KEAMANAN INFORMASI MENGGUNAKAN TEKNOLOGI BLOCKCHAIN: SEBUAH TINJAUAN LITERATUR

Research Proposal · April 2023

CITATIONS
0

READS
23

4 authors, including:

Aldi Rezeki Ramdani
Universitas Komputer Indonesia
3 PUBLICATIONS **0** CITATIONS

SEE PROFILE

KEAMANAN INFORMASI MENGGUNAKAN TEKNOLOGI BLOCKCHAIN: SEBUAH TINJAUAN LITERATUR

Disusun Oleh :

10119273 – Aldi Rezeki Ramdani

KSI-2

SEMESTER GENAP

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN ILMU KOMPUTER

UNIVERSITAS KOMPUTER INDONESIA

2023

1. Latar Belakang

Dalam era digital saat ini, keamanan informasi menjadi hal yang sangat penting bagi organisasi atau perusahaan. Informasi yang penting seperti data karyawan, informasi pelanggan, dan data keuangan harus dilindungi dengan cara yang efektif agar tidak jatuh ke tangan yang salah. Sayangnya, banyak organisasi dan perusahaan masih menghadapi tantangan dalam melindungi informasi mereka karena serangan siber yang semakin canggih dan kompleks.

Salah satu teknologi terbaru yang dapat membantu melindungi keamanan informasi adalah teknologi blockchain. Blockchain merupakan urutan blok-blok di mana setiap blok terhubung dengan blok sebelumnya. Setiap blok harus memiliki kunci yang aman secara kriptografi, hash blok sebelumnya, serta informasinya [1]. Teknologi blockchain menggunakan penyimpanan terdistribusi terdesentralisasi[2], yang memungkinkan dengan ketidakdapatan diubah, ketidakpercayaan, dan anonimitas, dan dapat mewujudkan berbagi data, koordinasi, dan kerja sama kredit terdesentralisasi di jaringan. Keamanan dan privasi teknologi blockchain dapat melindungi informasi privasi secara efektif dan mencegah pencurian informasi [3][4].

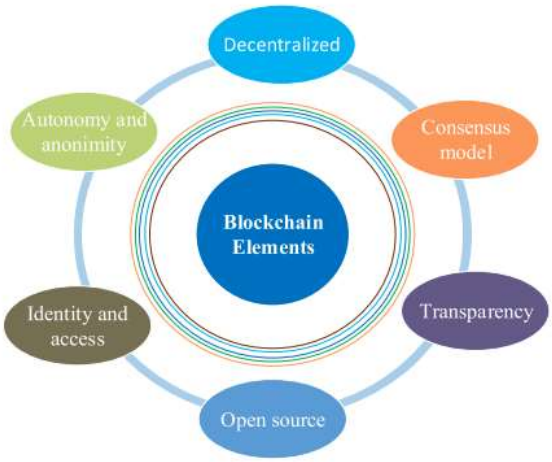
Teknologi blockchain sedang mengubah cara pemodelan data, dan pemerintah telah mengimplementasikannya dalam banyak aplikasi seperti aplikasi Internet of Things (IoT). Teknologi ini sangat menarik untuk aplikasi semacam itu karena kemampuannya yang belum pernah ada sebelumnya dalam beradaptasi serta melindungi dan membagikan data dan layanan IoT. Saat ini, teknologi blockchain berada di pusat banyak perkembangan di industri IoT [5]. Salah satu alasan untuk hal ini adalah karena banyak layanan IoT rentan terhadap serangan dan tantangan. Dengan menggunakan teknologi blockchain, banyak masalah dengan sistem siber-fisik di sektor IoT dapat diatasi. Karena industri IoT sedang beralih ke model sensor jaringan, kota pintar yang berkelanjutan, dan banyak komponen yang terlibat, perlu dipertimbangkan manfaat tertentu dalam mengaturnya [6] Blockchain berkembang di banyak sektor Bisni seperti di bidang Akademik, Kesehatan, pemerintah, manufaktur, Logistik dan masih banyak lagi.

