**INTEGRITAS DATA INTELIJEN MILITER *PRIVATE BLOCKCHAIN* MENGGUNAKAN METODE *PRACTICAL BYZANTINE FAULT TOLERANCE* DAN *PROOF OF AUTHORITY***

**Muhammad Rizal Supriadi\*1, Roni Andarsyah2**

1,2Universitas Logistik dan Bisnis Internasional

Email: 11194059@std.poltekpos.ac.id, 2roniandarsyah@ulbi.ac.id

**Abstrak**

Keamanan dan integritas data intelijen militer menjadi hal yang sangat penting dalam menghadapi ancaman di era modern saat ini. Penelitian ini mengembangkan solusi berbasis *blockchain* dengan menggunakan *private* *blockchain* yang diterapkan dengan metode *Practical* *Byzantine* *Fault* *Tolerance* (PBFT) dan *Proof* *of* *Authority* (PoA) untuk menjaga keamanan dan integritas data intelijen militer. *Private* *blockchain* digunakan untuk memastikan hanya pihak yang berwenang yang dapat mengakses data intelijen militer, sedangkan PBFT dan PoA digunakan untuk menjaga integritas dan konsistensi data serta memberikan otoritas kepada partisipan yang dipercaya untuk validasi transaksi dalam *blockchain*. Selain itu, solusi ini juga terintegrasi dengan IPFS untuk penyimpanan dokumen yang aman dan *Hyperledger* *Explorer* untuk memantau, mencari, dan memelihara *blockchain* dan data terkait. Dengan memanfaatkan IPFS, data intelijen militer dapat disimpan dengan aman dan terenkripsi secara terdesentralisasi, sedangkan *Hyperledger* *Explorer* memudahkan *monitoring* dan pemeliharaan *blockchain*. Penelitian ini bertujuan untuk memberikan kontribusi pada pengembangan teknologi *blockchain* yang lebih baik untuk menjaga keamanan dan integritas data dalam lingkungan intelijen militer, serta memperkuat pertahanan negara dari ancaman dan konflik modern. Solusi berbasis *blockchain* dengan PBFT dan PoA, serta terintegrasi dengan IPFS dan *Hyperledger* *Explorer*, diharapkan dapat menjadi alternatif yang efektif dan efisien dalam menjaga keamanan dan integritas data intelijen militer.

**Kata kunci**: *Blockchain,* Intelijen*, Private Blockchain, Practical Byzantine Fault Tolerance, Proof of Authority*

***Abstract***

*The security and integrity of military intelligence data are extremely important in facing threats in the modern era. This study develops a blockchain-based solution using a private blockchain applied with the Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) methods to maintain the security and integrity of military intelligence data. Private blockchain is used to ensure that only authorized parties can access military intelligence data, while PBFT and PoA are used to maintain data integrity and consistency and provide authority to trusted participants for validating transactions in the blockchain. In addition, this solution is also integrated with IPFS for secure document storage and Hyperledger Explorer for monitoring, searching, and maintaining the blockchain and related data. By utilizing IPFS, military intelligence data can be securely and encryptedly stored in a decentralized manner, while Hyperledger Explorer facilitates blockchain monitoring and maintenance. This research aims to contribute to the development of better blockchain technology for maintaining the security and integrity of data in the military intelligence environment and strengthening the defense of the country against modern threats and conflicts. A blockchain-based solution with PBFT and PoA, as well as integrated with IPFS and Hyperledger Explorer, It is hoped that this solution can become an effective and efficient alternative in maintaining the security and integrity of military intelligence data.*

**Keywords**: *Blockchain, Intelligence, Private Blockchain, Practical Byzantine Fault Tolerance, Proof of Authority*

D

# PENDAHULUAN

alam era modern yang didominasi oleh teknologi, penggunaan intelijen militer menjadi salah satu komponen penting dalam operasi keamanan negara. Namun, tantangan dalam menjaga keamanan dan integritas data intelijen militer menjadi semakin kompleks dengan adanya ancaman siber dan serangan terhadap sistem informasi militer. Oleh karena itu, penggunaan teknologi *blockchain* dalam konteks ini menjadi sangat relevan, khususnya penggunaan private *blockchain* yang memberikan keberlanjutan, kehandalan, dan privasi dalam mengelola data intelijen militer.

