Journal of Empowerment Community and Education
Volume 3 Nomor 2 Tahun: 2023 e-ISSN : 2774-8308

BLOCKCHAIN UNTUK SISTEM PENYIMPANAN DATA PADA ORGANISASI PEMERINTAH

Fikroh Amali Fahmi Addiani[1*)]

[1)] Department of Civil Engineering, Faculty of Engineering, Universitas Indonesia, Salemba, Indonesia, fahmiaddi@yahoo.co.id
*Corresponding author
Email : fahmiaddi@yahoo.co.id

Article history
Received : 18 September 2023
Revised : 24 Oktober 2023
Accepted : 28 Oktober 2023

Abstrak, dalam bahasa Indonesia

Data-data rahasia yang dimiliki oleh Pemerintah Indonesia memerlukan pusat data yang wajib dikelola sendiri oleh Pemerintah, dan membutuhkan waktu lama dan biaya tinggi dalam pembangunannya. Keamanan dalam sharing data rawan terhadap serangan siber. Dengan semakin meningkatnya data yang ada setiap tahunnya, penting untuk memperhatikan aspek infrastruktur, penyimpanan kerahasiaan, dan keamanan data yang tersimpan serta ketersediaan data dan integrasi data lama dalam media penyimpanan yang lebih besar. Dalam sistem cloud storage, pengendalian data bersifat terpusat sehingga tidak menjamin kerahasiaan, integritas dan keaslian data. Untuk itu dibutuhkan teknologi penyimpanan data terdistribusi yang dapat menjamin keaslian, kerahasiaan dan integritas data. Sistem cloud storage memiliki beberapa risiko antara lain rendahnya tingkat keamanan; kehilangan data karena kerusakan entitas atau penghapusan oleh orang yang tidak berwenang; kehilangan akses; serta perubahan atau modifikasi data di luar kontrol karena tidak adanya log aktivitas dan transparansi. Teknologi *blockchain* dapat dimanfaatkan untuk penyimpanan data terdistribusi karena bersifat peer-to-peer, tanpa pihak ketiga, dan bersifat transparan serta terjamin keamanannya karena tereplikasi di seluruh jaringan *blockchain*. Artikel ini memaparkan solusi atas berbagai permasalahan yang muncul sebagai faktor-faktor risiko dalam sistem cloud storage melalui teknologi *blockchain* sehingga dapat diimplementasikan sebagai sistem penyimpanan data organisasi pemerintah.

Kata Kunci : keamanan data; cloud storage; organisasi pemerintah; teknologi *blockchain*

PENDAHULUAN

Keamanan siber atau keamanan teknologi informasi menyangkut perlindungan dan meminimalkan gangguan terhadap aspek-aspek kerahasiaan, integritas, dan ketersediaan [1] atas aset informasi yang meliputi penggunaan, penyimpanan atau pengiriman informasi melalui penerapan kebijakan, pendidikan dan teknologi [2].

Ancaman keamanan siber juga terjadi pada organisasi pemerintahan. Menurut data dari IBM X-Force Threat Intellegence Index 2019, Organisasi Pemerintah menduduki peringkat ketujuh untuk industri dengan ancaman keamanan siber terbesar (8%). Pelanggaran yang terjadi meliputi penggunaan, penjualan, dan pengiriman informasi, utamanya untuk keuntungan ekonomi dan politik.

Organisasi Pemerintah mengelola banyak data dan informasi rahasia yang bernilai kritis. Untuk menjaga data dan informasi dari seluruh ancaman, maka dibutuhkan sistem penyimpanan data dan informasi yang mumpuni dari sisi keamanan, akses, dan penyediaan informasi secara cepat dan akurat.

Keamanan dalam sharing data rawan terhadap serangan siber. Data yang ada semakin meningkat setiap tahunnya, sehingga penting untuk memperhatikan aspek infrastruktur, penyimpanan kerahasiaan, dan keamanan data yang tersimpan serta integrasi data lama dalam media penyimpanan yang lebih besar [5].

Dalam sistem basis data tradisional seperti cloud storage, pengendalian data bersifat terpusat sehingga tidak menjamin kerahasiaan, integritas dan keaslian data. Untuk itu dibutuhkan teknologi penyimpanan data terdistribusi yang dapat menjamin keaslian, kerahasiaan dan integritas data [6].

