

# Meningkatkan Keamanan Data Rekam Medis Puskesmas Gajahan Melalui Teknologi Blockchain dengan Implementasi Penggunaan Metode Smart Contract dan Algoritma Konsensus Proof-of-Work

Eriska Setyaningtyas Rahmasari<sup>1</sup>, Agung Frisky Ardianto<sup>2\*</sup>

<sup>1</sup>Teknik Informatika/Illmu Komputer  
Universitas Duta Bangsa Surakarta

<sup>1</sup>eriskarahmasari@gmail.com

<sup>2</sup>Teknik Informatika/Illmu Komputer  
Universitas Duta Bangsa Surakarta

<sup>2</sup>agungfrisky3@gmail.com

**Abstrak**— Meningkatnya akan minat digitalisasi akan data rekam medis terutama sejak adanya pandemi COVID-19 menambah minat penggunaan system rekam medis oleh penyedia layanan kesehatan. Akan tetapi, system ini masih memiliki resiko terkait dengan pelanggaran privasi, penghapusan data dan juga terbatasnya performa. Oleh karena itu beberapa penelitian menunjukkan bahwa teknologi blockchain mampu mengatasi permasalahan ini. Penelitian ini bertujuan untuk mengeksplorasi pemanfaatan teknologi blockchain dalam konteks tersebut, memberikan wawasan baru, dan rekomendasi praktis bagi pengelola. Penelitian ini berhasil menunjukkan bahwa penerapan teknologi blockchain, khususnya dengan metode Smart contract dan algoritma konsensus Proof-of-Work (PoW), dapat secara signifikan meningkatkan keamanan dan efisiensi pengelolaan data rekam medis di Puskesmas Gajahan. Dengan teknologi blockchain, setiap transaksi dan perubahan data direkam secara permanen dan transparan, sehingga memastikan integritas dan kepercayaan terhadap data medis. Penerapan ini juga memberikan keamanan tambahan terhadap ancaman serangan seperti SQL injection dengan memastikan tidak ada koneksi langsung antara aplikasi web dan database. Secara keseluruhan, teknologi blockchain menunjukkan potensi besar dalam meningkatkan perlindungan dan manajemen data sensitif di sektor kesehatan, khususnya di institusi seperti Puskesmas Gajahan.

**Kata kunci**— Keamanan Informasi, Blockchain, Smart contract, Proof of Work, Rekam Medis.

**Abstract**— Information security is the process of protecting data from different types of attacks to reduce risk, optimize return on investment, and secure commercial possibilities. *Blockchain* offers high security through encryption and consensus mechanisms that are difficult to hack. In this system, *Smart contracts* automatically execute digital contracts when certain conditions are met, reducing human error and improving the efficiency of medical record data management. This study uses primary data from the medical records of BPJS patients at Puskesmas Gajahan and secondary data from previous studies and the implementation of *blockchain* technology in other health centers. The results show that the implementation of *blockchain* technology with PoW can increase trust between patients, nurses, and doctors in the security and integrity of the medical data they access and manage. The main conclusion of this study is that *blockchain* technology can be an innovative solution to improve the security and efficiency of medical record data management at Puskesmas Gajahan.

**Keywords**— Information Security, Blockchain, Smart contracts, Proof of Work, EHR.

## I. PENDAHULUAN

Lan et al.(2021), Li et al.(2021), dan Lan et al.(2021) menyatakan bahwa keamanan informasi adalah proses melindungi data dari berbagai jenis serangan untuk mengurangi risiko, mengoptimalkan laba atas investasi, dan mengamankan kemungkinan komersial. Dalam industri perawatan kesehatan, keamanan informasi mengacu pada perlindungan data rekam medis pasien dari berbagai risiko seperti akses ilegal, pemalsuan, pelanggaran privasi, dan serangan seperti SQL injection yang dapat menyebabkan kelemahan sistem. Hal ini sangat penting karena informasi sensitif yang termasuk dalam data rekam medis harus dijaga kerahasiaannya untuk menjunjung tinggi hak privasi pasien.

