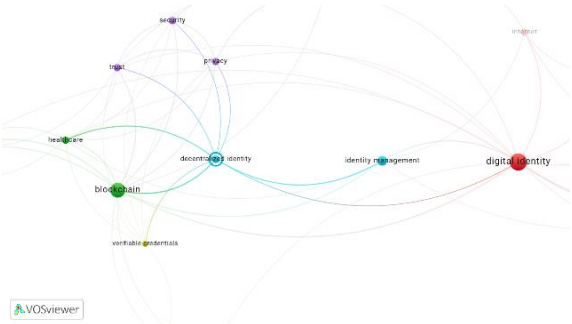
Gambar 5. Peta Overlay Analisis Keyword Co-Occurence

Gambar 5 memiliki struktur peta yang sama dengan peta jaring, tetapi hanya memiliki dua warna, yakni hijau tua untuk *keywords* tahun 2019 ke belakang, sedangkan warna kuning adalah representasi *keywords* yang muncul di tahun 2022. Gambar 5 menujukkan bahwa *keywords* yang menjadi 'hot topic' yaitu *decentralized identity*, *verifiable credentials*, dan *self-sovereign identity*. Artinya, hasil analisis bibliometrik terhadap data yang diperoleh dari *Lens.org* menunjukkan bahwa arah penelitian *digital identity* paling *novel* yaitu *decentralized identity*, *verifiable credentials*, dan *self-sovereign identity*.

4. DISKUSI

Perkembangan literatur terkait *Digital Identity* akan mengarah pada konsep *decentralized identity*, *self-sovereign identity*, dan *verifiable credentials*. Hasil tersebut dapat dilihat pada Gambar 4 yang menunjukkan bahwa teknologi *digital identity* sebagai inti penelitian memiliki hubungan dengan 5 *cluster* lainnya. Setiap *cluster* memiliki *keyword* utama yakni *blockchain* (*cluster* 2), *social media* (*cluster* 3), *verifiable credentials* (*cluster* 4), *trust* (*cluster* 5), dan *decentralized identity* (*cluster* 6). *Keyword* utama pada setiap *cluster* memiliki kekuatan hubungan paling tinggi dengan *keyword*

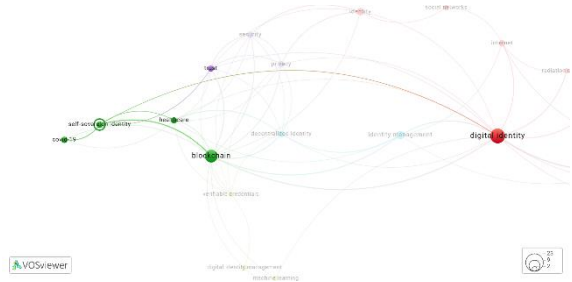
utama, *digital identity*. Setiap *cluster* kemudian berkembang sesuai dengan jaring-jaring yang mereka miliki. Jaring-jaring tersebut menghubungkan pusat *cluster* dengan jari-jari atau ujung *cluster*. Meskipun hubungannya lemah tapi seluruh *keyword* pada peta jaring saling terhubung satu sama lain. Hal tersebut membuktikan bahwa *keyword* masih berkorelasi kuat dengan *keyword* utama, *digital identity*.



Gambar 6. Peta Jaring *Decentralized Identity*

Gambar 6 menunjukkan bahwa *Decentralized identity* merupakan anggota *cluster* 6 dengan total nilai kekuatan link sebesar 12. *Decentralized identity* terhubung dengan 8 *keywords* dari cluster sekitarnya, yakni *digital identity*, *blockchain*, *healthcare*, *verifiable credentials*, *trust*, *privacy*, *security*, dan *digital identity management.*

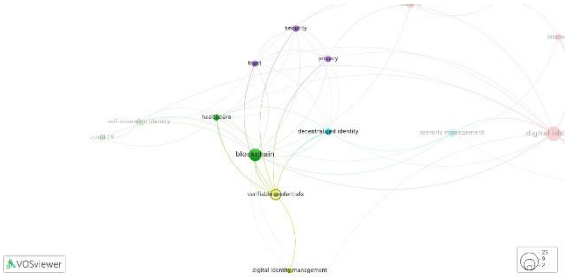
Decentralized identity merupakan salah satu perkembangan *digital identity* yang memungkinkan individu untuk mengendalikan arus dan akses penggunaan data milik diri sendiri [8]. *Decentralized identity* menawarkan solusi bagi permasalahan terkait *identity*, yakni dengan menyerahkan kuasa atas pengendalian data terhadap pemilik datanya langsung, tanpa adanya intervensi pihak ketiga ataupun otoritas terpusat [22]. Adopsi teknologi *decentralized identity* berpotensi menimbulkan disrupasi pada berbagai sektor industri, seperti industri teknologi informatika dan elektronika, industri keuangan, industri kesehatan, hingga industri retail. Berkat *decentralized identity*, penerapan *digital identity* mampu menghasilkan inovasi seperti *zero-trust architecture*, *self-sovereign identity*, dan *passwordless identity* [25].



