Jurnal Studi Kebijakan Publik

ARTIKEL

Memperkuat Keamanan Data melalui Teknologi *Blockchain*: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia

Strengthening Data Security through Blockchain Technology: Exploring Successful Implementations in Digital Transformation in Indonesia

Tito Wira Eka Suryawijaya

Universitas Dian Nuswantoro

211202080011@mhs.dinus.ac.id

Citation: Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *JSKP: Jurnal Studi Kebijakan Publik, 2*(1), 55–67. https://doi.org/10.21787/jskp.2.2023.55-67

Naskah Diterima: 5 Maret 2023

Naskah Disetujui: 27 Mei 2023

Naskah Diterbitkan: 31 Mei 2023

Kata Kunci: Transformasi Digital, *Blockchain*, Keamanan Data, Indonesia

Keywords: *Digital Transformation, Blockchain, Data Security, Indonesia*

Abstrak: Transformasi digital menjadi tren global yang telah mengubah cara bisnis dan pemerintahan di seluruh dunia. Di Indonesia, pemerintah dan sektor swasta sedang mempercepat transformasi digital dengan mengadopsi teknologi *blockchain* sebagai solusi untuk meningkatkan keamanan data dalam operasi sehari-hari. Beberapa proyek *blockchain* di Indonesia telah dilakukan, seperti verifikasi dan validasi sertifikat pendidikan, penyimpanan data medis, dan sistem pembayaran. Namun, implementasi teknologi *blockchain* di Indonesia masih menghadapi beberapa tantangan, seperti regulasi yang belum jelas, infrastruktur yang masih terbatas, dan kurangnya pemahaman tentang teknologi *blockchain*. Oleh karena itu, diperlukan dukungan dari semua pihak untuk mempercepat adopsi teknologi *blockchain* di Indonesia. Penelitian dan pengembangan lebih lanjut harus dilakukan untuk mengoptimalkan potensi teknologi *blockchain* dan mempercepat transformasi digital di Indonesia.

Abstract: *Digital transformation is becoming a global trend that has changed the way businesses and governments around the world. In Indonesia, the government and the private sector are accelerating digital transformation by adopting blockchain technology as a solution to increase data security in daily operations. Several blockchain projects in Indonesia have been carried out, such as verification and validation of educational certificates, medical data storage, and payment systems. However, the implementation of blockchain technology in Indonesia still faces several challenges, such as unclear regulations, limited infrastructure, and a lack of understanding of blockchain technology. Therefore, support from all parties is needed to accelerate the adoption of blockchain technology in Indonesia. Further research and development should be carried out to optimize the potential of blockchain technology and accelerate digital transformation in Indonesia.*

1. Pendahuluan

Transformasi digital telah mempengaruhi berbagai aspek kehidupan kita, mulai dari cara kita berkomunikasi, bekerja, berbelanja, dan melakukan bisnis (Panggabean, 2022). Hal ini terjadi karena digitalisasi telah memungkinkan pengumpulan, penyimpanan, dan pengolahan data yang lebih mudah dan cepat. Dalam era digital, data menjadi salah satu aset terpenting bagi organisasi dan individu. Data adalah sumber informasi yang digunakan untuk membuat keputusan penting, menghasilkan nilai tambah bagi perusahaan, dan mendorong inovasi (Jurnal Entrepreneur, 2022). Oleh karena itu, keamanan data menjadi sangat penting dan kritis dalam transformasi digital. Di Indonesia, transformasi digital sedang mengalami perkembangan yang pesat. Pemerintah Indonesia telah mengeluarkan berbagai inisiatif untuk mendorong transformasi digital di Indonesia, seperti Inisiatif Nasional 1000 *Startup Digital*, Gerakan Nasional 100 *Smart City*, dan lain-lain (Saefudin, 2022). Namun, meskipun transformasi digital dapat memberikan banyak manfaat bagi ekonomi Indonesia, namun ada resiko keamanan yang harus dihadapi. Masalah keamanan data telah menjadi masalah yang sangat serius di seluruh dunia. Data dapat diakses oleh pihak yang tidak berwenang dan digunakan untuk tujuan yang merugikan. Beberapa contoh termasuk pencurian identitas, penipuan, penggunaan data untuk melakukan aksi kejahatan, dan lain-lain. Oleh karena itu, dibutuhkan sistem keamanan yang kuat untuk melindungi data dari risiko tersebut (Situmeang, 2021). Dalam konteks ini, teknologi *blockchain* menawarkan solusi yang menarik untuk masalah keamanan data dalam transformasi digital. *Blockchain* adalah teknologi terdesentralisasi yang memungkinkan transaksi antara dua pihak yang tidak saling percaya tanpa melibatkan pihak ketiga. Data dalam *blockchain* disimpan secara terdesentralisasi di seluruh jaringan, sehingga tidak dapat diubah oleh satu pihak tanpa persetujuan dari seluruh jaringan. *Blockchain* juga dapat meningkatkan transparansi dan akuntabilitas dalam pengelolaan data.

Keamanan data dalam transformasi digital menjadi sangat penting karena data dapat diakses oleh pihak yang tidak berwenang dan digunakan untuk tujuan yang merugikan (Nugroho et al., 2021; Situmeang, 2021). Dalam konteks ini, teknologi *blockchain* dapat meningkatkan keamanan data dengan beberapa cara. Pertama, *blockchain* memungkinkan data untuk disimpan secara terdesentralisasi dan terenkripsi, sehingga meningkatkan keamanan data. Karena data tidak disimpan secara sentral, maka sulit bagi orang untuk mencuri data atau mengubahnya tanpa persetujuan dari seluruh jaringan *blockchain*. Kedua, dalam teknologi *blockchain*, setiap transaksi dan data dapat diverifikasi oleh semua pihak yang terlibat. Hal ini meningkatkan transparansi dan mengurangi risiko penipuan. Ketiga, proses verifikasi dan validasi dalam teknologi *blockchain* sangat efisien dan cepat, karena tidak memerlukan perantara atau pihak ketiga.

Namun, penggunaan teknologi *blockchain* juga memiliki beberapa risiko, seperti ketergantungan pada teknologi, risiko keamanan, dan keterbatasan skalabilitas. Jika teknologi *blockchain* mengalami masalah atau kegagalan, maka data dan transaksi yang disimpan dalam *blockchain* juga akan terkena dampaknya. Selain itu, masalah keamanan juga merupakan risiko utama dalam penggunaan teknologi *blockchain* untuk keamanan data. Meskipun teknologi *blockchain* dianggap sangat aman, namun tidak menutup kemungkinan adanya serangan yang berhasil menembus sistem keamanannya. Beberapa jenis serangan yang dapat terjadi pada *blockchain* antara lain serangan 51% *attack*, *double-spending attack, sybil attack*, dan lain-lain. Serangan 51% *attack* terjadi ketika seorang penyerang berhasil menguasai lebih dari 50% kekuatan jaringan *blockchain* (Trinowo, 2020). Dengan menguasai lebih dari 50% kekuatan jaringan, penyerang dapat memalsukan transaksi dan mengganti catatan transaksi yang telah dilakukan sebelumnya. Hal ini dapat merusak integritas data dan mengancam keamanan data dalam *blockchain*. *Double-spending attack* adalah serangan di mana seorang penyerang mencoba untuk melakukan transaksi yang sama dua kali menggunakan aset kripto yang sama. Dalam blockchain, setiap

transaksi harus diverifikasi dan disetujui oleh seluruh jaringan. Namun, dalam *double-spending attack*, penyerang mencoba untuk memalsukan transaksi dan mengirimkan aset kripto yang sama ke dua alamat yang berbeda secara bersamaan. Hal ini dapat mengakibatkan kerugian finansial yang signifikan bagi pihak yang menerima aset kripto tersebut. *Sybil attack* adalah serangan di mana seorang penyerang mencoba untuk mengambil alih jaringan *blockchain* dengan membuat banyak identitas palsu. Dalam *sybil attack*, penyerang membuat banyak identitas palsu yang tampaknya berasal dari banyak *node* jaringan yang berbeda. Hal ini dapat membuat penyerang memiliki kekuatan yang lebih besar dalam jaringan dan dapat memalsukan transaksi dan data (Bashar et al., 2022).