Berdasarkan Cloud Readiness Index (CRI) 2018, hasil penelitian Asia Cloud Computing Association tahun 2018, Indonesia menempati urutan ke-11 dengan total nilai 49,4 dari 100 jika dibandingkan dengan negara-negara di Asia Pasifik untuk pertumbuhan media penyimpanan berbasis komputasi awan [3].

Indonesia seharusnya memprioritaskan inisiatif untuk meningkatkan infrastruktur komputasi awan seperti dengan meningkatkan kecepatan broadband dan penyediaan listrik yang lebih dapat diandalkan.

Selain itu, meskipun mengalami penambahan infrastruktur pusat data setiap tahunnya namun tidak cukup signifikan untuk memenuhi kebutuhan komputasi awan di Indonesia khususnya bagi organisasi pemerintah. Dokumen-dokumen rahasia yang dimiliki oleh Pemerintah Indonesia memerlukan pusat data yang wajib dikelola sendiri oleh Pemerintah, dan membutuhkan waktu lama dan biaya tinggi dalam pembangunannya [4].

Sistem penyimpanan data berbasis komputasi awan memiliki beberapa risiko antara lain rendahnya tingkat keamanan sistem; kehilangan data karena kerusakan entitas; kehilangan data kerena penghapusan oleh orang yang tidak berwenang; kehilangan akses karena penutupan/kerusakan entitas; kehilangan akses karena tidak ada koneksi internet; kehilangan akses karena masalah konfigurasi OS; serta perubahan atau modifikasi data karena tidak adanya log aktivitas dan transaksi yang tidak transparan.

Teknologi *blockchain* adalah teknologi yang dapat dimanfaatkan untuk penyimpanan data terdistribusi karena bersifat peer-to-peer, sehingga dalam prosesnya data dapat dipindahkan dari satu pengguna ke pengguna lainnya tanpa melibatkan pihak ketiga, dan semua transaksi bersifat transparan serta penyimpanan data terjamin keamanannya karena tereplikasi di seluruh jaringan *blockchain* [1].

Artikel ini menyajikan informasi mengenai kekurangan-kekurangan pada sistem cloud storage yang dapat diatasi dengan kelebihan *blockchain* sebagai basis sistem penyimpanan data.

METODE

Penelitian ini dilakukan untuk mengetahui faktor-faktor risiko pada sistem penyimpanan data berbasis komputasi awan. Dari faktor-faktor risiko ini kemudian dianalisa dan dicari solusi pemecahannya berdasarkan pendekatan sifat dan karakter *blockchain* melalui studi literatur untuk mengetahui apakah kelebihan *blockchain* dapat menjadi penyelesaian permasalahan (risiko) dalam sistem penyimpanan data.

HASIL DAN PEMBAHASAN

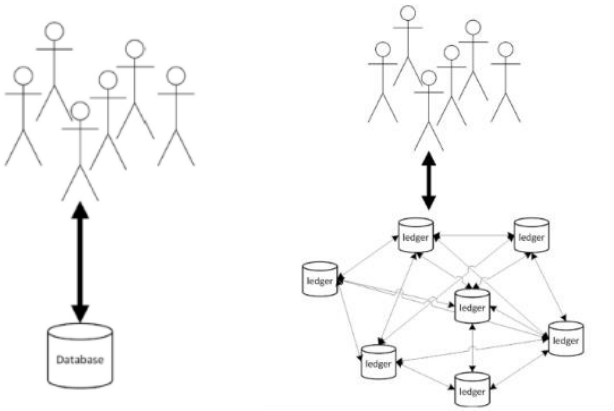
Sistem Penyimpanan Data berbasis Komputasi Awan

Menurut [7] berdasarkan basis datanya (database) sistem penyimpanan data dapat diklasifikasikan menjadi terpusat (centralized), dan terdesentralisasi atau terdistribusi (decentralized). Basis data terpusat adalah adalah suatu sistem yang mengatur semua data dalam single node. Sistem ini mudah untuk dikelola tetapi reliabilitas dan ketersediaannya rendah [8]. Contoh basis data centralized adalah cloud storage.

Sedangkan pada basis data terdesentralisasi sejumlah komputer yang tersebar pada beberapa lokasi saling terhubung dan masing-masing komputer mampu melakukan pemrosesan serupa secara mandiri, dan dapat saling terinteraksi dalam pertukaran data. Contoh basis data terdesentralisasi adalah blockchain [8].