*Private* *blockchain*, sebagai salah satu jenis *blockchain* yang membatasi akses hanya untuk pengguna yang diizinkan, dapat menjadi solusi untuk menjaga keamanan dan integritas data intelijen militer. Dalam pengaturan *private* *blockchain*, metode *Practical* *Byzantine* *Fault* *Tolerance* (PBFT) dan *Proof* *of* *Authority* (PoA) dapat menjadi pilihan untuk meningkatkan tingkat keamanan. Metode PBFT dapat mengatasi masalah *Byzantine* *Generals* *Problem* yang mungkin muncul dalam jaringan *blockchain*, sehingga memastikan integritas data yang tinggi. Sedangkan, PoA sebagai mekanisme konsensus dapat memastikan bahwa pengguna yang memiliki otoritas dan kepercayaan dalam jaringan memiliki kendali penuh atas proses verifikasi dan validasi transaksi.

Terdapat tiga jenis utama *blockchain*, yaitu publik (tanpa izin), konsorsium (izin publik), dan *private* (pribadi). Setiap jenis memiliki karakteristik yang berbeda terkait akses, penulisan, dan pembacaan data di dalamnya. Pada *blockchain* publik, data dapat dilihat oleh siapa pun dan siapa pun dapat bergabung serta berkontribusi dalam konsensus dan perubahan pada perangkat lunak inti. Keamanan *blockchain* bergantung pada validasi oleh komunitas untuk menjaga konsistensi konten buku besar yang direplikasi di antara pengguna atau otoritas yang berbeda. Selain itu, *blockchain* juga menjadi teknologi dasar untuk mata uang digital seperti *bitcoin* [1, p. 27].

Dalam *blockchain* publik atau tanpa izin, partisipasi dapat dilakukan oleh siapa pun tanpa identitas yang spesifik. Biasanya, *blockchain* publik melibatkan mata uang kripto asli dan menggunakan konsensus berdasarkan "*proof of work*" (PoW) serta insentif ekonomi. Di sisi lain, *blockchain* berizin atau berdasarkan izin beroperasi di antara sekelompok peserta yang dikenal dan teridentifikasi. *Blockchain* berizin memberikan cara untuk mengamankan interaksi antara entitas yang memiliki tujuan bersama tetapi tidak sepenuhnya saling percaya, seperti bisnis yang melakukan pertukaran dana, barang, atau informasi. Dengan mengandalkan identitas para peserta, *blockchain* berizin dapat menggunakan konsensus tradisional berdasarkan *Byzantine*-*fault* *tolerant* (BFT) [2, p. 1].

Penelitian ini bertujuan untuk memastikan keamanan dan integritas data yang lebih baik: Dengan mengimplementasikan teknologi *blockchain*, maka data dapat disimpan secara aman dan terlindungi dari ancaman keamanan serta perubahan data yang tidak sah. Hal ini akan membantu memastikan keamanan dan integritas data yang lebih baik serta mengurangi biaya dan waktu untuk memperbaiki data yang salah: Dengan memastikan integritas data yang lebih baik, maka akan mengurangi biaya dan waktu yang dibutuhkan untuk memperbaiki data yang salah atau tidak akurat. Hal ini akan membantu meningkatkan efisiensi dan produktivitas suatu organisasi atau perusahaan.

Penelitian *Systematic Literature Review* (SLR) mengenai penerapan teknologi *blockchain* dalam bidang *private* *blockchain* ditemukan dalam kurun waktu 2016-2023. Penelitian tersebut diinisialisasi oleh [3] Dalam hasil penelitian ini, ditemukan bahwa implementasi jaringan terdistribusi seperti *blockchain* pada sektor kesehatan berpotensi memberikan manfaat yang signifikan dalam berbagai aspek, seperti peningkatan kualitas hasil klinis, pengurangan kesalahan medis, manfaat keuangan dan operasional bagi organisasi, serta peningkatan kemampuan untuk melakukan penelitian dan meningkatkan kesehatan masyarakat secara keseluruhan. Oleh karena itu, teknologi *blockchain* dianggap sebagai solusi yang tepat untuk memastikan keamanan dan privasi data pasien dalam industri kesehatan modern.