Selain risiko keamanan, penggunaan teknologi *blockchain* dalam transformasi digital juga memiliki keterbatasan dalam skalabilitas. Teknologi *blockchain* memiliki keterbatasan dalam skala dan kapasitas transaksi yang dapat ditangani. Hal ini menjadi tantangan jika digunakan dalam implementasi transformasi digital yang besar dan kompleks (Lin & Liao, 2017; Bashar et al., 2022). Meskipun terdapat beberapa teknologi *blockchain* yang dikembangkan untuk meningkatkan skalabilitas, namun masih diperlukan penelitian dan pengembangan lebih lanjut untuk meningkatkan kapasitas transaksi yang dapat ditangani.

Meskipun penggunaan teknologi *blockchain* memiliki beberapa risiko dan keterbatasan, namun teknologi ini dapat memberikan manfaat yang signifikan bagi keamanan data dalam transformasi digital. Dalam implementasi *blockchain* untuk keamanan data, penting untuk memilih jenis *blockchain* yang paling sesuai dengan kebutuhan organisasi dan mempertimbangkan manfaat dan risiko yang terkait dengan penggunaan *blockchain*. Selain itu, penting juga untuk mempertimbangkan kebutuhan untuk integrasi dengan sistem yang ada dan kemampuan untuk mengatasi keterbatasan teknologi *blockchain* (Lin & Liao, 2017; Liu et al., 2019).

Dalam konteks transformasi digital di Indonesia, penggunaan teknologi *blockchain* untuk keamanan data memiliki potensi yang besar untuk meningkatkan keamanan dan transparansi dalam pengelolaan data. Namun, penggunaan teknologi *blockchain* dalam transformasi digital di Indonesia masih tergolong baru dan terbatas. Sejumlah perusahaan dan institusi di Indonesia mulai mempertimbangkan penggunaan *blockchain* dalam bisnis mereka, tetapi masih banyak yang belum memahami potensi penuh dan kelemahan teknologi ini (Liu et al., 2019). Selain itu, masih terdapat perbedaan pandangan antara regulator dan pelaku industri tentang penggunaan *blockchain* dan *cryptocurrency* (Manurung & Wijoyo, 2021). Beberapa regulator di Indonesia seperti Bank Indonesia dan Otoritas Jasa Keuangan (OJK) memiliki pandangan yang skeptis terhadap penggunaan *cryptocurrency* dan memperketat regulasi terkait. Hal ini dapat mempengaruhi pengembangan ekosistem *blockchain* di Indonesia dan menghambat adopsi teknologi ini (*Centre for Innovation Policy and Governance*, 2018).

Selain itu, masalah teknis dan infrastruktur juga menjadi tantangan bagi pengembangan *blockchain* di Indonesia. Ketersediaan infrastruktur yang memadai, ketersediaan SDM yang memiliki keahlian dalam bidang *blockchain*, serta dukungan dari lembaga keuangan dan pemerintah menjadi faktor penting dalam pengembangan teknologi *blockchain*. Masalah-masalah teknis yang muncul dalam pengembangan *blockchain* di Indonesia termasuk skala jaringan yang terbatas, ketergantungan pada jaringan internet yang tidak selalu stabil, dan keterbatasan teknologi yang digunakan dalam transaksi *blockchain*. Meskipun demikian, teknologi *blockchain* memiliki potensi besar untuk meningkatkan keamanan data dalam transformasi digital di Indonesia. Berbagai industri dan sektor yang terlibat dalam transformasi digital, seperti perbankan, logistik, dan pemerintahan, dapat memanfaatkan teknologi ini untuk meningkatkan keamanan data mereka. Dalam sektor perbankan, *blockchain* dapat digunakan untuk mengamankan transaksi keuangan dan meminimalkan risiko kecurangan dan kejahatan finansial. Dalam sektor logistik, *blockchain* dapat digunakan untuk memastikan keamanan dan keandalan pengiriman barang dan meminimalkan risiko kehilangan atau kerusakan barang. Dalam sektor pemerintahan,

blockchain dapat digunakan untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan data, serta meminimalkan risiko korupsi.

Namun, implementasi *blockchain* dalam transformasi digital di Indonesia perlu dilakukan dengan hati-hati dan mempertimbangkan berbagai faktor. Beberapa faktor yang perlu dipertimbangkan antara lain penggunaan teknologi yang tepat, pemilihan vendor atau *platform blockchain* yang dapat diandalkan, serta pemahaman tentang keamanan dan privasi data. Selain itu, perlu ada kerja sama antara regulator, pelaku industri, dan akademisi untuk memastikan adopsi *blockchain* yang berhasil dan berkelanjutan di Indonesia. Dalam hal ini, penting bagi para pemimpin dan pengambil keputusan di Indonesia untuk memahami potensi dan risiko yang terkait dengan teknologi *blockchain*, serta melakukan upaya-upaya yang diperlukan untuk mendukung pengembangan ekosistem *blockchain* di Indonesia. Hal ini dapat dilakukan melalui investasi dalam penelitian dan pengembangan *blockchain*, pembentukan regulasi yang memfasilitasi penggunaan *blockchain*, serta penyediaan infrastruktur dan SDM yang memadai (Bashar et al., 2022).

Dalam konteks transformasi digital di Indonesia, penggunaan teknologi *blockchain* untuk keamanan data menjadi solusi yang menarik dan inovatif. Namun, di tengah potensi manfaat yang besar, penggunaan teknologi *blockchain* juga membawa risiko dan tantangan yang tidak dapat diabaikan (Argani & Taraka, 2020; Bashar et al., 2022). Melalui penelitian ini, kami berharap dapat memberikan wawasan baru dan kontribusi terhadap pengembangan solusi keamanan data yang efektif dan efisien di Indonesia.

2. Metode

Metodologi penelitian ini dilakukan dengan menggunakan pendekatan deskriptif kualitatif. Penelitian ini dilakukan dengan menganalisis data dan informasi yang diperoleh dari studi pustaka melalui jurnal, artikel dan sumber resmi terkait transformasi digital dan implementasi teknologi *blockchain* di Indonesia yang dilaksanakan selama dua bulan. Selain itu, penelitian ini juga melibatkan wawancara dengan pakar dan praktisi di bidang teknologi dan transformasi digital di Indonesia (Kim et al., 2017).

Tahap awal penelitian dilakukan dengan mengumpulkan dan meninjau literatur terkait transformasi digital dan teknologi *blockchain* di Indonesia, serta analisis regulasi dan strategi yang telah dikeluarkan oleh pemerintah Indonesia terkait implementasi teknologi *blockchain*. Setelah itu, peneliti melakukan wawancara dengan pakar dan praktisi di bidang teknologi dan transformasi digital untuk mendapatkan sudut pandang yang lebih luas dan mendalam mengenai implementasi teknologi *blockchain* di Indonesia.