Dalam rangka itu, tulisan ini bertujuan untuk melakukan tinjauan literatur tentang penggunaan teknologi blockchain dalam menjaga keamanan informasi, serta menganalisis keuntungan dan tantangan penerapannya. Diharapkan hasil dari tulisan ini dapat memberikan pemahaman yang lebih baik tentang teknologi blockchain sebagai solusi untuk menjaga keamanan informasi.

2. Pembahasan

Satoshi Nakamoto menggambarkan blockchain sebagai teknologi dasar dalam Bitcoin, yang merupakan blockchain pertama dan terbesar di dunia. Meskipun blockchain dimulai dengan Bitcoin, teknologi ini telah mendapat banyak perhatian di luar ranah mata uang kripto juga [7].

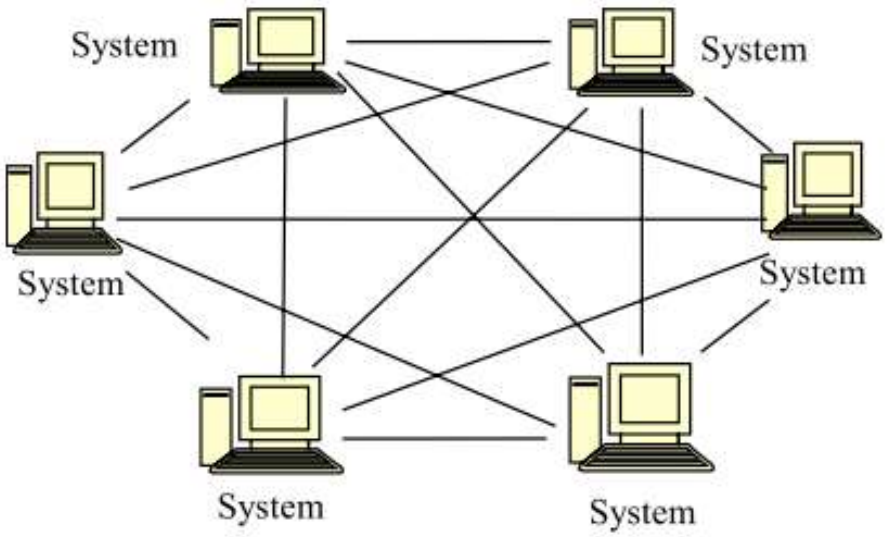
Bitcoin adalah mata uang kripto yang memungkinkan penggunanya tetap sangat anonim melalui penggunaan kriptografi kunci publik dan hashing kriptografis. Dengan menggunakan kriptografi kunci publik, pengguna menyimpan bitcoin mereka dalam dompet digital. Dompet ini berisi kunci pribadi akun yang digunakan untuk menandatangani semua transaksi dari akun tersebut. Setiap transaksi yang disajikan oleh akun tersebut akan diverifikasi oleh jaringan menggunakan kunci publik yang sesuai untuk akun tersebut. Meskipun umum, anonimitas bukanlah persyaratan dari platform blockchain. Banyak platform, terutama yang ditujukan untuk penggunaan bisnis dan perusahaan, menggantikan anonimitas dengan identitas untuk memungkinkan arsitek solusi dan administrator mendefinisikan dan menegakkan izin dan akses berbasis peran. Dalam banyak skenario bisnis, anonimitas dan transparansi penuh yang menentukan platform publik sama sekali tidak diinginkan, tetapi jenis buku besar yang hanya dapat ditambahkan tetap diperlukan[8].