Penelitian [1] juga memperkuat penelitian sebelumnya dimana Dengan memanfaatkan teknologi *blockchain*, jaringan *blockchain* dapat dibangun sehingga setiap node dapat saling memverifikasi keabsahan catatan transaksi di setiap departemen. Dengan demikian, model ini dapat menjawab masalah keamanan data nilai mahasiswa yang rentan terhadap peretasan oleh pihak yang tidak bertanggung jawab baik dari dalam kampus maupun dari luar kampus dalam mencatat perekaman nilai mahasiswa. Berbeda dengan hal tersebut, pada penelitian yang dilakukan oleh [4] berfokus pada SLR untuk melakukan klasifikasi kompherensif pengguan *blockchain* dan aplikasi yang diaktifkan menggunakan *blockchain*.

Penelitian mengenai penerapan teknologi *blockchain* dalam pengamanan data diperjatam dalam penggunaan metode konsensus. Sepertihalnya penelitian yang dilakukan oleh [5] menggunakan metode konsensus BFT dan PBFT dimana BFT (*Bizantine Fault Tolerance*) merupakan protokol yang dirancang untuk mengatasi kesalahan *Byzantine* dalam sistem terdistribusi. Protokol ini didasarkan pada konsep kriptografi dan menggunakan tanda tangan digital untuk mengotentikasi pengguna di dalam jaringan sedangkan PBFT adalah merupakan konsep keamanan inovatif yang meningkatkan keamanan data di lingkungan *blockchain* terdesentralisasi.

Penelitian yang dilakukan oleh [2] membahas tentang Fabric, sebuah sistem *open-source* modular dan dapat diperluas untuk menjalankan *blockchain* yang di-hosting oleh *Hyperledger*. *Fabric* merupakan sistem *blockchain* pertama yang mendukung protokol konsensus modular dan memungkinkan penggunaan bahasa pemrograman umum tanpa tergantung pada kriptocurrency asli. *Fabric* juga memperkenalkan desain *blockchain* baru untuk mendukung fleksibilitas. pernelitian tersebut juga menyajikan evaluasi implementasi *Fabric* dengan mengimplementasikan mata uang digital terinspirasi *Bitcoin* dan mendapatkan *throughput* lebih dari 3500 transaksi per detik dan waktu tunggu di bawah 1 detik. Penelitian ini juga memberikan pembahasan lengkap mengenai kebutuhan-kebutuhan dalam membangun sistem *blokchain*.

Berbagai ulasan yang mendalam terkait penggunaan *blockchain* dalam sistem pengamanan data dan privasi. Hasil dari pengembangan *blokchain* tersebut dilanjutkan melakukan integerasi dengan IPFS (*Interplanetary File System*) yang dilakukan penelitian oleh [6] Dalam model ini, *blockchain* menyediakan keamanan dan transparansi, dan *Interplanetary File System* (IPFS) menyediakan penyimpanan file terdesentralisasi dan keabadian, sehingga membuat penyimpanan ekonomis. Model yang diusulkan di masa depan akan diterapkan untuk menyimpan sejumlah besar data perguruan tinggi seperti detail biaya dan untuk menyimpan kertas-kertas soal dalam aplikasi terdesentralisasi.

Berdasarkan penelitian studi literature diatas, belum ditemukan implementasi blockchain yang bertujuan untuk keamanan dan integritas data intelijen militer. Mayoritas dari penelitian studi literatur yang sudah ada berupa implementasi pada sektor industri dan pendidikan serta implementasi sistem yang terpisah. Berbeda dengan hal tersebut pada artikel ini menyajikan kajian literature mengenai penerapan teknologi *blockchain* menggunakan *Hyperledger* *Fabric* dan diintegrasikan dengan IPFS serta *Hyperledger Explorer*. Kontribusi artikel ini terletak pada riset yang mendalam serta usulan riset kedepan mengenai penerapan teknologi *blockchain* dalam membangun sistem kemanan data Intelijen Militer dengan *integrase* IPFS dan *Hyperledger* *Explorer*. Tujuan dari artikel ini adalah melakukan peninjauan teknologi *blockchain* pada bidang Intelijen Militer serta melakukan integrasi untuk menambah keamanan sistem. Penelitian ini memiliki keunikan dalam bentuk studi literature menggunakan *sistematic* *literature* *review* (SLR) dalam memeriksa penggunaan teknologi *blockchain* pada bidang Intelijen Militer. Struktur penulisan artikel ini disusun secara sistematis, yang terdiri dari pendahuluan, tinjauan literatur sebelumnya, metodologi, hasil, pembahasan, dan kesimpulan.