Hasil dari penelitian ini kemudian dianalisis dan disusun menjadi sebuah kesimpulan mengenai potensi dan tantangan implementasi teknologi *blockchain* dalam transformasi digital di Indonesia, serta rekomendasi yang dapat dilakukan oleh pemerintah dan sektor swasta untuk memaksimalkan manfaat dari teknologi *blockchain* dalam transformasi digital di Indonesia (Moleong, 2014).

3. Hasil dan Pembahasan

Perkembangan teknologi digital telah memungkinkan data untuk diakses, dibagikan, dan disimpan secara mudah dan efisien. Namun, perkembangan ini juga menimbulkan risiko keamanan data yang semakin kompleks dan beragam (Bashar et al., 2022). Keamanan data menjadi penting karena data merupakan aset yang sangat berharga bagi organisasi dan individu. Data dapat digunakan untuk mempengaruhi keputusan, menghasilkan nilai tambah, dan memberikan keuntungan kompetitif. Oleh karena itu, keamanan data harus diperhatikan dengan serius dan diintegrasikan dalam semua aspek transformasi digital (Manurung & Wijoyo, 2021; Maulani et al., 2023).

Konsep keamanan data meliputi tiga aspek utama: kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan data berkaitan dengan privasi dan kerahasiaan data dari pihak yang tidak berwenang. Informasi yang dikategorikan sebagai rahasia antara lain data pribadi, data kesehatan, data keuangan, data rahasia perusahaan, dan data

pemerintah (*Centre for Innovation Policy and Governance,* 2018). Pengungkapan informasi rahasia dapat berdampak buruk pada kepentingan individu atau organisasi. Oleh karena itu, upaya untuk menjaga kerahasiaan data sangat penting dalam transformasi digital (Panggabean, 2022). Integritas data adalah kualitas data yang dijaga agar tetap benar, utuh, dan valid. Integritas data meliputi keabsahan data, konsistensi data, dan keutuhan data. Kehilangan integritas data dapat mengakibatkan data yang tidak akurat, tidak sesuai dengan kenyataan, dan menghasilkan keputusan yang salah. Oleh karena itu, menjaga integritas data sangat penting dalam transformasi digital (Universitas Islam Indonesia, 2021).

Ketersediaan data berkaitan dengan kemampuan untuk mengakses data secara mudah dan cepat oleh pihak yang berwenang. Ketersediaan data menjadi sangat penting dalam era digitalisasi yang semakin terkoneksi dan memerlukan data yang terus diperbarui. Ketersediaan data yang rendah dapat menghambat proses bisnis, mengganggu pengambilan keputusan, dan mengurangi kinerja organisasi. Oleh karena itu, upaya untuk menjaga ketersediaan data harus diperhatikan dalam transformasi digital. Selain aspek kerahasiaan, integritas, dan ketersediaan data, konsep keamanan data juga meliputi aspek keandalan dan kecepatan data. Keandalan data berkaitan dengan akurasi dan konsistensi data yang digunakan dalam proses bisnis (Liu et al., 2019). Kecepatan data berkaitan dengan kemampuan untuk mengakses data secara cepat dan tepat waktu. Dalam transformasi digital, keandalan dan kecepatan data menjadi sangat penting untuk memastikan pengambilan keputusan yang tepat dan waktu yang efisien.

3.1. Konsep Keamanan Data dalam Transformasi Digital

Dalam era digitalisasi yang semakin berkembang, data menjadi aset yang paling berharga bagi organisasi dan individu. Data adalah sumber daya penting yang digunakan untuk membuat keputusan yang tepat dalam bisnis, membantu memecahkan masalah, mengidentifikasi trend, dan meningkatkan efisiensi operasional. Namun, penggunaan teknologi digital juga meningkatkan risiko keamanan data. Ancaman keamanan data seperti kebocoran, pencurian, manipulasi, dan penggunaan yang tidak sah semakin meningkat seiring dengan perkembangan teknologi. Oleh karena itu, konsep keamanan data menjadi sangat penting dan krusial dalam era digitalisasi (Lin & Liao, 2017).

Konsep keamanan data meliputi tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan data berkaitan dengan pemeliharaan privasi data dari pihak yang tidak berhak mengaksesnya. Hal ini meliputi pencegahan akses tidak sah ke data atau penggunaan data secara tidak sah (*Centre for Innovation Policy and Governance,* 2018). Misalnya, data kesehatan seseorang adalah informasi yang sangat sensitif dan harus dilindungi dari pihak yang tidak berwenang. Integritas data meliputi keaslian dan keutuhan data yang diproses dan disimpan oleh organisasi (Bashar et al., 2022). Keaslian data menjamin bahwa data tidak dimanipulasi atau diubah tanpa sepengetahuan atau persetujuan dari pihak yang berwenang. Keutuhan data menjamin bahwa data tidak rusak atau hilang selama proses penyimpanan atau pengiriman data. Ketersediaan data berkaitan dengan aksesibilitas data oleh pihak yang berwenang saat dibutuhkan. Jika data tidak tersedia saat dibutuhkan, maka organisasi mungkin mengalami kerugian bisnis dan pelanggan mungkin kehilangan kepercayaan.

Dalam transformasi digital, penggunaan teknologi digital seperti *cloud computing, big data*, dan *internet of things (IoT)* dapat meningkatkan efisiensi dan produktivitas organisasi (Liu et al., 2019; Trinowo, 2020). Namun, penggunaan teknologi digital juga meningkatkan risiko keamanan data. Hal ini menekankan pentingnya penggunaan teknologi keamanan terbaru dan penerapan praktik pengamanan yang ketat dalam transformasi digital. Penerapan teknologi keamanan yang tepat akan memastikan bahwa data dan informasi penting terlindungi dari akses tidak sah atau manipulasi oleh pihak yang tidak berwenang. Selain itu, penggunaan teknologi keamanan juga

akan membantu organisasi untuk mematuhi undang-undang dan regulasi yang berkaitan dengan keamanan data (Liu et al., 2019; Putra et al., 2019).

Strategi keamanan data yang efektif harus mencakup penggunaan teknologi keamanan yang tepat, prosedur pengamanan yang ketat, pelatihan keamanan untuk karyawan, serta pengembangan rencana pemulihan bencana. Penggunaan teknologi keamanan yang tepat meliputi penggunaan *firewall*, enkripsi data, dan teknologi autentikasi ganda. *Firewall* adalah perangkat lunak atau perangkat keras yang digunakan untuk membatasi akses ke jaringan dan menghindari serangan dari pihak yang tidak berwenang. Enkripsi data adalah proses mengubah informasi menjadi kode rahasia sehingga hanya pihak yang berwenang yang dapat membaca dan mengaksesnya. Teknologi autentikasi ganda (*two-factor authentication*) melibatkan penggunaan dua jenis verifikasi untuk mengonfirmasi identitas pengguna sebelum diizinkan mengakses data atau sistem. Contohnya adalah penggunaan *password* dan kode yang dikirim ke perangkat seluler pengguna (Lin & Liao, 2017; Jurnal Entrepreneur, 2022).

Selain teknologi keamanan yang tepat, prosedur pengamanan yang ketat juga merupakan aspek penting dalam menjaga keamanan data. Hal ini termasuk kebijakan keamanan yang ketat, seperti pengaturan hak akses dan kontrol terhadap pengguna, serta kebijakan penggunaan perangkat yang aman dan diperbarui secara teratur (Tashia, 2017). Pelatihan keamanan untuk karyawan juga penting untuk meningkatkan kesadaran akan risiko keamanan data dan membantu karyawan untuk mengenali tanda-tanda serangan siber atau ancaman keamanan lainnya. Selain itu, pengembangan rencana pemulihan bencana juga perlu dilakukan untuk mengatasi kerugian yang mungkin terjadi akibat bencana alam atau serangan siber. Rencana pemulihan bencana harus mencakup prosedur untuk melakukan *backup* dan *restore* data, pemulihan sistem, dan pemulihan bisnis. Rencana ini harus diuji dan diperbarui secara berkala untuk memastikan bahwa organisasi siap menghadapi bencana atau kejadian yang merugikan (Hoesada, 2023).