Gambar 7. Peta Jaring Self-Sovereign Identity

Gambar 7 menunjukkan bahwa *self-sovereign identity* bagian dari *cluster* 2 terhubung dengan 5 *keywords* yaitu *digital identity*, *blockchain*, covid-19, *healthcare*, *trust.* Kelima *keywords* tersebut mengelilingi *self-sovereign identity* sebagai pusat peta jaring. *Digital identity*, covid-19, dan *healthcare* merupakan latar belakang permasalahan identitas digital dengan *blockchain* sebagai teknologi yang mampu memberikan solusi. Alhasil, kelima keywords tersebut berperan penting dalam lahirnya inovasi identitas digital baru, *self-sovereign identity.*

Self-Sovereign Identity, salah satu perkembangan lanjut *digital identity* [32], yang lahir dari teknologi *blockchain* [34], merupakan konsep dimana individu dapat mengendalikan dan mengatur data digital mereka sendiri, tanpa intervensi dari pusat data tertentu, karena banyaknya identitas digital yang dikendalikan oleh *provider* layanan online membuat banyak pemilik data tidak menguasai datanya sendiri [33], sehingga entitas pemilik data dapat memutuskan dengan siapa saja data tersebut dapat diakses [8]. Data yang dikendalikan dalam SSI yaitu *verifiable credentials* [32].



Gambar 8. Peta Jaring Verifiable Credentials

Gambar 8 menampilkan *verifiable credentials* (VCs), sebagai pusat dari 7 *keywords* di sekitarnya, yakni *blockchain*, *decentralized identity*, *digital identity management*, *healthcare*, *trust*, *privacy*, *security.* Hasil penelitian tersebut sesuai dengan literatur yang menyebutkan bahwa VCs merupakan bagian ekosistem *decentralized identity* [32], yang lahir dari inovasi *blockchain* [33], dan digunakan dalam *self-sovereign identity* [32][33].

Verifiable credentials merupakan representasi digital dari dokumen pribadi yang dimiliki oleh entitas, kekuatan hukum VCs sama dengan dokumen fisiknya, seperti tandatangan digital, serta dokumen lain yang dapat dipertanggung jawabkan validitas, integritas, autentifikasi, serta asal usulnya [33]..

5. KESIMPULAN

Hasil analisis bibliometrik terhadap *digital identity* yaitu *decentralized identity*, *verifiable credentials*, dan *self-sovereign identity*. Ketiga teknologi tersebut diprediksi akan banyak diadopsi oleh industri teknologi informasi dan elektronik [25], yakni untuk mendukung pembangunan *Web3*, *immersive reality* [17]. Selain itu, tren penelitian lebih jauh adalah teknologi *metaverse* untuk membangun sebuah avatar [55], dan penyimpanan terdesentralisasi berbasis *blockchain* untuk *Self Sovereign Identity* [32]-[34]. Oleh karena itu, *metaverse* merupakan masa depan *digital identity*,

dan juga katalis baik bagi industri teknologi informasi & elektronik, maupun bagi industri telekomunikasi untuk mengadopsi konsep *Digital ID*[55].

DAFTAR PUSTAKA

[1] A. House, "Asia House Annual Outlook 2024," Asia House. https://asiahouse.org/research_posts/asia-house-annual-outlook-2024/#:~:text=The%20Asia%20House%20Annual%20Outlook (accessed May 8, 2024).

[2] A. D. Bank, Asian Economic Integration Report 2024: Decarbonizing Global Value Chains. Asian Development Bank, 2024. Accessed: May 8, 2024. [Online]. Available: https://www.adb.org/publications/asian-economic-integration-report-2024.

[3] "The Mobile Economy China 2024 - The Mobile Economy," The Mobile Economy, Mar. 25, 2024. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/china/.

[4] "The Mobile Economy 2024," GSMA Intelligence. Accessed: May 11, 2024. [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf.

[5] "The Mobile Economy Asia Pacific 2023 - The Mobile Economy," The Mobile Economy, Apr. 29, 2024. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/asiapacific/.