# METODE PENELITIAN

Penelitian ini menggunakan *Systematic Literature Review* (SLR) dengan metode *text mining* untuk analisis deskriptif. SLR digunakan untuk memberikan gambaran yang komprehensif terkait topik penelitian yang sedang dilakukan. Sedangkan, *text mining* digunakan untuk memberikan gambaran umum dari artikel yang terkumpul berdasarkan kata-kata yang ada di seluruh artikel. Dalam studi literatur ini, proses *text mining* digunakan untuk memperkuat hasil dari proses SLR. Oleh karena itu, proses SLR dengan *text mining* yang digunakan dalam studi ini merupakan pengembangan proses SLR [7].

2.1 Proses Perencanaan

Tahapan literature review dalam proses pencaran serta proses klasifikasi artikel secara umum adalah sebagai berikut:

1. Menentukan kata kunci yang relevan dengan topik penelitian, seperti *blockchain*, *private* *blockchain*, IPFS, *hyperledger* *fabric*, dan *hyperledger explorer*.
2. Memilih artikel-artikel terbaru dengan rentang waktu publikasi antara 2017 hingga 2023, yang memiliki reputasi baik dan terindeks pada *database* yang relevan.
3. Melakukan pengelompokan artikel ke dalam subtopik yang sesuai dan memilih subtopik yang paling dominan jika ada artikel yang mencakup lebih dari satu subtopik.

2.2 Proses Pelaksanaan

Dalam penelitian mengenai blockchain, teknologi ini seringkali digunakan untuk meningkatkan keamanan dan integritas data. Oleh karena itu, penting untuk dapat memahami data yang tersimpan dalam blockchain dengan baik agar dapat dimanfaatkan secara maksimal. Salah satu metode yang digunakan untuk memproses data ini adalah *text processing* atau *text analysis*, yang merupakan suatu teknik yang digunakan untuk mengolah data teks atau dokumen dengan tujuan untuk mengekstraksi informasi yang berguna.

Pada tahapan ini, dilakukan sintesis hasil penelitian yang mencakup pembahasan tentang kontribusi artikel terhadap bidang keamanan dan integritas data, serta kendala-kendala yang dihadapi. Selain itu, pengembangan usulan riset terkait penerapan *blockchain* dalam bidang intelijen militer disusun dengan mempertimbangkan hasil *studi literature* dan kondisi intelijen militer di Indonesia. Proses sintesis ini bertujuan untuk memberikan gambaran keseluruhan tentang topik penelitian yang sedang dilakukan dan untuk mengidentifikasi kesimpulan dan saran yang dapat diambil dari hasil studi *literature*.

# HASIL DAN PEMBAHASAN

## 3.1. Hasil Pencarian dan Klasifikasi Artikel

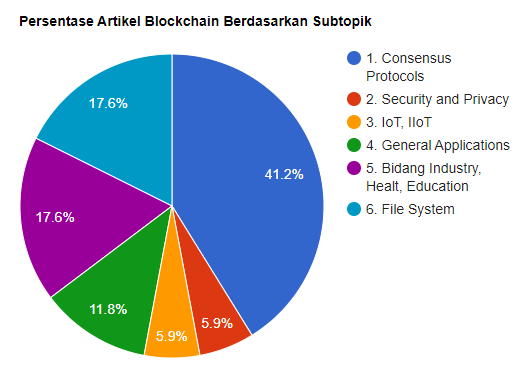
Dari hasil pencarian sesuai dengan kata kunci, diperoleh artikel ilmiah dalam bentuk jurnal dengan jumlah sebanyak 17. Artikel ilmiah tersebut diterbitkan pada tahun 2016 – 2023 serta memiliki tema *blockchain* dalam berbagai bidang untuk tujuan kemanan. Artikel ilmiah yang terkumpul kemudian dilakukan klasifikasi kembali berdasarkan subtopik dari artikel ilmiah yang secara umum terbagi dalam 6 kelompok yakni:

1. *Consensus Protocols*
2. *Security and Privacy*
3. *IoT, IIoT*
4. *General Applications*
5. Bidang *Industry, Healt, Education*
6. *File System*

Berikut adalah hasil dari pengelompokan dan pengumpulan artikel ilmiah yang telah dilakukan, yang disajikan pada Tabel 1.