Dalam era transformasi digital, perusahaan dapat menghadapi risiko keamanan data yang semakin kompleks dan meningkat. Oleh karena itu, organisasi harus memperhatikan pentingnya keamanan data dalam penggunaan teknologi digital. Penting untuk mengembangkan strategi keamanan data yang efektif dan terus memperbarui teknologi dan praktik keamanan untuk mengatasi risiko yang ada. Dengan demikian, organisasi dapat memastikan keamanan data dan meminimalkan risiko terhadap bisnis dan reputasi mereka (Bashar et al., 2022).

3.2. Teknologi *Blockchain*: Definisi, Karakteristik, dan Kelebihan

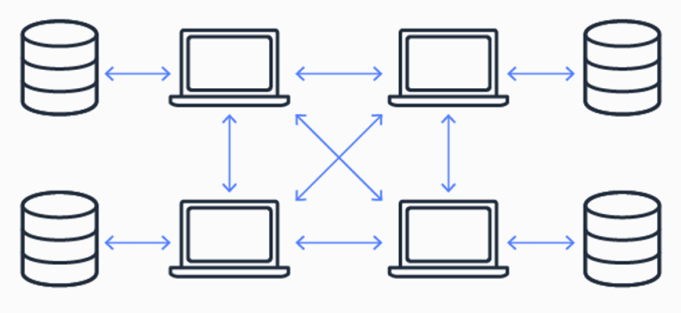
Teknologi *blockchain* telah banyak dikenal dalam beberapa tahun terakhir, terutama sebagai teknologi dasar dibalik *cryptocurrency* seperti *Bitcoin* (Azis et al., 2021). Namun, *blockchain* memiliki potensi yang jauh lebih besar dari sekedar sebagai dasar untuk *cryptocurrency* saja. *Blockchain* dapat digunakan untuk berbagai aplikasi lain dalam berbagai bidang, seperti perbankan, kesehatan, energi, dan lain-lain. Dalam konteks transformasi digital, *blockchain* juga dapat digunakan untuk meningkatkan keamanan data dalam transaksi *online*, pengolahan data terpusat, dan penyimpanan data secara digital. Salah satu kelebihan utama teknologi *blockchain* adalah kemampuannya untuk menyimpan dan mengirim data secara terdesentralisasi (*Centre for Innovation Policy and Governance*, 2018). Ini berarti bahwa data tidak terpusat di satu tempat, tetapi tersebar di seluruh jaringan. Setiap kali transaksi terjadi, data baru ditambahkan ke *blockchain* dan disimpan di setiap node jaringan yang terhubung. Ini berarti bahwa data yang disimpan di *blockchain* jauh lebih aman daripada data yang disimpan secara terpusat. Jika satu *node* dalam jaringan bermasalah atau diserang oleh peretas, data masih tersedia di *node* lain di jaringan (Liu et al., 2019; Argani & Taraka, 2020; Fazreen & Munajat, 2022).

Selain itu, *blockchain* juga memiliki sistem enkripsi yang kuat. Setiap data yang disimpan di *blockchain* dienkripsi dan hanya dapat diakses oleh orang yang memiliki

kunci enkripsi yang benar. Ini memastikan bahwa data yang disimpan di *blockchain* tidak dapat dibaca oleh pihak yang tidak berwenang, sehingga meningkatkan keamanan data secara signifikan. *Blockchain* juga memiliki sifat transparan yang sangat penting dalam konteks transformasi digital. Setiap transaksi atau blok dalam *blockchain* dapat diakses dan diverifikasi oleh semua pihak yang terlibat dalam transaksi. Ini berarti bahwa transaksi yang dilakukan di *blockchain* dapat dipantau dan diverifikasi oleh siapa saja, meningkatkan kepercayaan dan mengurangi risiko penipuan. Selain itu, *blockchain* juga sulit dimanipulasi. Setiap blok atau transaksi dalam *blockchain* terkait dengan blok sebelumnya dan setelahnya dalam urutan kronologis (Lin & Liao, 2017; Azis et al., 2021). Setiap *node* dalam jaringan harus menyetujui dan memverifikasi setiap transaksi baru sebelum ditambahkan ke *blockchain*. Jika ada upaya untuk memanipulasi data dalam satu blok, maka seluruh *blockchain* akan terpengaruh dan tidak akan disetujui oleh *node* lain di jaringan. Oleh karena itu, *blockchain* sangat aman dari upaya manipulasi data oleh pihak yang tidak berwenang.

Proses verifikasi dan validasi transaksi dalam *blockchain* juga sangat cepat dan efisien. Proses ini tidak memerlukan perantara atau pihak ketiga seperti bank atau lembaga keuangan, yang dapat mempercepat waktu transaksi dan mengurangi biaya yang terkait dengan transaksi. Dalam konteks transformasi digital, teknologi *blockchain* dapat digunakan untuk meningkatkan keamanan data dalam transaksi *online*. Saat ini, banyak transaksi *online* yang dilakukan melalui jaringan yang rentan terhadap serangan peretas. Data pribadi seperti nomor kartu kredit atau informasi pribadi lainnya dapat dicuri atau diretas dengan mudah, menyebabkan kerugian finansial dan keamanan. Dengan menggunakan *blockchain*, data yang disimpan dalam jaringan dapat dikunci dengan sistem enkripsi yang kuat sehingga hanya orang yang memiliki kunci enkripsi yang dapat mengakses dan membaca data tersebut. Ini berarti, keamanan data dapat ditingkatkan secara signifikan karena hanya pihak yang sah yang dapat mengakses data.

Selain itu, teknologi *blockchain* juga memungkinkan data untuk disimpan dan dibagikan dengan cara yang aman dan terdesentralisasi (Pratiwi, 2022). Dalam sistem tradisional, data disimpan dalam basis data terpusat yang diatur oleh satu atau beberapa perusahaan tertentu. Hal ini memungkinkan risiko keamanan yang lebih besar karena basis data tersebut dapat diakses dan dimanipulasi oleh orang-orang yang tidak berwenang. *Blockchain* juga memungkinkan data untuk disimpan secara terdesentralisasi. Ini berarti, data tidak disimpan di satu titik terpusat, melainkan disimpan di seluruh jaringan *blockchain* secara terdistribusi. Sehingga, setiap orang yang terhubung ke jaringan memiliki salinan yang sama dari data yang disimpan, dan jika satu salinan terkena serangan siber atau kerusakan lainnya, salinan lain masih dapat diakses (AWS, 2023).