[6] "Top Trends in Identity for 2024 Securing the Future of Identity in the AI Era," 2024. Available: https://www.rsa.com/wp-content/uploads/rsa-top-trends-in-identity-for-2024-ebook.pdf.

[7] "Deloitte's TMT predictions 2024," Deloitte Insights, Jan. 08, 2024. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2024/introduction.html.

[8] "Reimagining digital ID," World Economic Forum, Oct. 09, 2023. https://www.weforum.org/publications/reimagining-digital-id/.

[9] "Digital Identity Standards," ENISA, Jul. 03, 2023. https://www.enisa.europa.eu/publications/digital-identity-standards.

[10] "Consumer Sentinel Network Data Book 2023," Federal Trade Commission, Feb. 12, 2024. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023.

[11] GSMA, "Mobile Money Fraud Typologies and Mitigation Strategies | Mobile for Development," Mobile for Development, Mar. 04, 2024. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/mobile-money-fraud-typologies-and-mitigation-strategies/.

[12] "2024 State of Identity Fraud Report," AuthenticID. https://www.authenticid.com/2024-state-of-identity-fraud/ (accessed May 12, 2024).

[13]]"2024 Digital Identity Fraud in Africa Report." Accessed: May 12, 2024. [Online]. Available: https://bitcoinke.io/wp-content/uploads/2024/01/2024-Digital-Identity-Fraud-Africa-Report-SmileID.pdf.

[14] C. Busch, "eIDAS 2.0: DIGITAL IDENTITY SERVICES IN THE PLATFORM ECONOMY," 2022. Available: https://cerre.eu/wp-content/uploads/2022/10/CERRE_Digital-Identity_Issue-Paper_FINAL-2.pdf.

[15] "Your Guide to the Digital ID Legislation and Digital ID Rules," 2023. Accessed: May 12, 2024. [Online]. Available: https://www.digitalidentity.gov.au/sites/default/files/2023-09/Your%20guide%20to%20the%20Digital%20ID%20legislation%20and%20Digital%20ID%20Rules_2.pdf.

[16] C. C. Okafor, C. Aigbavboa, and W. D. Thwala, "A bibliometric evaluation and critical review of the smart city concept – making a case for social equity," Journal of Science and Technology Policy Management/Journal of Science & Technology Policy Management, vol. 14, no. 3, pp. 487–510, Jan. 2022, doi: 10.1108/jstpm-06-2020-0098.

[17] S. L. Nita and M. I. Mihailescu, "A Novel Authentication Scheme Based on Verifiable Credentials Using Digital Identity in the Context of Web 3.0," Electronics, vol. 13, no. 6, p. 1137, Jan. 2024, doi: https://doi.org/10.3390/electronics13061137.

[18] G Sreenath, G. T. Sridhar, A. A. Sannabhadti, R. Mercy, and M. R. Kounte, "Blockchain Based Digital Identity Solution," Jan. 2024, doi: https://doi.org/10.1109/idciot59759.2024.10467241.

[19] Wojciech Czakon, M. Jedynak, Aneta Kuźniarska, and K. Mania, "Social media and constructing the digital identity of

organizations: A bibliometric analysis," Entrepreneurial Business and Economics Review, vol. 11, no. 4, pp. 43–56, Jan. 2023, doi: https://doi.org/10.15678/eber.2023.110403.

[20] A. Zafeiropoulou and Evangelos Sakkopoulos, "Harmonising Digital Identity Documents," Jul. 2023, doi: https://doi.org/10.1109/iisa59645.2023.10345955.

[21] T. Giannini and J. P. Bowen, "Global Cultural Conflict and Digital Identity: Transforming Museums," Heritage, vol. 6, no. 2, pp. 1986–2005, Feb. 2023, doi: https://doi.org/10.3390/heritage6020107.

[22] M. Campbell, "The Road to Decentralized Identity: The Techniques, Promises, and Challenges of Tomorrow's Digital Identity," vol. 56, no. 6, pp. 96–100, Jun. 2023, doi: https://doi.org/10.1109/mc.2023.3263020.

[23] Prashant Kumar Choudhary, Sangeeta Shah Bharadwaj, and A. Kaushik, "Configurational Analysis of Infrastructuring in Digital Identity Platforms," International journal of public administration in the digital age, vol. 10, no. 1, pp. 1–41, Nov. 2023, doi: https://doi.org/10.4018/ijpada.333893.