Dalam beberapa tahun terakhir, teknologi Blockchain telah muncul sebagai sarana yang layak untuk meningkatkan keamanan informasi di berbagai industri, termasuk bidang medis. Blockchain adalah teknologi pencatatan terdesentralisasi yang menawarkan keamanan tinggi melalui mekanisme enkripsi dan konsensus yang sulit untuk diretas. Karena tidak ada transaksi yang tersimpan dalam blockchain yang dapat dihapus atau diubah, maka jejak audit yang akurat dan transparan dapat dihasilkan ((Bellavista et al.,2021; Belchior et al.,2022; Cheng et al.,2024, dan Cohen et al.,2020)

Li dan Kassem (2021) dan Garriga et al. (2021)) menyatakan bahwa salah satu fitur unggulan dari blockchain adalah Smart contract, yaitu kontrak digital yang dijalankan secara otomatis ketika kondisi tertentu terpenuhi. Smart contract dapat

membantu mengurangi kesalahan manusia dan meningkatkan efisiensi dalam pengelolaan data rekam medis, karena transaksi dan proses dapat dilakukan tanpa memerlukan pihak ketiga sebagai perantara.

Puskesmas Gajahan, sebagai salah satu institusi kesehatan di Indonesia, menghadapi tantangan dalam menjaga keamanan data rekam medis pasiennya. Penerapan teknologi blockchain dengan metode Smart contract dapat menjadi solusi inovatif untuk meningkatkan keamanan dan efisiensi pengelolaan data rekam medis di Puskesmas Gajahan. Penelitian ini bertujuan untuk mengeksplorasi pemanfaatan teknologi blockchain dalam konteks tersebut, memberikan wawasan baru, dan rekomendasi praktis bagi pengelola Puskesmas ((Honari et al.,2023; Koç dan Gürkün,2020; Kumari et al.,2020; Lu et al., 2021; Nie dan Liu, 2021; Purwono et al.,2023; Tith, et al.,2020, dan Cohan et al.,2020)).

Penelitian yang dilakukan ini memiliki tujuan untuk melakukan eksplorasi potensi penggunaan teknologi Blockchain untuk tujuan keamanan dan menilai efisiensi pengelolaan data rekam medis, khususnya dengan menggunakan metode Smart contract dan algoritma konsensus Proof-of-Work (PoW) untuk keamanan data rekam medis pada Puskesmas Gajahan.

## II. METODOLOGI PENELITIAN

Bagian ini menjelaskan secara rinci tentang tahapan penelitian yang dilakukan.

### A. Jenis Data

Jenis data yang digunakan dalam penelitian ini adalah:

#### 1) Data Primer

Data primer yang digunakan dalam penelitian ini adalah data rekam medis pasien BPJS di Puskesmas Gajahan. Data ini berisi informasi kesehatan yang komprehensif dan spesifik tentang diagnosis pasien, pengobatan, dan obat yang diresepkan.

#### 2) Data Sekunder

Data sekunder yang digunakan dalam penelitian ini berasal dari penelitian sebelumnya mengenai penggunaan Smart contract dan teknologi blockchain dalam

sistem keamanan data rekam medis; data mengenai implementasi teknologi ini di pusat kesehatan lainnya; dan rincian mengenai keamanan data rekam medis dan perlindungan data pribadi di dalam sistem kesehatan.

### B. Metode Pengumpulan Data

#### 1) Studi Literatur

Melibatkan pengumpulan dan analisis informasi dari sumber-sumber teks yang relevan, seperti buku, jurnal, artikel, dan dokumen resmi lainnya, untuk memahami konsep, teori, dan aplikasi blockchain serta Smart contract dalam keamanan data rekam medis.

#### 2) Studi Kasus

Melibatkan analisis implementasi blockchain dan Smart contract dalam konteks yang relevan dengan penelitian Anda, mungkin dari puskesmas lain atau sistem keamanan data lainnya, untuk memahami potensi dan tantangan implementasi di Puskesmas Gajahan.

### C. Analisis Permasalahan

Digitalisasi akan data rekam medis terutama sejak adanya pandemi COVID-19 menambah minat penggunaan system rekam medis oleh penyedia layanan kesehatan. Akan tetapi, system ini masih memiliki resiko terkait dengan pelanggaran privasi, penghapusan data dan juga terbatasnya performa. Oleh karena itu beberapa penelitian menunjukkan bahwa teknologi blockchain mampu mengatasi permasalahan ini. Sehingga, peneliti ingin mengeksplorasi penggunaan teknologi blockchain dengan menggunakan metode smart Contract dan Algoritma Konsensus Proof-of-Work untuk mengamankan data rekam medis khususnya data rekam medis di Puskesmas Gajahan.