Cloud storage adalah sebuah sistem layanan penyimpanan data yang terintegrasi dan tersinkronisasi melalui internet dan dapat diakses dengan menggunakan berbagai platform (OSX, iOS, Windows, Windows Mobile, Android, Linux, dll) [9].

Cloud storage adalah salah satu teknologi yang dikembangkan dari cloud computing (komputasi awan) yaitu model komputasi dengan sumber daya seperti processor/computing power, storage network, dan software menjadi abstrak sebagai layanan di jaringan internet dengan pola akses jarak jauh [10].



(A) (B)

Gambar 1. Database; (A) Terpusat dan (B) Terdesentralisasi
(Sumber: Olnes, Ubacht, dan Janssen, 2017)

Ada banyak kelebihan yang dimiliki oleh Cloud storage jika dibandingkan dengan penyimpanan data secara tradisional diantaranya adalah kemudahan pengaksesan kapan saja dan di mana saja dengan jaringan internet [11] dan file sharing [9] tidak perlu membeli alat penyimpanan namun hanya cukup membayar penyimpanan sebanyak yang digunakan [12], memungkinkan pengguna untuk mengakses berbagai aplikasi lainnya secara langsung [13].

Namun demikian, cloud storage juga memiliki beberapa kekurangan, diantaranya yaitu kemungkinan diretas, keamanan data tidak dijamin sepenuhnya oleh penyedia layanan, mahal untuk penggunaan sehari-hari [13].

Ancaman keamanan data dalam komputasi awan juga disampaikan oleh [14] dalam penelitiannya. Sistem komputasi awan seharusnya dapat memberikan kepastian integritas, kerahasiaan, privasi, dan ketersediaan data. [12] merangkum beberapa kekurangan cloud storage, yaitu:

1. Immaturity. Vendor harus mencari ulang solusi penyelesaian ketidakcocokan dengan penyimpanan data secara online, dan itu telah menciptakan kesulitan bagi organisasi.
2. Harga dan Keandalan. Pengguna harus menghitung keefektifan biaya hosting dan pemeliharaan data oleh cloud.
3. Keamanan. Ada kemungkinan data dapat dicuri atau dilihat oleh orang yang tidak berwenang.
4. Batasan bandwidth. Jika bandwidth tidak secepat yang dibutuhkan pengguna, solusinya tidak akan cocok.
5. Network distance (Latency). Jumlah keterlambatan temporal dalam propagasi dan paket transmisi dalam jaringan akan mempengaruhi sousi penyimpanan cloud.

Selain itu, menurut [13] diperlukan kehati-hatian dalam memindahkan dokumen ke cloud storage, karena akan pindah permanen dari folder aslinya ke lokasi cloud storage. Lakukan copy – paste jika ingin dokumen tetap pada folder aslinya dan cloud storage. Cloud storage juga memiliki batas bandwidth spesifik, jika melebihi batas akan ada kenaikan biaya signifikan; tidak dapat mengakses data tanpa koneksi internet.

Dalam cloud storage, jika ingin memanipulasi file secara lokal melalui beberapa perangkat maka perlu mengunduh layanan di semua perangkat. Masalah utama pada cloud storage adalah masalah dengan keamanan dan privasi data yang disimpan dari jarak jauh [15].

Keamanan dalam Sistem Penyimpanan Data

[12] mengungkapkan cloud storage adalah layanan yang memiliki banyak kekurangan, akan tetapi hal ini tidak menjadi pertimbangan bagi pengguna karena alasan ekonomis dan fleksibilitas. Lebih lanjut, pengguna akan kehilangan kontrol dari sisi keamanan, dan muncul kekhawatiran data diakses oleh orang yang tidak berwenang.

Secara keseluruhan, keamanan data mencakup tiga aspek yaitu kerahasiaan, integritas, dan ketersediaan [13]:

1. Kerahasiaan: perlindungan data dan informasi dari pengungkapan kepada orang yang tidak berwenang.
2. Integritas: perlindungan data dan informasi dari agar tidak dimodifikasi oleh orang yang tidak berwenang.
3. Ketersediaan: akses data kapan pun diperlukan oleh orang yang berwenang.