Gambar 1. Ilustrasi Kerangka Kerja *Blockchain*

Sumber: *aws.amazon.com*

Keuntungan lain dari teknologi *blockchain* adalah kemampuannya untuk menciptakan transparansi yang tinggi dalam pengolahan data. Setiap transaksi atau blok dalam *blockchain* terkait dengan blok sebelumnya dan setelahnya, sehingga sulit bagi pihak yang tidak berwenang untuk memanipulasi data. Sehingga, *blockchain* dapat membantu mengurangi risiko penipuan, dan menghasilkan transparansi

dan kepercayaan dalam jaringan. Tidak hanya itu, teknologi *blockchain* juga dapat digunakan dalam berbagai sektor, termasuk sektor keuangan, kesehatan, logistik, dan lain-lain (Liu et al., 2019; AWS, 2023). Misalnya, dalam sektor keuangan, *blockchain* dapat digunakan untuk meningkatkan keamanan transaksi dan mengurangi biaya yang terkait dengan proses verifikasi dan validasi. Hal ini dapat membantu mengurangi biaya transaksi dan meningkatkan kecepatan penyelesaian transaksi. Di sektor kesehatan, *blockchain* dapat digunakan untuk memperkuat keamanan data medis dan meningkatkan interoperabilitas antara sistem medis yang berbeda. Dalam sektor logistik, *blockchain* dapat digunakan untuk meningkatkan transparansi dan akuntabilitas dalam rantai pasokan, yang dapat membantu mempercepat proses pengiriman dan mengurangi biaya pengiriman (Pusat Inovasi Kota dan Komunitas Cerdas, 2021).

Selain itu, *blockchain* juga dapat digunakan dalam aplikasi *IoT (Internet of Things)*. Kombinasi antara *blockchain* dan *IoT* dapat membantu meningkatkan keamanan dan privasi dalam pengolahan data yang dihasilkan oleh perangkat IoT (Liu et al., 2019). Misalnya, pada sistem pengumpulan *data smart city, blockchain* dapat digunakan untuk memberikan verifikasi dan validasi yang aman atas data yang dikumpulkan. Meskipun *blockchain* menawarkan banyak manfaat, masih ada beberapa tantangan yang perlu diatasi. Salah satu tantangan terbesar adalah masalah skalabilitas. Dalam *blockchain*, setiap transaksi harus diverifikasi oleh *node* dalam jaringan sebelum disimpan di *blockchain*. Hal ini dapat memperlambat proses dan meningkatkan biaya transaksi ketika jaringan dalam kondisi lemah (Atmomintarso & Wirawan, 2021).

Namun, teknologi *blockchain* hingga saat ini terus mengalami perkembangan dan peningkatan kinerja yang signifikan. Beberapa inovasi seperti algoritma konsensus baru dan penggunaan teknologi sampingan seperti *Lightning Network* telah mempercepat proses verifikasi dan validasi transaksi dalam jaringan *blockchain*, sehingga mengurangi biaya transaksi dan meningkatkan skala penggunaan (Pluang, 2022). Penggunaan teknologi *blockchain* dalam transformasi digital juga tidak terbatas pada sektor keuangan. Berbagai sektor industri juga mulai mengadopsi teknologi *blockchain* untuk meningkatkan keamanan dan efisiensi dalam proses bisnis mereka. Sebagai contoh, dalam industri logistik, teknologi *blockchain* dapat digunakan untuk melacak pengiriman barang dengan lebih akurat dan transparan. Data mengenai pengiriman barang, mulai dari lokasi, waktu, hingga kondisi pengiriman, dapat disimpan dalam *blockchain* dan diakses oleh semua pihak yang terlibat dalam proses pengiriman (Teknik Logistik, 2021; AWS, 2023).

Sementara itu, dalam sektor kesehatan, teknologi *blockchain* dapat digunakan untuk menyimpan dan membagikan data medis pasien dengan aman dan terenkripsi. Hal ini dapat meningkatkan keamanan dan privasi data medis pasien, serta memudahkan proses berbagi data medis antara berbagai pihak yang terlibat dalam perawatan pasien. Di Indonesia, beberapa perusahaan dan institusi mulai mengadopsi teknologi *blockchain* dalam transformasi digital mereka. Sebagai contoh, Bank Indonesia (BI) telah meluncurkan sistem pembayaran digital yang berbasis *blockchain* bernama *Bank Indonesia Payment System (BI-PS)*. Sistem ini memungkinkan transaksi pembayaran dengan cepat, aman, dan hemat biaya melalui teknologi *blockchain* (Bank Indonesia, 2020). Meskipun penggunaan teknologi *blockchain* semakin meluas di Indonesia, masih ada beberapa tantangan dan hambatan yang perlu diatasi. Salah satu tantangan utama adalah kurangnya pemahaman dan kesadaran tentang teknologi *blockchain* di kalangan masyarakat dan pebisnis. Hal ini dapat menghambat adopsi teknologi *blockchain* di berbagai sektor bisnis.

Selain itu, regulasi yang belum jelas dan konsisten juga menjadi hambatan bagi penggunaan teknologi *blockchain* di Indonesia. Meskipun BI telah meluncurkan regulasi terkait penggunaan teknologi *blockchain*, namun masih banyak institusi dan perusahaan yang belum sepenuhnya memahami dan menerapkan regulasi tersebut. Namun, meskipun masih ada beberapa tantangan yang perlu diatasi, penggunaan teknologi *blockchain* dalam transformasi digital di Indonesia terus berkembang dan menunjukkan potensi yang besar untuk meningkatkan keamanan dan efisiensi dalam

berbagai sektor industri (Bashar et al., 2022). Dengan adanya inovasi dan pemahaman yang lebih baik tentang teknologi *blockchain*, diharapkan penggunaan teknologi ini dapat semakin meluas di masa yang akan datang.

3.3. Implementasi Blockchain dalam Transformasi Digital di Indonesia

Dalam era transformasi digital, penggunaan teknologi *blockchain* di Indonesia memberikan potensi besar dalam meningkatkan keamanan data dan efisiensi dalam berbagai sektor (Argani & Taraka, 2020). Pemerintah Indonesia telah meluncurkan berbagai inisiatif untuk memperkuat penggunaan teknologi digital di negara ini, seperti penggunaan teknologi *blockchain* untuk verifikasi dan validasi sertifikat pendidikan, penyimpanan data medis, dan sistem pembayaran. Meskipun demikian, implementasi teknologi *blockchain* di Indonesia masih menghadapi beberapa tantangan, seperti regulasi yang belum jelas, infrastruktur yang masih terbatas, dan kurangnya pemahaman tentang teknologi *blockchain* (*Centre for Innovation Policy and Governance*, 2018).

Salah satu proyek penggunaan teknologi *blockchain* di Indonesia adalah solusi verifikasi dan validasi sertifikat pendidikan (Argani & Taraka, 2020). Pemerintah Indonesia telah bekerja sama dengan beberapa perusahaan *blockchain* untuk mengembangkan solusi ini. Dengan menggunakan teknologi *blockchain*, proses verifikasi dan validasi sertifikat pendidikan dapat dilakukan dengan cepat dan efisien. Solusi ini memberikan keuntungan bagi pihak-pihak yang membutuhkan verifikasi sertifikat pendidikan, seperti pihak-pihak yang sedang melakukan perekrutan karyawan. Proses verifikasi sertifikat pendidikan yang cepat dan akurat juga dapat membantu mengurangi risiko penipuan dalam proses perekrutan. Selain itu, teknologi *blockchain* juga digunakan dalam penyimpanan data medis di beberapa rumah sakit di Indonesia (Hoesada, 2023). Dengan menggunakan teknologi *blockchain*, pasien dapat mengakses data medis mereka dengan aman dan nyaman, dan dokter dan rumah sakit dapat memperoleh data medis dengan cepat dan efisien. Keamanan data medis sangat penting dalam menjaga kerahasiaan pasien dan mencegah manipulasi atau perubahan data medis. Pada sektor pembayaran, teknologi *blockchain* digunakan dalam penggunaan *cryptocurrency* atau token sebagai alat pembayaran. Salah satu contoh penggunaan teknologi *blockchain* dalam sistem pembayaran di Indonesia adalah *platform Tokocrypto*. Platform ini memungkinkan pengguna untuk membeli dan menjual *cryptocurrency* dengan mudah dan aman (Azis et al., 2021). Selain itu, penggunaan *cryptocurrency* juga dapat memfasilitasi perdagangan internasional, karena transaksi menggunakan *cryptocurrency* dapat dilakukan dengan cepat dan aman tanpa memerlukan perantara.