Beberapa penelitian menunjukkan bahwa teknologi blockchain memiliki potensi untuk mengatasi permasalahan tersebut. Blockchain, dengan metode smart contract dan algoritma konsensus Proof-of-Work, dapat menyediakan solusi yang lebih aman dan andal untuk pengelolaan data rekam medis. Peneliti tertarik untuk mengeksplorasi penggunaan teknologi ini dalam konteks Puskesmas Gajahan, dengan

harapan dapat meningkatkan keamanan dan keandalan data rekam medis di fasilitas tersebut.

#### D. Analisis Serangan

SQL Injection adalah jenis serangan siber di mana penyerang menyuntikkan perintah SQL berbahaya ke dalam basis data melalui aplikasi web yang memiliki validasi input yang lemah. Serangan ini dapat mengakibatkan akses tidak sah, modifikasi, atau penghapusan data sensitif seperti rekam medis pasien. Dengan SQL Injection, penyerang bisa mendapatkan akses ke informasi pribadi, menjalankan perintah berbahaya, dan mengganggu integritas serta kerahasiaan data dalam sistem rumah sakit.

Untuk mengatasi ancaman ini, rumah sakit modern mengadopsi teknologi blockchain dan Smart contract dengan algoritma konsensus Proof of Work (PoW). Blockchain memastikan integritas dan transparansi data rekam medis dengan menyimpan hash data di blockchain, sehingga setiap perubahan dapat dideteksi. Smart contract mengatur dan memverifikasi izin akses berdasarkan identitas pengguna, memastikan hanya pengguna yang diotorisasi yang dapat mengakses atau memodifikasi data. Dengan API Gateway yang aman dan penggunaan teknik seperti parameterized queries atau ORM untuk berinteraksi dengan basis data, risiko serangan SQL Injection dapat diminimalisir, meningkatkan keamanan dan keandalan data rekam medis ((Lan et al.,2021; Falazi et al.,2024; Garriga et al., 2021; dan Honari et al.,2023).

#### E. Validasi dan Verifikasi

##### 1) Validasi Data

Validasi data dilakukan untuk memastikan bahwa data yang digunakan dalam penelitian ini akurat dan relevan. Proses validasi melibatkan pengecekan kesesuaian data dengan sumber aslinya dan pengecekan ulang data yang dikumpulkan melalui studi literatur dan studi kasus.

##### 2) Verifikasi Hasil

Verifikasi hasil penelitian dilakukan dengan membandingkan temuan penelitian ini dengan hasil penelitian sebelumnya yang sejenis. Proses ini membantu memastikan bahwa hasil

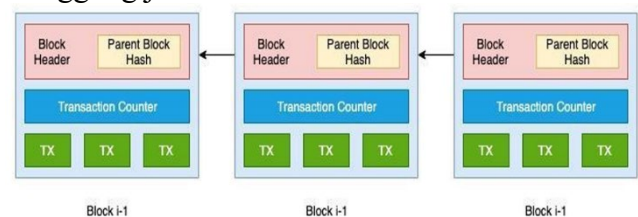
penelitian ini konsisten dan dapat diandalkan. Selain itu, verifikasi juga dilakukan melalui diskusi dengan ahli di bidang keamanan data dan teknologi blockchain.

Dengan tahapan penelitian yang rinci dan terstruktur ini, diharapkan penelitian dapat memberikan wawasan yang komprehensif dan dapat diandalkan mengenai penggunaan teknologi blockchain dan smart contract untuk meningkatkan keamanan data rekam medis di Puskesmas Gajahan.

### III. HASIL DAN PEMBAHASAN

#### A. Arsitektur Blockchain

Dalam arsitektur blockchain, algoritma yang digunakan adalah algoritma konsensus. Karena mekanisme konsensus yang digunakan oleh blockchain, data transaksi dapat disebar dan disimpan dengan aman di jaringan setelah melalui verifikasi dan validasi independen. Secara alami, tidak ada satu entitas pun yang memiliki akses ke keseluruhan data transaksi yang tercatat di seluruh jaringan Blockchain. Sistem ini mencatat setiap transaksi yang terjadi di setiap node, sehingga lebih sulit untuk diubah oleh pihak yang tidak bertanggung jawab.



Gambar 1. Gambar rantai blockchain

Contoh penerapan teknologi blockchain ditunjukkan pada Gambar 1. Sebuah blok hanya memiliki satu blok permanen, yaitu hash dari blok sebelumnya yang disimpan dalam header blok. Tidak ada blok induk untuk blok genesis, yang merupakan blok pertama pada blockchain (Purwono et al., 2023).