Keamanan dalam sistem penyimpanan data merupakan salah satu aspek dalam Sistem Manajemen Keamanan Informasi (SMKI). Keamanan informasi meliputi keamanan dokumen, perangkat keras, perangkat lunak, infrastruktur dan bangunan yang melindunginya [16]. Dalam SMKI, istilah informasi merujuk pada informasi dalam bentuk dokumen dan data. [16] menyebutkan beberapa aspek dalam keamanan informasi meliputi:

1. Privasi. Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data. Privasi menjamin keamanan data bagi pemilik informasi dari orang lain.
2. Identifikasi. Langkah pertama yang harus dipenuhi untuk memperoleh hak akses ke informasi yang diamankan, misalnya dengan penggunaan username.
3. Otentifikasi. Sistem dapat membuktikan bahwa pengguna memang benar orang yang memiliki identitas yang di-klaim.

4. Otorisasi. Jaminan bahwa pengguna telah mendapatkan otorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dan informasi.
5. Akuntabilitas. Sistem dapat menyajikan data semua aktifitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktifitas tersebut.

Sedangkan menurut dokumen ISO/IEC 27002, 2005 yang terkait dengan dokumen ISO 27001, menyebutkan ada tujuh aspek informasi yaitu confidentiality, integrity, availability, authenticity, accountabilty, non-repudiation, dan reliability. Sedangkan untuk aspek keamanan informasi meliputi confidentiality, integrity, dan availibility (CIA).

1. Confidentiality. Jaminan informasi tertentu hanya dapat diakses oleh orang yang berhak mengaksesnya.
2. Integrity. Jaminan kelengkapan informasi dan menjaga dari korupsi, kerusakan, dan ancaman lainnya yang menyebabkan informasi berubah dari informasi aslinya.
3. Availability. Jaminan informasi dapat diakses oleh pengguna kapanpun, tanpa ada gangguan dan tidak dalam format yang tidak bisa digunakan.

Keamanan dalam sistem dan aplikasi juga menjadi salah satu dari empat pondasi pengembangan strategi nasional pembangunan cyber – security di Indonesia [17].

Blockchain

Blockchain, teknologi jaringan peer – to – peer [1] yang awalnya diperkenalkan oleh Satoshi Nakamoto pada tahun 2008 sebagai bagian dari bitcoin – sebuah sistem mata uang virtual.

Sebagai inovasi*, blockchain* hadir untuk menyimpan berbagai data serta informasi, termasuk transaksi keuangan [18]. *Blockchain* adalah basis data berupa catatan atau buku besar dari semua transaksi digital yang tersebar pada semua pengguna sistem [19].

Blockchain adalah aplikasi terdesentralisasi, tanpa otoritas terpusat, tanpa entitas pengontrol [20], dan kekal [21]. *Blockchain* terdiri dari sekelompok node, dimana setiap node memiliki replikasi data yang sama [21].

Karakteristik Blockchain

Blockchain mempunyai beberapa karakteristik, yaitu:

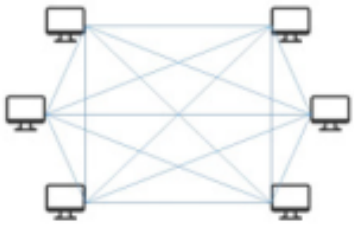
1. Desentralisasi. Sebagai basis data yang tersebar, setiap bagian dari *blockchain* memiliki akses untuk keseluruhan basis data dengan riwayat lengkap, dan setiap bagian dapat memverifikasi rekaman transaksi secara langsung tanpa penghubung [22], dan tanpa otentikasi oleh agen pusat [23] untuk menghindarisatu pihak mengambil kontrol penuh terhadap jaringan [24]. Dengan cara ini, *blockchain* dapat secara signifikan mengurangi biaya server (termasuk biaya pengembangan dan biaya operasi) dan mengurangi kemacetan kinerja di server pusat [23].
2. Transmisi peer – to – peer. Dengan *blockchain* sebuah data dapat dipindahkan tanpa pihak ketiga. Komunikasi terjadi secara langsung tanpa melalui pusat node. Setiap node menyimpan dan meneruskan informasi ke semua node lainnya [25].
3. Transparansi melalui enkripsi. Setiap transaksi dapat dilihat oleh semua pengguna, dan *blockchain* akan mengotetikasi data-data pengguna secara real time sebelum transaksi disahkan (Working Paper Bank Indonesia, 2017 dalam Adinigsih 2019). Setiap node dalam *blockchain* memiliki keunikan 30 lebih karakter alpanumerik yang teridentifikasi. Pengguna dapat memilih untuk tetap anonim atau memberikan bukti identitas kepada orang lain [22].