Gambar 1 Blockchain element

Teknologi blockchain merupakan manifestasi dari teknologi distributed ledger (DLT) yang lebih umum, yang memuat infrastruktur dan proses untuk jaringan menghasilkan catatan konsensus perubahan keadaan atau pembaruan pada ledger yang disinkronkan dan didistribusikan di berbagai simpul di jaringan. Bentuk DLT populer lainnya adalah directed acyclic graph (DAG), sering dianggap sebagai teknologi rival dan pendorong untuk blockchain. Berbeda dengan blockchain yang mengorganisir catatan dalam urutan kronologis yang tidak dapat diubah, DAG mewakili jaringan catatan individual yang terhubung ke banyak transaksi lainnya. Dalam istilah teknis, blockchain adalah daftar terkait, sedangkan DAG adalah pohon yang bercabang dari satu catatan ke catatan lainnya, dan seterusnya. Meskipun diskusi berikut sering sama berlakunya untuk DLT lainnya, kami mendorong pembaca untuk fokus pada blockchain untuk kejelasan. Dalam arti ini, "blockchain" dapat dipandang sebagai referensi umum untuk sistem konsensus terdesentralisasi [9][10][11].

Gambar 2 menunjukkan diagram blok dari jaringan P2P. Di sini, catatan disimpan pada banyak sistem yang saling terkait, yang menyimpan informasi yang sama. Jika pembaruan komputer tidak terotentikasi, jaringan akan menolaknya. Pada Blockchain, banyak transaksi pertukaran nilai dikelompokkan menjadi beberapa blok.



Gambar 2 Peer-To-Peer Network

Teknologi blockchain terdiri dari serangkaian blok yang terhubung satu sama lain, dimana setiap blok terhubung dengan blok sebelumnya. Dengan menggunakan mekanisme jaminan dan kepercayaan kriptografi, setiap blok merekam informasi yang tidak dapat diubah melalui jaringan peer-to-peer (P2P). Hal ini menjaga keadaan yang disepakati secara rasional oleh semua peserta atau individu tanpa adanya otoritas pusat atau terpercaya. Teknologi blockchain berbeda dari teknologi basis data. Dalam Blockchain, entri baru ditambahkan di akhir buku besar, dan tidak ada yang diizinkan untuk mengedit atau menghapus data. Di sisi lain, data dapat dimodifikasi atau dihapus oleh administrator pusat dalam basis data relasional. Selain itu, basis data relasional dirancang untuk aplikasi terpusat [12].

Dalam teknologi blockchain, terdapat beberapa jenis node yang digunakan tergantung pada tingkat partisipasi dan jenis jaringan blockchain. Setiap jaringan memiliki peran masing-masing. Berikut ini adalah penjelasan mengenai jenis-jenis node blockchain [13].

Publik vs. Privat

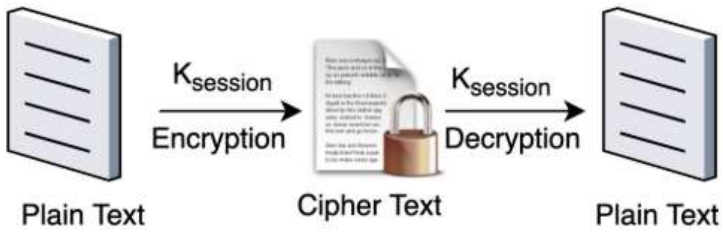
Blockchain publik memperbolehkan audiens besar atau masyarakat umum untuk menambahkan data ke buku besar. Bitcoin adalah contoh dari jaringan blockchain publik - tidak ada aturan atau izin tentang siapa yang dapat memperdagangkan Bitcoin. Siapa pun dapat membeli, menjual, atau mengirimkan Bitcoin kepada siapa pun. Sebagai contoh, sebuah solusi blockchain yang digunakan untuk melacak bagaimana donasi amal digunakan oleh sebuah organisasi nirlaba adalah contoh dari solusi yang bersifat privat. Dalam solusi seperti itu, hanya pejabat yang ditunjuk dari organisasi nirlaba yang harus diizinkan untuk berbagi metrik yang menjelaskan bagaimana donasi dialokasikan dan dihabiskan [7].