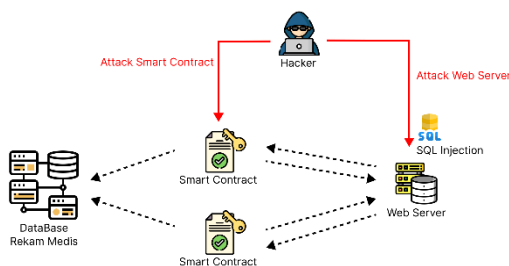
#### B. Algoritma Konsensus Proof of Work Sebagai Solusi Keamanan Data Rekam Medis Puskesmas Gajahan

Algoritma konsensus Proof-of-Work (PoW) adalah mekanisme yang digunakan dalam jaringan

blockchain untuk memastikan semua peserta setuju pada satu versi dari data yang benar. Cara kerjanya melibatkan penambang (miners) yang bersaing untuk memecahkan teka-teki kriptografis kompleks yang memerlukan sumber daya komputasi signifikan. Penambang pertama yang memecahkan teka-teki ini berhak menambahkan blok transaksi baru ke blockchain dan mendapatkan imbalan. Algoritma ini dianggap aman karena memerlukan biaya komputasi yang tinggi untuk memanipulasi data, sehingga menjadikannya pilihan yang kuat untuk mengamankan data rekam medis. Keamanan ini penting dalam konteks rekam medis karena memastikan bahwa data tidak dapat diubah atau dipalsukan tanpa deteksi, menjaga integritas dan kepercayaan terhadap data tersebut.

### C. Skenario Keamanan Data Rekam Medis

Mengamankan data rekam medis pasien dari berbagai ancaman, seperti serangan SQL Injection, merupakan perhatian utama bagi rumah sakit modern. Untuk mengatasi masalah ini, rumah sakit menerapkan teknologi Smart contract dan blockchain. Dalam sistem ini, Smart contract mengontrol akses dan modifikasi data rekam medis, sementara blockchain memastikan transparansi dan integritas data. Data rekam medis disimpan dalam database yang aman dan terpusat, namun untuk menjamin integritasnya, hash dari data tersebut disimpan di blockchain.



Gambar 2. Gambar skenario serangan *SQL Injection*.

Pada gambar 2 setiap permintaan untuk mengakses atau mengedit data rekam medis dilakukan melalui aplikasi web yang terhubung ke API Gateway, guna mencegah serangan SQL Injection. Untuk mengonfirmasi hak akses, API Gateway ini berkomunikasi dengan Smart

contract pada blockchain, tergantung pada identifikasi pengguna seperti perawat, dokter, atau pasien. Smart contract ini memiliki logika yang dibangun untuk memeriksa integritas data dan memvalidasi hak akses. Sebagai contoh, hash data rekam medis hanya dapat disimpan oleh dokter yang disetujui oleh institusi yang memiliki Smart contract.

Hash data dari rekam medis disimpan dan diverifikasi, serta otorisasi dokter adalah dua contoh fungsi Smart contract. Bahaya serangan SQL Injection akan berkurang ketika tidak ada koneksi langsung antara aplikasi web dan database. Selanjutnya, setiap perubahan pada data rekam medis akan diidentifikasi dan diverifikasi dengan mencatat hash data pada blockchain, menjamin integritas data.

Dengan menggunakan strategi seperti parameterized query atau object relational mapping (ORM) untuk berkomunikasi dengan database, API Gateway yang aman juga bertindak sebagai penghalang tambahan untuk memvalidasi permintaan dan menghentikan akses yang tidak diinginkan. Dengan metode ini, rumah sakit dapat memastikan bahwa data tidak rusak serta memperkuat keamanan data rekam medis, melindunginya dari serangan SQL Injection.