4. Perekaman data secara permanen. Transaksi dalam *blockchain* selalu diperbarui dan riwayatnya tidak dapat diubah atau dihapus karena terhubung dengan setiap rekaman transaksi [25]. Setiap entitas dapat meninjau informasi yang disimpan, namun perubahan ke basis data hanya dapat diimplementasikan dengan mencapai konsensus [26].
5. Aman. *Blockchain* adalah teknologi tanpa pengaruh atau keterlibatan orang tengah. Selain itu, diperlukan mekanisme konsensus untuk memvalidasi transaksi, dan transaksi otentik diletakan pada blok yang berisi cap waktu dan hash dari blok sebelumnya [24]. Jadi terjadi pemalsuan dapat terdeteksi dengan mudah [23]. Selain itu, beberapa sumber mengatakan karena data tersebar pada berbagai pihak, *blockchain* termasuk teknologi yang aman jika terjadi serangan siber, dibandingkan dengan teknologi lama yang hanya memakai satu pihak dalam penyimpanan data dan informasi [18].
6. Berbasis pemrograman digital. Transaksi *blockchain* terikat dengan logika komputasi dan terprogram [22].
7. Traceability. Kemampuan untuk menelusuri dan melacak transaksi sebelumnya secara iteratif [24].
8. Anonimitas. Setiap pengguna dapat berinteraksi dengan jaringan *blockchain*, untuk menghindari paparan identitas pengguna dapat menghasilkan banyak alamat. Informasi pribadi pengguna tidak disimpan oleh pihak pusat [23].
9. Kekal. Data dalam *blockchain* tidak dapat diubah atau dihapus. Kekekalan bekerja secara total berdasarkan konsensus [24].

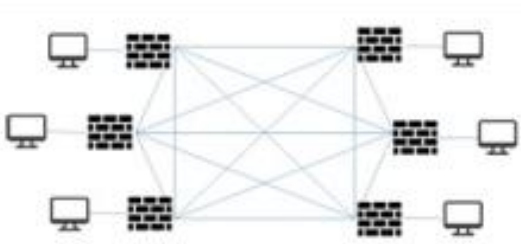
Jenis Blockchain

[24] membagi *blockchain* dalam tiga jenis, yaitu *public blockchain, private blockchain*, dan *consortium blockchain*.

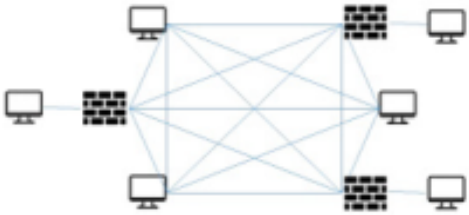
1. *Public blockchain* adalah blockchain yang mengizinkan semua node untuk mengakses data. Contohnya Bitcoin dan koin lite. Semua cryptocurrencies menjalankan blockchain umum [27].
2. *Private Blockchain*. Diperlukan pra-registrasi, undangan atau validasi oleh otoritas pusat, berarti hanya untuk yang memiliki izin. Secara umum digunakan dalam intraperusahaan atau solusi antar bisnis [27].
3. *Consortium Blockchain*. *Blockchain* tidak dikontrol oleh otoritas tunggal, melainkan oleh sekelompok otoritas yang disetujui. *Blockchain* konsorsium merupakan semi-desentralisasi.



(A)



(B)



(C)

Gambar 2. Jenis – Jenis *Blockchain*: (A) *Public blockchain*; (B) *Private Blockchain*; dan (C) *Consortium Blockchain*

Sumber: (Lin & Chun Liao, 2017)

Blockchain sebagai Basis Sistem Penyimpanan Data

[23] menekankan bahwa *Blockchain* dapat berfungsi sebagai manajemen data maupun analisis data. Sebagai manajemen data, *blockchain* dapat digunakan untuk menyimpan data penting karena sifatnya didistribusikan dan aman. Selain itu, *blockchain* juga bisa memastikan keaslian data. Misalnya untuk data informasi pasien, tidak dapat dirusak dan sulit dicuri.

Dalam hal analisis data, transaksi pada *blockchain* dapat digunakan untuk analisa. Misalnya dengan ekstraksi data pola perdagangan, pengguna dapat memprediksi perilaku mitra potensial mereka dengan analisis.