[24] H. Kumar, Rameshwar Shivadas Ture, M. Gupta, and R. Sharma, "Technological Solutions for Digital Identity," Journal of Database Management, vol. 34, no. 1, pp. 1–17, Jul. 2023, doi: https://doi.org/10.4018/jdm.325352.

[25] "McKinsey Technology Trends Outlook 2022." Accessed: Feb. 24, 2024. [Online]. Available: https://www.mckinsey.com/spContent/bespoke/tech-trends/pdfs/mckinsey-tech-trends-outlook-2022-trust-arch-digid.pdf.

[26] S. Li, J. G. Wu, J. Bian, Z. Ding, and Y. Sun, "Understanding Digital Identity during the Pandemic: An Investigation of Two Chinese Spanish Teachers," Sustainability, vol. 15, no. 2, p. 1208, Jan. 2023, doi: https://doi.org/10.3390/su15021208.

[27] S. Masiero, "Digital identity as platform-mediated surveillance," Big Data & Society, vol. 10, no. 1, p. 205395172211351, Jan. 2023, doi: https://doi.org/10.1177/2053951722113517.

[28] V. Aanandaram and P. Deepalakshmi, "Blockchain-based Digital Identity for Secure Authentication of IoT Devices In 5G Networks," Mar. 2024, doi: https://doi.org/10.1109/incos59338.2024.10527739.

[29] W. Czakon, K. Mania, M. Jedynak, A. Kuźniarska, M. Choiński, and M. Dabić, "Who are we? Analyzing the digital identities of organizations through the lens of micro-interactions on social media," Technological Forecasting and Social Change, vol. 198, p. 123012, Jan. 2024, doi: https://doi.org/10.1016/j.techfore.2023.123012.

[30] D. Pöhn and W. Hommel, "Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems," Security and Communication Networks, vol. 2023, p. e5573310, Jun. 2023, doi: https://doi.org/10.1155/2023/5573310.

[31] T. Friedhoff, C.-D. Au, N. Ladnar, D. Stein, and A. Zureck, "Analysis of Social Acceptance for the Use of Digital Identities," Computers, vol. 12, no. 3, p. 51, Mar. 2023, doi: https://doi.org/10.3390/computers12030051.

[32] V. Srinivas, Aniruddha Krishna Jha, G. Ganesh, V Nitish, and Shruti Jadon, "Decentralized User Identity Management using Blockchain," May 2023, doi: https://doi.org/10.1109/vitecon58111.2023.10157380.

[33] R. Mecozzi, G. Perrone, D. Anelli, N. Saitto, E. Paggi, and D. Mancini, "Blockchain-related identity and access management challenges: (de)centralized digital identities regulation," 2022 IEEE International Conference on Blockchain (Blockchain), Aug. 2022, doi: https://doi.org/10.1109/blockchain55522.2022.00068.

[34] Shipra Ravi Kumar and M. Goyal, "Administration of Digital Identities Using Blockchain," Dec. 2022, doi: https://doi.org/10.1109/ic3i56241.2022.10072845.

[35] E. Cioroaica, B. Buhnova, F. Jacobi, and D. Schneider, "The Concept of Ethical Digital Identities," IEEE Xplore, May 01, 2022. https://ieeexplore.ieee.org/document/9808646 (accessed Jan. 13, 2023).

[36] Y. Wang, Y. Li, and J. Wu, "Digital identities of female founders and crowdfunding performance: an exploration based on the LDA topic model," Gender in Management: An International Journal, vol. 37, no. 5, pp. 659–678, Apr. 2022, doi: https://doi.org/10.1108/gm-12-2020-0360.

[37] A. Jorge, L. Marôpo, and F. Neto, "'When you realise your dad is Cristiano Ronaldo': celebrity sharenting and children's digital identities," Information, Communication & Society, vol. 25, no. 4, pp. 1–20, Jan. 2022, doi: https://doi.org/10.1080/1369118x.2022.2026

996.

[38] A. A. Sathio, M. Ali Dootio, A. Lakhan, M. ur Rehman, A. Orangzeb Pnhwar, and M. A. Sahito, "Pervasive Futuristic Healthcare and Blockchain enabled Digital Identities-Challenges and Future Intensions," 2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Aug. 2021, doi: https://doi.org/10.1109/iccece52344.2021.9534846.

[39] P. Renee Carnley, P. Rowland, D. Bishop, Sikha Bagui, and M. Miller, "Trusted Digital Identities for Mobile Devices," Aug. 2020, doi: https://doi.org/10.1109/dasc-picom-cbdcom-cyberscitech49142.2020.00090.