### D. Smart contract Dengan Menggunakan Algoritma Konsensus Prof of Work

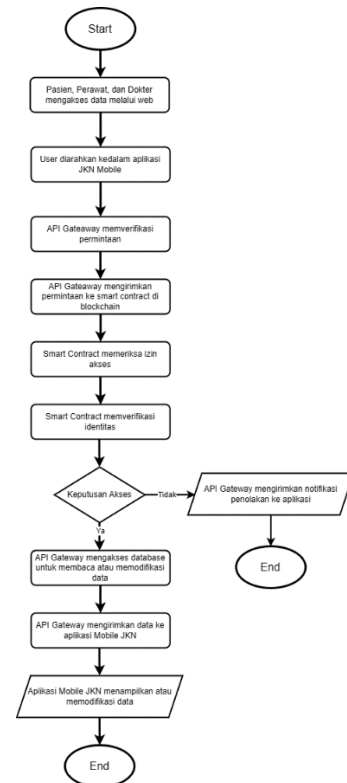
Smart contract adalah program komputer yang secara otomatis mengeksekusi perjanjian atau transaksi ketika kondisi yang telah ditentukan sebelumnya terpenuhi. Dalam konteks blockchain, Smart contract sering digunakan untuk menjalankan transaksi secara otomatis tanpa perlu adanya pihak ketiga. Algoritma konsensus Proof of Work (PoW) adalah salah satu mekanisme yang digunakan untuk mencapai konsensus di antara node dalam jaringan blockchain, memastikan bahwa semua transaksi yang terjadi adalah valid dan tidak dapat diubah.

Cara kerja Smart contract dengan menggunakan algoritma konsensus PoW melibatkan beberapa langkah kunci. Pertama, Smart contract ditulis dalam kode dan diterapkan pada blockchain. Ketika kondisi yang ditentukan dalam Smart contract terpenuhi, kontrak tersebut memicu

transaksi. Untuk memastikan transaksi tersebut valid, node dalam jaringan harus menyelesaikan teka-teki matematika yang kompleks (dikenal sebagai "mining"). Node yang pertama kali menyelesaikan teka-teki ini mendapat hak untuk menambahkan blok baru yang berisi transaksi ke blockchain. Proses ini memerlukan banyak tenaga komputasi dan waktu, yang menjadikan manipulasi transaksi menjadi sangat mahal dan tidak praktis.

Smart contract yang menggunakan algoritma konsensus PoW sering digunakan untuk meningkatkan keamanan informasi karena beberapa alasan. Pertama, proses mining yang memerlukan banyak sumber daya membuat serangan terhadap jaringan menjadi sangat mahal dan sulit untuk dilakukan. Kedua, setiap blok yang ditambahkan ke blockchain terkait dengan blok sebelumnya melalui hash kriptografi, yang membuat perubahan data pada satu blok akan mempengaruhi semua blok berikutnya, sehingga sangat sulit untuk memanipulasi data yang sudah tercatat. Ketiga, desentralisasi dalam jaringan PoW memastikan tidak ada satu pihak yang memiliki kontrol penuh atas jaringan, mengurangi risiko kegagalan sistem dan manipulasi data. Dengan demikian, Smart contract yang menggunakan PoW memberikan tingkat keamanan yang tinggi, membuatnya ideal untuk aplikasi yang membutuhkan integritas dan kepercayaan data yang kuat.

#### E. Alur Keamanan Data Rekam Medis Puskesmas Gajah Menggunakan Smart contract



Gambar 3. Flowchart alur sistem

Pada gambar 3 merupakan gambaran alur cara kerja smart contract dengan menggunakan algoritma konsensus pada puskesmas Gajah. Flowchart di atas menggambarkan alur keamanan data rekam medis puskesmas Gajah yang melibatkan beberapa pihak dan teknologi untuk memastikan integritas serta keamanan data. Proses dimulai ketika pasien, perawat, dan dokter mengakses data melalui web puskesmas Gajah. Setelah itu, user diarahkan ke dalam aplikasi JKN Mobile untuk melanjutkan akses. Permintaan dari user kemudian diverifikasi oleh API Gateway. API Gateway bertindak sebagai penghubung yang mengirimkan permintaan tersebut ke Smart contract di blockchain. Smart contract ini berfungsi untuk memeriksa izin akses dan memverifikasi identitas user. Jika izin akses diberikan, Smart contract akan memberikan keputusan akses.