Berdasarkan hasil penelitiannya [28] menampilkan potensi-potensi manfaat *blockchain* yang dirangkum dari berbagai literatur dan ditampilkan pada tabel berikut:

Tabel 1. Manfaat *Blockchain*

Manfaat	Penjelasan
Strategi	
Transparansi	Riwayat transaksi tetap terlihat dan setiap node memiliki gambaran lengkap transaksi.
Menghindari penipuan dan manipulasi	Perubahan ilegal sulit dilakukan karena informasi disimpan dalam banyak legder yang didistribusikan.
Mengurangi korupsi	Penyimpanan dalam *blockchain* mencegah terjadinya korupsi, karena data sulit untuk dimanipulasi.
Organisasi	
Meningkatkan kepercayaan	Verifikasi data dengan banyak node dan pencatatannya yang tidak berubah meningkatkan kontrol data.
Transparan dan dapat diaudit	Mampu melacak riwayat transaksi dan membuat jejak audit.
Meningkatkan kemampuan prediksi	Ketersediaan riwayat informasi meningkatkan kemampuan prediksi.
Meningkatkan kontrol	Kebutuhan kesepakatan untuk menambah transaksi meningkatkan kontrol.
Kejelasan kepemilikan	Tata kelola perlu didefinisikan dengan jelas dan bagaimana informasi dapat diubah.
Ekonomi	
Mengurangi biaya	Biaya memvalidasi transaksi dapat dikurangi karena tidak melibatkan manusia.
Peningkatan ketahanan terhadap spam dan serangan DDOS	Tingkat ketahanan dan keamanan yang lebih tinggi mengurangi biaya pencegahan serangan.
Informasi	

Manfaat	Penjelasan
Integritas data dan peningkatan kualitas data	Informasi yang disimpan sesuai dengan apa yang diwakili pada kenyataannya karena kebutuhan konsensus dan sifatnya yang terdistribusi. Ini menghasilkan kualitas data yang lebih tinggi.
Mengurangi kesalahan manusia	Transaksi dan kontrol secara otomatis mengurangi kesalahan manusia
Akses ke informasi	Informasi disimpan di banyak tempat yang dapat meningkatkan kemudahan akses dan kecepatan akses.
Privasi	Pengguna bisa anonim dengan memberikan kunci enkripsi atau akses, untuk menghindari orang lain melihat informasi.
Reliabilitas	Data disimpan di banyak tempat. Mekanisme konsensus memastikan informasi hanya dapat diubah ketika semua pihak terkait setuju.
Teknologi	
Ketangguhan	Tangguh terhadap kejahatan
Keamanan	Karena data disimpan dalam banyak basis data menggunakan enkripsi, maka lebh sulit dimanipulasi. Kemungkinan peretasan pada saat yang sama sangat kecil.
Persistensi dan ireversibel	Setelah data ditulis ke *blockchain*, sulit untuk mengubah atau menghapusnya.
Mengurangi konsumsi energi	Konsumsi energi jaringan berkurang dengan peningkatan efisiensi dan mekanisme transaksi.

Sumber: Svein Ølnes, Jolien Ubacht, dan Marijn Janssen, (2017)

Potensi-potensi manfaat *blockchain* tersebut dapat menjadi solusi permasalahan sistem penyimpanan data yang telah disampaikan pada Bab I, diantaranya yaitu rendahnya tingkat keamanan sistem, risiko kehilangan data karena kerusakan, risiko kehilangan akses karena penutupan/kerusakan entitas, risiko perubahan data karena tidak adanya log aktivitas dan transaksi yang tidak transparan.

Penggunaan *blockchain* akan meningkatan desentralisasi, integritas data, dan transparansi – bersama dengan peningkatan efisiensi dan pengurangan biaya operasional. *Blockchain* memaksimalkan efisiensi kinerja institusi Sistem *blockchain* dan kontrak cerdas dapat dipakai untuk otomasi tugas dan alur kerja, yang dapat secara signifikan mengurangi waktu dan uang yang dihabiskan dalam proses birokrasi.

Selain pengurangan pengeluaran yang sangat praktis, hal ini juga akan membantu untuk memperkuat kepercayaan dan kepuasan dari masyarakat. Efisiensi yang lebih dan pengurangan biaya kemungkinan besar akan menaikkan tingkat penerimaan yang tinggi terhadap badan pemerintahan. Dengan pemotongan biaya operasional, pemerintah dapat berinvestasi di area lain seperti pendidikan, keamanan dan kesehatan masyarakat.

Blockchain untuk Keamanan Data

Blockchain adalah revolusi proses manajemen yang dapat menjadi solusi terkait interoperabilitas, kepercayaan, dan transparansi dalam jaringan atau sistem. Sesuai dengan fungsinya, *blockchain* adalah buku besar terdistribusi dari aset dan penyimpanan transaksi [29].