Meskipun penggunaan teknologi *blockchain* di Indonesia menawarkan banyak manfaat, namun implementasinya masih menghadapi beberapa tantangan. Salah satu tantangan yang dihadapi adalah regulasi yang belum jelas seperti regulasi tentang pajak dan keamanan data (Atmomintarso & Wirawan, 2021; Budhijanto, 2023). Kondisi ini dapat membingungkan perusahaan yang ingin mengadopsi teknologi *blockchain*, karena mereka tidak yakin tentang implikasi pajak dan aspek hukum lainnya. Tantangan lainnya adalah infrastruktur digital yang masih terbatas di Indonesia, terutama di daerah-daerah yang terpencil. Infrastruktur digital yang cepat dan stabil sangat penting dalam mengadopsi teknologi *blockchain*, karena teknologi *blockchain* memerlukan akses internet yang cepat dan stabil. Kurangnya infrastruktur digital yang memadai dapat mempersulit implementasi teknologi *blockchain* yang memerlukan akses internet yang cepat dan stabil (Atmomintarso & Wirawan, 2021; Iswanto et al., 2022). Masalah ini menjadi perhatian bagi pemerintah Indonesia, dan saat ini sedang dilakukan berbagai upaya untuk meningkatkan akses internet di seluruh wilayah Indonesia. Salah satu inisiatif yang dilakukan adalah program Palapa Ring, yang bertujuan untuk membangun infrastruktur jaringan internet di seluruh Indonesia. Selain itu, pemerintah juga berencana untuk membangun pusat data nasional untuk memfasilitasi penyimpanan data secara terpusat dan aman.

Selain tantangan infrastruktur, kurangnya pemahaman tentang teknologi *blockchain* juga menjadi masalah dalam mengadopsi teknologi ini di Indonesia. Beberapa orang mungkin masih menganggap *blockchain* sebagai teknologi yang terlalu kompleks dan sulit dipahami (Maulani et al., 2023). Untuk mengatasi masalah ini, pemerintah dan sektor swasta perlu meningkatkan kampanye edukasi dan sosialisasi tentang teknologi *blockchain* dan manfaatnya bagi masyarakat. Pelatihan dan kursus tentang *blockchain* dapat diberikan kepada pelajar, mahasiswa, dan masyarakat umum untuk meningkatkan pemahaman dan kesadaran tentang teknologi ini.

Selain itu, regulasu yang belum jelas juga menjadi tantangan dalam mengadopsi teknologi *blockchain* di Indonesia. Meskipun pemerintah Indonesia telah mengeluarkan beberapa regulasi terkait teknologi *blockchain*, masih banyak regulasi yang belum jelas dan perlu diperjelas. Beberapa hal yang perlu diatur antara lain adalah keamanan data, perlindungan konsumen, dan pajak (Nugroho et al., 2021; Pusat Inovasi Kota dan Komunitas Cerdas, 2021). Regulasi yang jelas dan transparan akan memberikan kepastian hukum dan mempermudah penggunaan teknologi *blockchain* di Indonesia. Untuk mempercepat adopsi teknologi *blockchain* di Indonesia, pemerintah dan sektor swasta perlu terus mendorong dan mendukung penggunaan teknologi ini. Pemerintah dapat memberikan insentif bagi perusahaan dan startup yang mengembangkan solusi *blockchain*, seperti pajak yang lebih rendah atau akses ke pendanaan yang lebih mudah (Atmomintarso & Wirawan, 2021; Saefudin, 2022). Selain itu, pemerintah dapat bekerja sama dengan perusahaan blockchain dalam mengembangkan solusi *blockchain* yang sesuai dengan kebutuhan masyarakat Indonesia. Sementara itu, sektor swasta juga dapat berperan aktif dalam mengadopsi teknologi *blockchain*. Perusahaan dapat mengembangkan solusi *blockchain* untuk meningkatkan keamanan data, meningkatkan efisiensi operasional, dan mengurangi biaya. Selain itu, perusahaan dapat mengadopsi teknologi *blockchain* dalam sistem pembayaran dan perdagangan (Sutandi, 2018).

Secara keseluruhan, implementasi teknologi *blockchain* dalam transformasi digital di Indonesia memiliki potensi besar untuk meningkatkan keamanan data dan efisiensi operasional (Trinowo, 2020; AWS, 2023; Maulani et al., 2023). Meskipun masih menghadapi beberapa tantangan, seperti infrastruktur yang masih terbatas, kurangnya pemahaman tentang teknologi *blockchain*, dan regulasi yang belum jelas, namun pemerintah dan sektor swasta dapat bekerja sama untuk mengatasi tantangan tersebut dan mempercepat adopsi teknologi *blockchain* di Indonesia (Nugroho et al., 2021). Dengan adopsi teknologi *blockchain* yang tepat, Indonesia dapat menjadi pemain penting dalam ekosistem *blockchain* global dan memperkuat posisinya sebagai negara yang sedang melakukan transformasi digital yang pesat. Selain tantangan yang dihadapi, implementasi teknologi *blockchain* dalam transformasi digital di Indonesia juga memiliki potensi untuk memberikan manfaat besar. Penggunaan teknologi *blockchain* dalam transformasi digital dapat meningkatkan efisiensi, transparansi, dan keamanan data dalam berbagai sektor, seperti sektor keuangan, kesehatan, dan pendidikan (Pluang, 2022). Implementasi teknologi *blockchain* juga dapat membantu meningkatkan keterlibatan masyarakat dalam proses pemerintahan, seperti melalui sistem voting elektronik yang aman dan transparan. Pemerintah Indonesia juga telah menyadari potensi besar dari teknologi *blockchain* dalam transformasi digital. Pemerintah Indonesia telah berkomitmen untuk meningkatkan penggunaan teknologi *blockchain* dalam berbagai sektor, seperti dalam pembangunan *Smart City* dan pembayaran digital. Pemerintah Indonesia juga telah bekerja sama dengan berbagai perusahaan teknologi blockchain dalam mempromosikan penggunaan teknologi *blockchain* di Indonesia (Saefudin, 2022).

Selain itu, sejumlah lembaga riset dan pendidikan juga mulai mengembangkan penelitian dan pengajaran tentang teknologi *blockchain* di Indonesia. Hal ini diharapkan dapat meningkatkan pemahaman dan keterampilan masyarakat Indonesia dalam memanfaatkan teknologi *blockchain* untuk menghadapi tantangan transformasi digital (Pusat Inovasi Kota dan Komunitas Cerdas, 2021; Iswanto et al., 2022). Dalam konteks global, implementasi teknologi *blockchain* dalam transformasi digital menjadi

trend yang semakin berkembang di seluruh dunia. Negara maju seperti Amerika Serikat dan China, telah mengembangkan inisiatif dan proyek penggunaan teknologi *blockchain* dalam berbagai sektor. Indonesia perlu terus mengembangkan dan meningkatkan penggunaan teknologi *blockchain* dalam transformasi digital agar tidak tertinggal dari negara-negara lain (Liu et al., 2019). Secara keseluruhan, implementasi teknologi *blockchain* dalam transformasi digital di Indonesia memiliki potensi besar untuk meningkatkan keamanan dan efisiensi data, serta memungkinkan terciptanya inovasi baru dalam berbagai sektor. Meskipun menghadapi tantangan, pemerintah Indonesia dan berbagai pemangku kepentingan perlu terus mengembangkan dan mempromosikan penggunaan teknologi *blockchain* agar Indonesia dapat mengambil manfaat penuh dari transformasi digital (*Centre for Innovation Policy and Governance,* 2018; Panggabean, 2022).