## 3.2 Hasil Analisa Deskriptif

Diagram dan grafik dapat digunakan sebagai alat analisis untuk mengevaluasi posisi riset dalam suatu topik tertentu, seperti pada contoh kasus ini yaitu dalam penelitian terkait teknologi *blockchain*. Gambar 1 yang disajikan menunjukkan persentase hasil klasifikasi dari sejumlah artikel ilmiah yang dianalisis terkait dengan teknologi *blockchain*. Dengan adanya grafik tersebut, dapat membantu para peneliti untuk memahami secara visual distribusi topik yang paling banyak diteliti dalam bidang *blockchain*. Dari grafik tersebut, dapat dilihat bahwa terdapat variasi topik yang diangkat dalam artikel ilmiah terkait blockchain, yang meliputi protokol konsensus, keamanan dan privasi, penerapan pada *Internet of Things*, aplikasi umum, serta penggunaan *blockchain* di industri, kesehatan, pendidikan, dan sistem file. Berikut disajikan Gambar 2 yang menunjukkan presentase hasil klasifikasi artikel ilmiah terkait teknologi *blockchain* berdasarkan objek penelitian yang meliputi *blockchain*, *kripto* mata uang, dan IPFS. Melalui diagram ini, dapat dilihat distribusi artikel ilmiah yang terkait dengan masing-masing objek penelitian, sehingga dapat memberikan gambaran yang lebih jelas mengenai fokus penelitian dalam bidang teknologi *blockchain*.

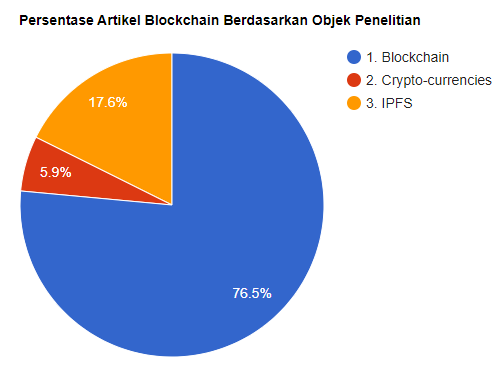


Gambar 1. Persentase Artikel Subtopik

Dari hasil persentase *blockchain* berdasarkan subtopik dapat dilihat hasilnya sebagai berikut:

1. Pada *consensus protocols* hasil yang didapat sebesar 41,2 %.
2. Pada subtopik *security and privacy* hasil yang didapat sebesar 5,9%.
3. Pada subtopik IoT sebesar 5,9%.
4. Pada subtopik general *applications* hasil yang didapat sebesar 11,8%.
5. Pada subtopik mengenai bidang *industry*, *healt, education* sebesar 17,6
6. Pada subtopik mengenai *file system* hasil yang didapat sebesar 17,6%

Dengan demikian, hasil analisis persentase *blockchain* berdasarkan subtopik ini memberikan gambaran yang jelas tentang berbagai aspek penting dalam pengembangan teknologi *blockchain* dan aplikasinya dalam berbagai bidang.



Gambar 2. Persentase Artikel Objek

Berdasarkan presentase diagram yang menunjukkan objek penelitian terkait dengan teknologi *blockchain*, diperoleh hasil sebagai berikut: sebesar 76,5% artikel yang dianalisis memiliki fokus penelitian pada *blockchain* sebagai teknologi utama yang menjadi dasar dalam pembuatan sistem yang menggunakan teknologi *blockchain*. Selain itu, ditemukan bahwa sebesar 5,9% artikel yang dianalisis membahas tentang penggunaan teknologi *blockchain* dalam pengembangan mata uang kripto atau *crypto-currencies*. Sementara itu, sebesar 17,6% artikel yang dianalisis membahas tentang teknologi IPFS atau *InterPlanetary File System*.