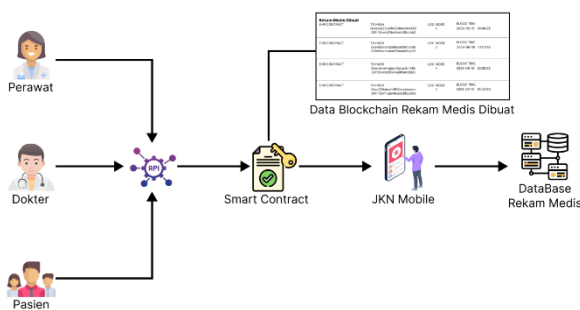
Jika keputusan akses disetujui, API Gateway akan mengakses database untuk membaca atau memodifikasi data yang diminta. Setelah data diproses, API Gateway mengirimkan data tersebut kembali ke aplikasi Mobile JKN. Aplikasi Mobile JKN kemudian menampilkan atau memodifikasi

data sesuai dengan permintaan user. Jika keputusan akses ditolak, API Gateway akan mengirimkan notifikasi penolakan ke aplikasi sehingga user mendapatkan informasi bahwa akses tidak diizinkan.

Dengan menggunakan blockchain dan Smart contract, alur ini memastikan bahwa setiap permintaan akses harus melalui proses verifikasi ketat, yang membantu dalam menjaga keamanan dan integritas data rekam medis dari potensi penyalahgunaan atau akses yang tidak sah.

#### F. Implementasi Pemanfaatan Teknologi Blockchain Dalam Keamanan Data Rekam Medis Puskesmas Gajahan Dengan Metode Smart contract Menggunakan Algoritma Konsensus Proof-of-Work

Pemanfaatan teknologi blockchain dalam keamanan data rekam medis di Puskesmas Gajahan menggunakan metode Smart contract dengan algoritma konsensus Proof-of-Work (PoW) dapat dilihat dari gambar skenario dibawah ini.



Gambar 4. Skenario implementasi smartcontract dan algoritma konsensus.

Pada gambar 4 skenario implementasi ini, pasien, perawat, dan dokter memiliki akses terhadap data rekam medis melalui API yang terhubung dengan Smart contract di blockchain. Proses dimulai dengan pengguna (dokter, perawat, atau pasien) yang melakukan permintaan akses data melalui aplikasi JKN Mobile. Permintaan ini pertama-tama diverifikasi oleh API Gateway untuk memastikan validitasnya sebelum diteruskan ke Smart contract. Smart contract, yang berfungsi sebagai penjaga izin dan identitas, memverifikasi apakah permintaan akses sah dan pengguna memiliki izin yang diperlukan. Algoritma konsensus Proof-of-Work digunakan

untuk memastikan bahwa setiap transaksi yang tercatat di blockchain telah melalui proses verifikasi yang kompleks, sehingga sulit untuk dimanipulasi atau diubah tanpa deteksi.

Setelah verifikasi berhasil, Smart contract memberikan keputusan akses. Jika akses diizinkan, API Gateway mengakses database rekam medis untuk membaca atau memodifikasi data sesuai permintaan dan kemudian mengirimkan data tersebut ke aplikasi JKN Mobile untuk ditampilkan atau dimodifikasi lebih lanjut oleh pengguna. Data rekam medis yang telah diproses dan divalidasi kemudian dicatat dalam blockchain. Setiap perubahan atau penambahan data rekam medis memiliki hash transaksi unik yang memastikan transparansi dan integritas data, serta memungkinkan pelacakan semua aktivitas yang terjadi.

Penggunaan teknologi blockchain dengan Smart contract dan PoW dalam sistem ini memastikan bahwa data rekam medis di Puskesmas Gajahan tetap aman, tidak dapat diubah tanpa izin, dan dapat diverifikasi kebenarannya. Sistem ini juga meningkatkan kepercayaan antara pasien, perawat, dan dokter terhadap keamanan dan integritas data medis yang mereka akses dan kelola.

#### IV. KESIMPULAN

Penelitian ini berhasil menunjukkan bahwa penerapan teknologi blockchain, khususnya dengan metode Smart contract dan algoritma konsensus Proof-of-Work (PoW), dapat secara signifikan meningkatkan keamanan dan efisiensi pengelolaan data rekam medis di Puskesmas Gajahan. Dengan teknologi blockchain, setiap transaksi dan perubahan data direkam secara permanen dan transparan, sehingga memastikan integritas dan kepercayaan terhadap data medis. Smart contract membantu mengurangi kesalahan manusia dan meningkatkan efisiensi melalui otomatisasi proses tanpa memerlukan perantara pihak ketiga. Penerapan ini juga memberikan keamanan tambahan terhadap ancaman serangan seperti SQL injection dengan memastikan tidak ada koneksi langsung antara aplikasi web dan database. Secara keseluruhan, teknologi

blockchain menunjukkan potensi besar dalam meningkatkan perlindungan dan manajemen data sensitif di sektor kesehatan, khususnya di institusi seperti Puskesmas Gajahan.