Permissioned vs. Permissionless

Platform permissionless adalah solusi yang terbuka, dan di mana masyarakat umum memiliki sedikit kebutuhan izin atau akses berbasis peran. Platform-platform ini tidak memiliki kemampuan alami untuk melacak dan mengelola identitas dan kemudian menentukan dan menegakkan izin berdasarkan identitas tersebut. Ini tidak berarti bahwa Anda tidak dapat membangun solusi berizin pada platform permissionless, ini hanya berarti jika Anda memilih untuk melakukannya, Anda bertanggung jawab untuk merancang dan menerapkan metode untuk melacak dan mengelola identitas serta menetapkan izin berdasarkan identitas tersebut. Ketika mengembangkan solusi, cara terbaik untuk menentukan jenis blockchain yang diperlukan adalah dengan menentukan apakah semua peserta dianggap sama atau seharusnya beberapa memiliki kemampuan atau izin yang tidak dimiliki oleh yang lain. Menjawab pertanyaan ini akan membantu memandu keputusan untuk menggunakan teknologi blockchain yang bersifat berizin atau berizin terbuka. Contoh dari blockchain berizin adalah solusi blockchain enterprise di mana hanya karyawan yang diotorisasi yang memiliki akses. Mata uang digital, yang dapat ditukar dan diperdagangkan oleh semua orang, adalah contoh dari blockchain berizin terbuka [7].

Blockchain dan Kriptografi

Penggabungan teknologi blockchain dengan kriptografi Advanced Encryption Standard (AES) dapat meningkatkan keamanan dan privasi data yang disimpan dalam blockchain. AES merupakan algoritma kriptografi simetris yang dapat mengenkripsi dan mendekripsi data dalam jumlah besar dengan cepat dan efisien. Dengan mengenkripsi data yang disimpan di dalam blok blockchain dengan AES, data yang sensitif dan pribadi dapat terlindungi dengan baik. Dalam hal ini, hanya pihak yang memiliki kunci dekripsi yang dapat membuka dan membaca data tersebut, sehingga privasi dan integritas data lebih terjamin. Kombinasi blockchain dan AES juga memungkinkan transaksi digital dapat dilakukan secara aman dan terenkripsi, sehingga keamanan pengguna dalam melakukan transaksi digital dapat lebih terjaga. Dengan demikian, penggabungan antara teknologi blockchain dan kriptografi AES dapat meningkatkan tingkat keamanan dan privasi dalam penggunaan teknologi blockchain [3][14].



Gambar 3 Symmetric key encryption.

Keamanan dari Smart contract

Smart contract merujuk pada skrip yang dieksekusi secara otomatis pada jaringan terdistribusi yang terdiri dari node-node yang saling tidak percaya tanpa adanya pihak ketiga yang dapat dipercaya secara eksternal. Untuk menyelesaikan transaksi data antara peserta, smart contract memperlihatkan data transaksi tersebut pada risiko kompromi informasi sensitif. Jika tidak, maka kesulitan pengawasan akan timbul. Karena smart contract mentransfer nilai, maka eksekusi yang benar dan implementasi yang aman terhadap serangan/penyusupan sangat penting. Para penjahat dapat memanfaatkan Smart Contract Kejahatan (CSC), senjata cyber baru

yang kritis, untuk menghasilkan transaksi data kerentanan 0-hari. Smart contract adalah salah satu sumber masalah keamanan yang signifikan pada level proses blockchain. Selain itu, smart contract (misalnya, dompet blockchain, dana crowdfunding) sulit direvisi setelah diterbitkan. Kesalahan yang tercatat atau transaksi data jahat tidak dapat dihapus dari aplikasi blockchain. Cara untuk mengembalikan transaksi data yang tercatat adalah dengan membuat hard fork pada blockchain, dan ini memerlukan konsensus baru di antara anggota yang berpartisipasi dan dengan demikian merusak kepercayaan sistem. Oleh karena itu, keamanan smart contract sering menentukan keamanan blockchain. Banyak smart contract rentan terhadap serangan [15].