3.4. Manfaat dan Risiko Penggunaan Blockchain untuk Keamanan Data

Penggunaan teknologi *blockchain* dalam meningkatkan keamanan data memiliki sejumlah manfaat yang signifikan. Pertama, teknologi ini memberikan keamanan data yang lebih baik dibandingkan dengan teknologi konvensional. Dalam teknologi *blockchain*, data disimpan secara terdesentralisasi dan terenkripsi, sehingga meningkatkan keamanan dan meminimalkan risiko pengrusakan atau manipulasi data. Data yang disimpan dalam *blockchain* juga memiliki tingkat integritas yang tinggi, karena setiap transaksi dan data yang dimasukkan ke dalam *blockchain* tidak dapat diubah atau dihapus tanpa persetujuan dari semua pihak yang terlibat (Pluang, 2022). Disisi lain, teknologi *blockchain* juga memberikan transparansi yang lebih tinggi dalam setiap transaksi atau data yang dilakukan (Panggabean, 2022; Maulani et al., 2023). Karena semua transaksi dan data dapat diverifikasi oleh semua pihak yang terlibat, maka risiko penipuan atau kecurangan dapat dikurangi secara signifikan. Ini dapat memberikan manfaat bagi berbagai sektor, seperti sektor keuangan atau logistik, yang memerlukan transaksi atau data yang akurat dan terpercaya.

Teknologi *blockchain* juga memberikan efisiensi dan kecepatan dalam proses verifikasi dan validasi data (Lin & Liao, 2017; Fazreen & Munajat, 2022). Dalam teknologi *blockchain*, setiap transaksi dapat diverifikasi dengan cepat dan efisien, tanpa perlu melalui perantara atau pihak ketiga. Hal ini dapat mengurangi biaya dan waktu yang dibutuhkan dalam proses verifikasi dan validasi data, serta mempercepat waktu transaksi. Namun, penggunaan teknologi *blockchain* juga memiliki beberapa risiko yang perlu diperhatikan. Salah satunya adalah ketergantungan pada teknologi *blockchain* itu sendiri. Jika teknologi ini mengalami masalah atau kegagalan, maka data dan transaksi yang disimpan dalam *blockchain* juga akan terkena dampaknya. Selain itu, risiko keamanan juga menjadi perhatian utama dalam penggunaan teknologi *blockchain* (Bashar et al., 2022). Meskipun teknologi ini diklaim aman, namun tidak menutup kemungkinan adanya serangan yang berhasil menembus sistem keamanannya (Lin & Liao, 2017; Liu et al., 2019). Keterbatasan skalabilitas juga menjadi tantangan dalam penggunaan teknologi *blockchain*. Teknologi ini memiliki keterbatasan dalam skala dan kapasitas transaksi yang dapat ditangani. Hal ini menjadi tantangan jika digunakan dalam implementasi transformasi digital yang besar dan kompleks (Maulani et al., 2023). Oleh karena itu, perlu dilakukan perencanaan dan pengelolaan yang matang dalam penggunaan teknologi *blockchain* dalam implementasi transformasi digital (Panggabean, 2022). Secara keseluruhan, penggunaan teknologi *blockchain* dalam meningkatkan keamanan data memberikan manfaat yang signifikan, seperti keamanan data yang lebih baik, transparansi, efisiensi, dan kecepatan. Namun, penggunaan teknologi *blockchain* juga memiliki risiko, seperti ketergantungan pada teknologi, risiko keamanan, dan keterbatasan skalabilitas. Oleh karena itu, perlu dilakukan perencanaan dan pengelolaan yang matang dalam penggunaan teknologi blockchain dalam implementasi transformasi digital di Indonesia (Liu et al., 2019; Panggabean, 2022).

4. Kesimpulan

Dalam era transformasi digital yang pesat, penggunaan teknologi *blockchain* memiliki potensi besar untuk meningkatkan keamanan data dan mengurangi risiko manipulasi atau perubahan data oleh pihak yang tidak berwenang. Pemerintah Indonesia telah memperhatikan potensi tersebut dan mengeluarkan regulasi dan strategi untuk meningkatkan penggunaan teknologi *blockchain* dalam operasional pemerintah dan sektor swasta. Beberapa proyek penggunaan teknologi *blockchain* di Indonesia telah dilakukan, seperti verifikasi dan validasi sertifikat pendidikan, penyimpanan data medis, dan penggunaan *cryptocurrency* sebagai alat pembayaran (Manurung & Wijoyo, 2021). Meskipun demikian, implementasi teknologi *blockchain* di Indonesia masih menghadapi beberapa tantangan, seperti regulasi yang belum jelas, infrastruktur yang masih terbatas, dan kurangnya pemahaman tentang teknologi *blockchain*. Untuk mengatasi tantangan tersebut, pemerintah Indonesia perlu meningkatkan regulasi dan kebijakan terkait dengan teknologi *blockchain*, terutama terkait dengan pajak dan keamanan data (Maulani et al., 2023). Selain itu, pemerintah perlu meningkatkan infrastruktur digital di Indonesia, terutama di daerah-daerah terpencil, sehingga implementasi teknologi *blockchain* dapat berjalan dengan lancar. Selain pemerintah, perusahaan-perusahaan di Indonesia juga perlu memperhatikan penggunaan teknologi *blockchain* untuk meningkatkan keamanan data dalam operasional mereka.

Peningkatan pemahaman tentang teknologi *blockchain* juga perlu dilakukan melalui edukasi dan sosialisasi kepada masyarakat. Di sisi lain, perusahaan teknologi *blockchain* juga perlu memperhatikan potensi pasar Indonesia yang besar dan mulai memperluas bisnis mereka ke Indonesia (*Centre for Innovation Policy and Governance,* 2018). Peningkatan jumlah perusahaan teknologi *blockchain* di Indonesia dapat membuka peluang baru dalam penggunaan teknologi *blockchain* dan mendorong pertumbuhan ekonomi digital di Indonesia (Panggabean, 2022). Dalam kesimpulan, penggunaan teknologi *blockchain* dalam transformasi digital di Indonesia memiliki potensi besar untuk meningkatkan keamanan data dan mendorong pertumbuhan ekonomi digital (Pusat Inovasi Kota dan Komunitas Cerdas, 2021). Meskipun demikian, implementasi teknologi *blockchain* masih menghadapi beberapa tantangan yang perlu diatasi oleh pemerintah dan perusahaan di Indonesia (Putra et al., 2019; Saefudin, 2022). Dengan upaya bersama, penggunaan teknologi *blockchain* dapat diintegrasikan dengan baik dalam transformasi digital di Indonesia dan membawa manfaat bagi masyarakat dan perekonomian Indonesia secara keseluruhan.

UCAPAN TERIMA KASIH

Terima kasih saya sampaikan kepada Universitas Dian Nuswantoro yang mana telah memberikan atas selesainya penelitian ini. Saya sampaikan kepada Kementerian Dalam Negeri karena telah memfasilitasi kami untuk menulis demi masa depan Indonesia yang lebih baik. Dan juga pihak-pihak terkait lainya yang tidak bisa disebutkan satu persatu sudah membantu dalam penelitian ini. Serta Tim Rekdaksi JPKP yang telah memberikan Kesempatan dalam mempublikasikan hasil penelian ini.