#### UCAPAN TERIMA KASIH

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penelitian ini dengan baik. Penelitian yang berjudul "Pemanfaatan Teknologi Blockchain dalam Keamanan Data Rekam Medis Puskesmas Gajahan dengan Metode Smart contract". Ucapan terimakasih disampaikan penulis kepada Bapak Bondan Wahyu Pamekas, S.Kom, M.Kom selaku dosen pembimbing yang telah memberikan bimbingan, masukan, dan dukungan penuh selama proses penelitian ini berlangsung. Bimbingan dan saran yang diberikan sangat berharga dalam penyelesaian penelitian ini. Penulis juga mengucapkan terimakasih kepada penulis kedua, Agung Frisky Ardianto, yang telah berkontribusi secara signifikan dalam penelitian ini, memberikan ide-ide, serta dukungan yang sangat berharga selama proses penyusunan penelitian ini.

#### REFERENSI

- [1] P. Bellavista, C. Esposito, L. Foschini, C. Giannelli, N. Mazzocca, and R. Montanari, "Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing," *Sensors*, vol. 21, no. 15, p. 4955, 2021.
- [2] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *Comput. Surveys*, vol. 54, no. 8, pp. 1–41, 2022.
- [3] M. Cheng, H. Y. Chong, and Y. Xu, "Blockchain-smart contracts for sustainable project performance: Bibliometric and content analyses," *Environment, Development and Sustainability*, vol. 26, pp. 8159–8182, 2024.
- [4] S. Cohen, A. Rosenthal, and A. Zohar, "Reasoning about the future in blockchain databases," in *2020 IEEE 36th International Conference on Data Engineering (ICDE)*, 2020, pp. 1930–1933.
- [5] G. Falazi, U. Breitenbücher, F. Leymann, and S. Schulte, "Cross-chain smart contract invocations: A systematic multi-vocal literature review," *ACM Comput. Surv.*, January 2024.
- [6] M. Garriga, S. Dalla Palma, M. Arias, A. De Renzis, R. Pareschi, and D. A. Tamburri, "Blockchain and cryptocurrencies: A classification and comparison of architecture drivers," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 8, p. e5992, 2021.
- [7] K. Honari, S. Rouhani, N. E. Falak, Y. Liu, Y. Li, and H. Liang, "Smart contract design in distributed energy systems: A systematic review," *Energies*, vol. 16, no. 12, p. 4797, 2023.
- [8] K. Koç and A. Gürgün, "Drivers for construction stakeholders to adopt smart contracts," *Journal of Construction Engineering, Management & Innovation*, vol. 3, pp. 101–112, 2020.
- [9] A. Kumari, A. Shukla, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Et-deal: A P2P smart contract-based secure energy trading scheme for smart grid systems," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 1051–1056.
- [10] Y. Lan, J. Gao, Y. Li, K. Wang, Y. Zhu, and Z. Chen, "TrustCross: Enabling confidential interoperability across blockchains using trusted hardware," in *BRAINS'21, ACM*, 2021, pp. 17–23.
- [11] C. Li, J. Long, Y. Liu, Q. Li, W. Liu, P. Feng, B. Li, and J. J. Xian, "Mechanism analysis and partition characteristics of a recent highway landslide in Southwest China based on a 3D multipoint deformation monitoring system," *Landslides*, vol. 18, pp. 2895–2906, 2021.
- [12] J. Li and M. Kassem, "Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction," *Automation in Construction*, vol. 132, p. 103955, 2021.
- [13] W. Lu, X. Li, F. Xue, R. Zhao, L. Wu, and A. G. Yeh, "Exploring smart construction objects as blockchain oracles in construction supply chain management," *Automation in Construction*, vol. 129, p. 103816, 2021.
- [14] W. Nie and L. Liu, "A ring signature trust model for project review based on blockchain smart contract," *Tehnički Vjesnik*, vol. 28, pp. 347–356, 2021.
- [15] P. Purwono, P. Dewi, and S. D. Kurniawan, "Pengembangan keamanan sistem rekam medis berbasis blockchain dengan smart contract," *Smart Comp*, vol. 12, no. 2, 2023.
- [16] D. Tith, et al., "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthc. Inform. Res.*, vol. 26, no. 1, pp. 3–12, 2020.