Data security pada Blockchain

Gambar 4 Aspek utama Keamanan Data pada blockchain

Keamanan data pada blockchain menjadi salah satu aspek yang sangat penting dalam teknologi blockchain. Keamanan data pada blockchain dapat digambarkan menjadi integritas, kerahasiaan, dan ketersediaan. Integritas data pada blockchain mengacu pada konsistensi dan keaslian data yang disimpan di dalamnya. Setiap transaksi yang terjadi di blockchain harus diotentikasi dan diverifikasi oleh seluruh jaringan, sehingga memastikan bahwa setiap data yang masuk atau keluar dari sistem adalah benar dan tidak dirubah oleh pihak yang tidak berwenang [16].

Kerahasiaan data pada blockchain berfokus pada perlindungan informasi yang bersifat pribadi atau rahasia dari akses yang tidak sah. Blockchain menggunakan

teknologi kriptografi yang kuat, seperti enkripsi dan tanda tangan digital, untuk memastikan bahwa hanya pemilik data yang dapat mengakses dan membukanya.

Ketersediaan data pada blockchain merujuk pada ketersediaan data dan jaringan itu sendiri. Sebuah blockchain yang aman harus dapat berjalan secara terus-menerus tanpa terputus, memastikan bahwa data dapat diakses dan digunakan oleh pengguna dengan cepat dan mudah. Untuk memastikan ketersediaan data, blockchain harus memiliki jaringan yang terdistribusi dan redundant, sehingga tidak mudah terpengaruh oleh serangan atau bencana.

Dalam aspek kriptografi, skema tanda tangan, teknik enkripsi (termasuk komputasi dan pengambilan data), perlindungan privasi, dan algoritma konsensus, menjadi beberapa hal yang harus diperhatikan dalam menjaga keamanan data pada blockchain.

Sebagai contoh, penggunaan skema tanda tangan yang salah dapat membuat transaksi blockchain menjadi tidak valid, sehingga harus dilakukan verifikasi yang teliti dalam memilih skema tanda tangan yang tepat. Sedangkan dalam algoritma konsensus, terdapat risiko serangan yang dapat mengancam keamanan data pada blockchain, seperti serangan 51% yang dapat merusak keamanan jaringan blockchain. Oleh karena itu, perlu dilakukan penelitian dan pengembangan yang terus menerus untuk menjaga keamanan data pada blockchain.[17].

Kesimpulan dan Saran

Dalam kesimpulannya, blockchain adalah teknologi yang dapat menghasilkan transaksi aman dan terpercaya dengan menggunakan beberapa metode keamanan, termasuk kriptografi dan kontrak cerdas. Namun, ada beberapa tantangan dalam hal keamanan data yang harus diatasi, seperti masalah privasi, kesalahan atau transaksi jahat, dan kelemahan dalam kontrak cerdas. Oleh karena itu, penting bagi para pengembang dan pengguna blockchain untuk memperhatikan dan mengimplementasikan praktik keamanan yang baik, seperti penggunaan algoritma enkripsi yang aman, manajemen identitas yang kuat, dan pemantauan secara teratur untuk memperbaiki kerentanan. Selain itu, para pengguna blockchain harus tetap waspada terhadap serangan keamanan seperti CSC dan penggunaan alat keamanan yang tepat seperti firewall dan sistem deteksi intrusi.

Saran yang dapat diberikan adalah agar para pengembang dan pengguna blockchain terus meningkatkan pemahaman mereka tentang teknologi blockchain dan up-to-date dengan praktik keamanan terbaru. Mereka juga harus terus melakukan penelitian dan pengembangan dalam hal keamanan data blockchain, serta berkolaborasi dengan para ahli keamanan terkait. Selain itu, para regulator harus mempertimbangkan cara untuk memastikan bahwa praktik keamanan blockchain diikuti oleh para pengguna dan pengembang, dan untuk menentukan tanggung jawab dan hukuman untuk pelanggaran keamanan data yang terjadi di blockchain. Dengan demikian, blockchain dapat terus berkembang menjadi teknologi yang dapat diandalkan dan aman untuk digunakan dalam berbagai industri.