[40] J. Lopez-Solano and Juan Diego Castañeda, "'A promising playground': IDEMIA and the digital ID infrastructuring in Colombia," Information, communication & society, pp. 1–17, Jan. 2024, doi: https://doi.org/10.1080/1369118x.2024.2302995.

[41] B. Wang, Wouter Lueks, Justinas Sukaitis, Vincent Graf Narbel, and C. Troncoso, "Not Yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution," May 2023, doi: https://doi.org/10.1109/sp46215.2023.10179306.

[42] T. Solanki, K. Patel, S. Pande, and A. V. Nimkar, "BlockID: Blockchain based Digital ID and Authentication System for Privacy Improvement," May 2023, doi: https://doi.org/10.1109/access57397.2023.10199733.

[43] Stefanus Van Staden and N. J. Bidwell, "Localised Trust in a Globalised Knot: Designing Information Privacy for Digital-ID," Aug. 2023, doi: https://doi.org/10.1145/3616024.

[44] A. Mitra, D. Bigioi, S. P. Mohanty, P. Corcoran, and E. Kougianos, "iFace 1.1: A Proof-of-Concept of a Facial Authentication Based Digital ID for Smart Cities," IEEE Access, pp. 1–1, 2022, doi: https://doi.org/10.1109/access.2022.318768.

[45] X. Lou, "The Financial Information Management System Mechanism of Domestic Top Three Hospitals Based on Digital ID Technology and Crawler Mining," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Dec. 2021, doi: https://doi.org/10.1109/iceca52323.2021.9676134.

[46] J. Cheng and J. Ma, "Construction of food digital ID and intelligent monitoring platform based on blockchain traceability and GPS locationing," 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Dec. 2021, doi: https://doi.org/10.1109/iceca52323.2021.9676143.

[47] Mads Schaarup Andersen, "Towards the Design of a Privacy-preserving Attribute Based Credentials-based Digital ID in Denmark – Usefulness, Barriers, and Recommendations," Scopus (Elsevier), Aug. 2021, doi: https://doi.org/10.1145/3465481.3469211.

[48] B. Braim, Abdelali El Gourari, Mustapha Raoufi, and M. Skouri, "Autonomous Door with Face Recognition for Enhanced Security Systems of Educational Institutions," Apr. 2024, doi: https://doi.org/10.1109/gast60528.2024.10520771.

[49] "Your Guide to the Digital ID Legislation and Digital ID Rules," 2023. Accessed: Jun. 04, 2024. [Online]. Available: https://www.digitalidentity.gov.au/sites/default/files/2023-09/Your%20guide%20to%20the%20Digital%20ID%20legislation%20and%20Digital%20ID%20Rules_1.pdf.

[50] C. Münch, M. Wehrle, T. Kuhn, and E. Hartmann, "The research landscape around the physical internet – a bibliometric analysis," International journal of production research, vol. 62, no. 6, pp. 2015–2033, May 2023, doi: https://doi.org/10.1080/00207543.2023.2205969.

[51] Abderahman Rejeb, Karim Rejeb, A. Appolloni, and S. Seuring, "Public procurement research: a bibliometric analysis," International Journal of Public Sector Management, Jan. 2024, doi: https://doi.org/10.1108/ijpsm-07-2022-0157.

[52] D. O. Aghimien, C. O. Aigbavboa, A. E. Oke, and W. D. Thwala, "Mapping out research focus for robotics and automation research in construction-related studies," Journal of Engineering, Design and Technology, vol. ahead-of-print, no. ahead-of-print, Dec. 2019, doi: https://doi.org/10.1108/jedt-09-2019-0237.

[53] N. Kumar, A. Singh, S. Gupta, M. S. Kaswan, and M. Singh, "Integration of Lean manufacturing and Industry 4.0: a bibliometric analysis," The TQM Journal, Mar. 2023, doi: https://doi.org/10.1108/tqm-07-2022-0243.

[54] B. B. Santos, Tiago, Izabela Simon

Rampasso, G. Hermínio, Walter Leal Filho, and Rosley Anholon, "Lean leadership: a bibliometric analysis," Feb. 2023, doi: https://doi.org/10.1108/bij-07-2022-0468.

[55] C. Zhang, M. Zhao, W. Zhang, Q. Fan, J. Ni, and L. Zhu, "Privacy-Preserving Identity-Based Data Rights Governance for Blockchain-Empowered Human-Centric Metaverse Communications," IEEE journal on selected areas in communications, vol. 42, no. 4, pp. 963–977, Apr. 2024, doi: https://doi.org/10.1109/jsac.2023.3345392.