Berdasarkan hasil penelitian Sibarani, Pramukantoro, dan Bakhtiar, 2019 *blockchain* mampu mengetahui jika terjadi manipulasi data dan dapat mengembalikan keadaan awal data seperti semula, dan dapat menjaga integritas data yang telah disimpan.

Dokumen-dokumen dalam basis data *blockchain* kecil kemungkinannya untuk diretas atau dipalsukan karena sistem berjalan tanpa pihak ketiga dan adanya otomasi algoritma. Selain itu, dengan basis data yang terpecah dalam ratusan juta server, memastikan otomasi perjanjian, data terekam dalam sistem yang transparan sehingga kebenarannya dapat dicek.

Blockchain dapat menambah hasil efisiensi jaringan dan meningkatkan keamanan jaringan [25].

Pemanfatan Teknologi Blockchain

Teknologi *blockchain* telah menarik banyak pemangku kepentingan dan telah diterapkan di berbagai sektor seperti jasa keuangan dan pengiriman [27], kesehatan, utilitas, perumahan, pemerintahan [20], perbankan, dan pelayanan umum [25], IOT, dan pendidikan [24].

[29] dalam hasil penelitiannya mengungkapkan bahwa teknologi *blockchain* dapat digunakan dalam sistem pemungutan suara oleh pemerintah sebagaimana yang dilakukan oleh Pemerintah Denmark. Dengan anonimitas pemilih, catatan hasil pemungutan suara tidak akan berubah.

Selain itu, masih dalam penelitian [29], disampaikan *blockchain* juga diterapkan oleh pemerintah untuk keamanan makanan dengan menggunakan aplikasi yang menghubungkan petani dengan pasar untuk memastikan keamanan dan kualitas makanan.

Dalam hasil penelitiannya, [24] menekankan bahwa *blockchain* dengan karakteristiknya yang terdesentralisasi, transparansi, dan smart contract dapat memperbaiki masalah tata kelola pemerintah seperti privasi data, keamanan pangan, dan pemilihan.

Teknologi *Blockchain* telah diterapkan pada banyak organisasi pemerintah. Misalnya di Estonia, *blockchain* digunakan dalam Sistem Database Pemerintah, rekam medis, pencatatan sipil/kependudukan (akte kelahiran dan data pendidikan penduduk). Pemerintah Dubai mulai tahun 2020 mengklaim semua sistem pemerintah akan berbasis *blockchain.* Amerika Serikat menggunakan *blockchain* untuk sistem keuangan. Penggunaan lainnya dalam bidang agraria untuk registrasi tanah, perbankan, asuransi, IT, pangan, dan logistik.

Pemanfaatan teknologi *blockchain* di Indonesia berdasarkan literatur antara lain penelitian *blockchain* sebagai basis untuk e-voting, dengan kelebihan *blockchain* yang anonimitas, otonomi, rahasia, transparansi, terdistribusi dan teraudit diharapkan dapat lebih membuat pemilihan berlangsung lebih baik sesuai dengan prinsip langsung, umum, bebas, rahasia, jujur dan adil [30].

[31] dalam penelitiannya mengenai *Blockchain* sebagai basis e-commerce di Indonesia menekankan bahwa *blockchain* memiliki potensi untuk menyelesaikan tantangan penipuan, biaya komisi, kontak terbatas dan penyalahgunaan data pribadi dalam e-commerce dengan peningkatan keamanan dan transparansi melalui penerapan *cryptocurrency* dalam pembayaran dan kontrak pintar. Sebagai hasilnya ia mengusulkan teknologi *blockchain* sebagai arsitektur dan sistem platform e-commerce di Indonesia.

DAFTAR PUSTAKA

A, Rajalakshmi,et al, (2018) A Blockchain and IPFS Based Framework for Secure Research. International Journal of Pure and Applied Mathematics, Volume 119 No. 15 2018, 1437-1442.

Adiningsih, S. (2019). Transformasi Ekonomi Berbasis Digital di Indonesia. Jakarta: PT. Gramedia Pustaka Utama.

Afdhal. (2013). Studi Perbandingan Layanan Cloud Computing. Jurnal Rekayasa Elektrika, 193-201.

Albrecht, S., Reichert, S., & Neumann, D. (2018). Dynamics of Blockchain Implementation – A Case Study from the Energy Sector . the 51st Hawaii International Conference on System Sciences , (hal. 3527-3536). Hawaii.