REFERENSI

Argani, A., & Taraka, W. (2020). Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi. P*emanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi, 1*(1). https://doi.org/10.34306/abdi.v1i1.121

Atmomintarso, B. E., & Wirawan. (2021). Sistem Pelaporan Pajak Pertambahan Nilai pada Web dengan Menggunakan Teknik Blockchain. *Jurnal Teknik ITS, 10*(2), 175-181. https://media.neliti.com/media/publications/499988-none-094e50e4.pdf

AWS. (2023). *Apa itu Teknologi Blockchain? - Penjelasan tentang Blockchain - AWS. Amazon AWS*. Retrieved February 9, 2023, from https://aws.amazon.com/id/what-is/blockchain/

Azis, M. T. E., Apriani, ,. R., & Kamal, M. F. (2021). Perlindungan Hukum Investasi Mata Uang Digital (Cryptocurrency). *Jurnal Pemikiran dan Penelitian Ilmu-ilmu Sosial, Hukum, & Pengajarannya, 16*(2). https://ojs.unm.ac.id/supremasi

Bank Indonesia. (2020). *Sistem Pembayaran & Pengelolaan Uang Rupiah*. Bank Indonesia. Retrieved February 24, 2023, from https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/default.aspx

Bashar, H. S., Purnamasari, H., & Priyanti, E. (2022). Analisis Penerapan Blockchain Di Indonesia, Menuju Revolusi Pelayanan Publik Dan Kearsipan. *Nusantara (Jurnal Ilmu Pengetahuan Sosial), 9*(8). http://dx.doi.org/10.31604/jips.v9i8.2022.3023-3029

Budhijanto, D. (2023). *Blockchain Law, Pelindungan Data Pribadi dalam Ekonomi Digital*. Hukumonline. Retrieved Februari 10, 2023, from https://www.hukumonline.com/berita/a/blockchain-law--pelindungan-data-pribadi-dalam-ekonomi-digital-lt63cf37949e450/

Centre for Innovation Policy and Governance. (2018). *Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia Usulan Desain, Prinsip, dan Rekomendasi Kebijakan*. Ditjen Aptika. Retrieved Desember 12, 2022, from https://aptika.kominfo.go.id/wp-content/uploads/2018/12/Kajian-Kominfo-CIPG-compressed.pdf

Fazreen, T., & Munajat, M. D. E. (2022). SOLUSI PEMANFAATAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI PERMASALAHAN PENYALURAN DANA BANTUAN SOSIAL COVID-19. *JANE (Jurnal Administrasi Negara), 12*(2).

Hoesada, J. (2023). *Disaster Recovery Planning: Manajemen Bencana Administrasi dan Akuntansi*. CRMS. Retrieved February 14, 2023, from https://crmsindonesia.org/publications/disaster-recovery-planning-manajemen-bencana-administrasi-dan-akuntansi/

Iswanto, Putri, N. I., Munawar, Z., Komalasari, R., & Widhiantoro, D. (2022). Pemanfaatan Teknologi Blockchain di Bidang Pendidikan. *ematik : Jurnal Teknologi Informasi Komunikasi (e-Journal), 9*(2), 171-181. https://doi.org/10.38204/tematik.v9i2.1082

Jurnal Entrepreneur. (2022). *Sistem Informasi Manajemen dan Manfaatnya bagi Perusahaan - Mekari Jurnal*. Jurnal.id. Retrieved Februari 13, 2023, from https://www.jurnal.id/id/blog/mengenal-sistem-informasi-manajemen-dan-manfaatnya-bagi-perusahaan/

Kim, H., Sefcik, J. S., & Bradway, C. (2017). Characteristics of Qualitative Descriptive Studies: A Systematic Review. *Wiley Online Library, 40*(1), 23-42. https://doi.org/10.1002%2Fnur.21768

Lin, I. -C., & Liao, T. -C. (2017). A Survey of Blockchain Security Issues and Challenges. *Airiti Library, 19*(5). http://dx.doi.org/10.6633/IJNS.201709.19(5).01

Liu, C. H., Lin, Q., & Wen, S. (2019). Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning. *IEEE Transactions on Industrial Informatics, 15*(6), 3516-3526. https://doi.org/10.1109/TII.2018.2890203

Manurung, R., & Wijoyo, H. (2021). *Sistem Informasi Akuntansi Cryptocurrency Bitcoin*. Insan Cendekia Mandiri, indonesia.

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). PENERAPAN TEKNOLOGI BLOCKCHAIN PADA SISTEM KEAMANAN INFORMASI. *Jurnal Sosial dan Teknologi (SOSTECH), 3*(2). https://sostech.greenvest.co.id/index.php/sostech/article/view/634/1006

Moleong. (2014). *Metode Penelitian Kualitati*. Remaja Rosdakarya. Bandung.

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 1*(2). https://doi.org/10.15294/ipmhi.v1i2.53698

Panggabean, A. N. (2022). *Memahami Dan Mengelola Transformasi Digital*. OSF Preprints. https://doi.org/10.31219/osf.io/s36wq

Pluang. (2022). *Mengenal Konsep Algoritma Konsensus Dalam Blockchain*. Apakah Itu? Pluang.com. Retrieved February 18, 2023, from https://pluang.com/id/blog/resource/mengenal-konsep-algoritma-konsensus

Pratiwi, L. L. (2022). Implementasi Blockchain Pada Akuntansi Dan Audit Di Indonesia. *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan, 4*(6).

Pusat Inovasi Kota dan Komunitas Cerdas. (2021). *Penerapan Teknologi Blockchain pada Industri Kesehatan*. PIKKC. Retrieved February 5, 2023, from https://citylab.itb.ac.id/pikkc/2021/10/13/penerapan-teknologi-blockchain-pada-industri-kesehatan/

Putra, H. F., Wirawan, W., & Penangsang, O. (2019). Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid. *E-Jurnal ITS, 8*(1). http://dx.doi.org/10.12962/j23373539.v8i1.38525

Saefudin. (2022). *Gerakan Smart City sebagai Muara Kemajuan Transformasi Digital Indonesia*. Ditjen Aptika. Retrieved January 4, 2023, from https://aptika.kominfo.go.id/2022/12/gerakan-smart-city-sebagai-muara-kemajuan-transformasi-digital-indonesia/

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *SASI, 27*(1). https://doi.org/10.47268/sasi.v27i1

Sutandi. (2018). Pengaruh Big Data Dan Teknologi Blockchain Terhadap Model Bisnis Sektor Logistik Dengan Pendekatan Business Model Canvas . *Jurnal Logistik Indonesia, 2*(1).

Tashia. (2017). *Keamanan Jaringan Internet dan Firewall – Ditjen Aptika*. Ditjen Aptika. Retrieved February 11, 2023, from https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/

Teknik Logistik. (2021). *Pemanfaatan Blockchain dalam Dunia Logistik - Teknik Logistik*. Teknik Logistik. Retrieved February 24, 2023, from https://tekniklogistik.ittelkom-pwt.ac.id/pemanfaatan-blockchain-dalam-dunia-logistik/

Trinowo, L. E. (2020). *Blockchain Proof-of-Work Threat: 51% Attack*. Budi Rahardjo. Retrieved January 12, 2023, from http://budi.rahardjo.id/files/courses/2020STEI/18217018_Makalah_Luthfi_Eko_Trinowo.pdf

Universitas Islam Indonesia. (2021). *Blockchain Tingkatkan Keamanan Data Dari Peretasan - UII*. Universitas Islam Indonesia. Retrieved Januari 11, 2023, from https://www.uii.ac.id/blockchain-tingkatkan-keamanan-data-dari-peretasan/