DAFTAR PUSTAKA

[1] T. Alam and M. Benaida, "Blockchain and internet of things in higher education," *Univers. J. Educ. Res.*, vol. 8, no. 5, pp. 2164–2174, 2020, doi: 10.13189/ujer.2020.080556.

[2] T. Kanan, A. T. Obaidat, and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," *2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc.*, pp. 629–633, 2019, doi: 10.1109/JEEIT.2019.8717505.

[3] H. Wu, A. D. Dwivedi, and G. Srivastava, "Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 17, no. 2s, 2021, doi: 10.1145/3408321.

[4] I. Afrianto, T. Djatna, Y. Arkeman, I. Sukaesih Sitanggang, and I. Hermadi, "Disrupting Agro-industry Supply Chain in Indonesia with Blockchain Technology: Current and Future Challenges," *2020 8th Int. Conf. Cyber IT Serv. Manag. CITSM 2020*, 2020, doi: 10.1109/CITSM50537.2020.9268872.

[5] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, "BDSS-FA: A Blockchain-Based Data Security Sharing Platform with Fine-Grained Access Control," *IEEE Access*, vol. 8, pp. 87552–87561, 2020, doi: 10.1109/ACCESS.2020.2992649.

[6] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[7] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: Vision and future opportunities," *Comput. Commun.*, vol. 154, pp. 223–235, 2020, doi: 10.1016/j.comcom.2020.02.058.

[8] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, 2020, doi: 10.1109/JIOT.2020.3004273.

[9] L. Chen, L. W. Cong, and Y. Xiao, *A brief introduction to blockchain economics*, no. iv. 2020. doi: 10.1142/9789811220470_0001.

[10] S. Tabrez Siddiqui, M. Shuaib, A. Kumar Gupta, and S. Alam, "Implementing Blockchain Technology: Way to Avoid Evasive Threats to Information Security on Cloud," *2020 Int. Conf. Comput. Inf. Technol. ICCIT 2020*, pp. 87–91, 2020, doi: 10.1109/ICCIT-144147971.2020.9213798.

[11] I. Afrianto, T. Djatna, Y. Arkeman, I. Hermadi, and I. S. Sitanggang,

"Block chain technology architecture for supply chain traceability of fisheries products in Indonesia: Future challenge," *J. Eng. Sci. Technol.*, vol. 15, pp. 41–49, 2020.

[12] S. Namasudra, G. C. Deka, P. Johri, M. Hosseinpour, and A. H. Gandomi, "The Revolution of Blockchain: State-of-the-Art and Research Challenges," *Arch. Comput. Methods Eng.*, vol. 28, no. 3, pp. 1497–1515, 2021, doi: 10.1007/s11831-020-09426-0.

[13] D. Firdayati, I. Ranggadara, I. Afrianto, and N. R. Kurnianda, "Designing Architecture Blockchain of Hyperledger Fabric for Purchasing Strategy," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 2, pp. 464–468, 2021, doi: 10.30534/ijatcse/2021/041022021.

[14] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[15] Q. Lu *et al.*, "Integrated model-driven engineering of blockchain applications for business processes and asset management," *Softw. - Pract. Exp.*, vol. 51, no. 5, pp. 1059–1079, 2021, doi: 10.1002/spe.2931.

[16] M. Warkentin and C. Orgeron, "Using the security triad to assess blockchain technology in public sector applications," *Int. J. Inf. Manage.*, vol. 52, no. January 2019, p. 102090, 2020, doi: 10.1016/j.ijinfomgt.2020.102090.

[17] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, 2022, doi: 10.1109/TSC.2020.3038641.