Albrecht, S., Reichert, S., & Neumann, D. (2018). Dynamics of Blockchain Implementation – A Case Study from the Energy Sector . the 51st Hawaii International Conference on System Sciences , (hal. 3527-3536). Hawaii.

Alketbi, A., Nasir, Q., & Talib , M. A. (2017). Blockchain for Government Services – Use Cases, Security Benefits and Challenges . IEEEE, 112-119.

Ardiyanti, H. (2014). Cyber - Security dan Tantangan Pengembangan di Indonesia. Politica, 96-110.

Asia Cloud Computing Association. (2018). Cloud Readiness Index 2018. ACCA.

Diordiiev, V. (2018). Blockchain Technology and Its Impact on Financial and Shipping Services. Economic Ecology Socium.

Iansiti, M., & Lakhani, K. R. (2017, Januari - February). The Thruth About Blockchain. Harvard Business Report.

Ibrahim, M., & Kusnawi. (2013). Analisis dan Implementasi Owncloud Sebagai Media Penyimpanan pada Yayasan Salman Al-Farisi Yogyakarta. DASI, 32-37.

Ismanto, Leonando;et al. (2018). Blockchain as E-Commerce Platform in Indonesia. *Journal of Physics: Conference Series*.

Lacob, N. M., & Moise, L. M. (2015). Centralized vs. Distributed Databases. Case Study. Journal of Economic Studies, 119–130.

M. Hussein, D. E.-D., Taha, M. H., & Khalifa, N. E. (2018). A Blockchain Technology Evolution between Business Process Management (BPM) and Internet-of-Things (IoT). (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.9, No.8, 442-450.

Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. Informa Politeknik Indonusa Surakarta, Vol 5 No.1:28-34.

Obrutsky, S. (2016). Cloud Storage: Advantages, Disadvantages and Enterprise Solutions for Business. ResearchGate.

Olnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger. *Government Information Quarterly 34*, 355-364

Perdani, M. K., & Santosa, P. I. (2018). Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ). Seminar Nasional Teknologi Informasi dan Multimedia 2018 (hal. 1.14.7-12). Yogyakarta: Universitas Amikom Yogyakarta.

Prabu, H. K. (2019). Analisis Manajemen Proyek untuk Implementasi Penyimpanan Arsip Rahasia Negara Menggunakan Blockchain.

Razzaq, A., Khan, M., Talib, R., Butt, A. D., Hanif, N., Afzal, S., & Raouf, M. R. (2019). Use of Blockchain in Governance: A Systematic Literature Review. International Journal of Advanced Computer Science and Application, Vol. 10 No. 5. 685 - 691.

Santiko, I., Rosido, R., & Wibawa, S. A. (2017). Pemanfaatan Private Cloud Storage Sebagai Media Penyimpanan Data E-Learning pada Lembaga Pendidikan. Jurnal Teknik Informatika Vol. 10 No. 2, 137-146.

Sarno, R., & Iffano, I. (2009). Sistem Manajemen Keamanan Informasi. Surabaya: ITSPress.

Selvananthan, N., & Poravi, G. (2018). Comparative Study on Decentralized Cloud Collaboration (DCC). International Conference for Convergence in Technology.

Shetty, S. S., Kamhoua, C. A., & Njilla, L. L. (2019). *Blockchain for Distributed Systems Security.* New Jersey: IEEE Press.

Sibarani, I., Pramukantoro, E. S., & Bakhtiar, F. A. (2019). Implementasi Blockchain berbasis Bigchain DB dan Tendermint pada Sistem Penyimpanan Data IoT. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 7603-7611.

Singh, I., & Won Lee, S. (2018). Comparative REquirement Analysis for the Feasibility of Blockchain for Secure Cloud. CCIS, 57-72.

Vurukonda, N., & Rao, B. (2016). A Study on Data Storage Security Issues in Cloud Computing. 2nd International Conference on Intelligent Computing, Communication & Convergence, 128 – 135.

Vyas, J., & Modi, P. (2017). Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-data Approach. International Journal of Advance Research in Engineering, Science & Technology, 38-50.

Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security Sixth Edition. Boston: Cangage Learning.

Winarno, A., Harsari, J., & Ardianto, B. (2018). Block-Chain Based E-Voting For Indonesia. *Journal of Engineering and Science Research*, 2 (5): 13-17.

Zheng, Z., & Xie, S. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 352-375.