Tabel 1 Penelitian terkait penerapan *blockchain*

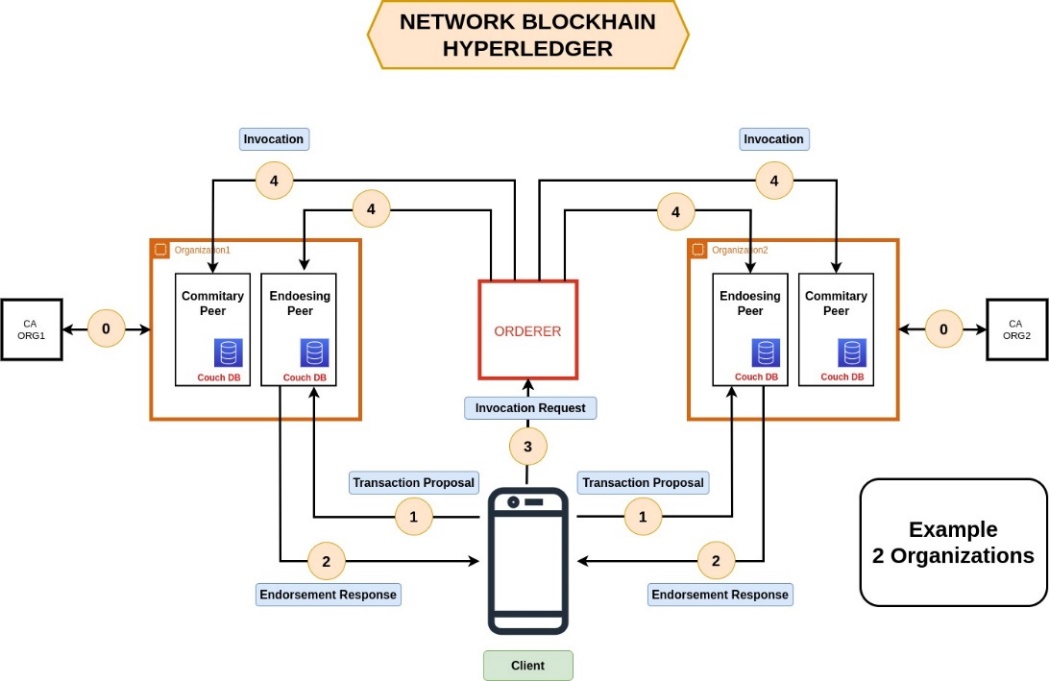
|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Sitasi** | **Judul** | **Deskripsi Singkat** |
| 1 | [8] | *A Study on Byzantine Fault Tolerance Methods in Distributed Networks* | Metode BFT untuk mengatasi kesalahan *Byzantine*. |
| 2 | [9] | *Blockchain Consensus: An analysis of Proof-of-Work and its applications* | Consensus *proof of work* dapat menjamin konsistensi antara *node-node* yang terlibat. |
| 3 | [10] | *Orphanage Management Using IPFS and Hyperledger Fabric* | Penggunaan IPFS digunakan untuk membantu melindungi data sensitive dalam lingkungan terdesentralisasi. |
| 4 | [11] | *Performance Analysis Of Proof-of-Elapsed-Time (POET) Consensus In The Saawtooth blockchain framework* | Penggunaan metode PoET dapat menyediakan dasar untuk analisis dan pengembangan model relasional formal dimasa depan. |
| 5 | [12] | *RPoA: Redefined Proof of Activity* | RPoA merupakan protokol konsensus yang mengatasi masalah utama dari protokol sebelumnya. |
| 6 | [13] | *Proofs of Proof-of-Stake with Sublinear Complexity* | PoS merupakan protokol konsensus *blockchian* yang menawarkan alternatif bagi PoW dalam hal efisien dan ramah lingkungan. |
| 7 | [14] | *Exploring Unfairness on Proof of Authority: Order Manipulation*  *Attacks and Remedies* | PoA memiliki kecepatan dalam hal transaksi namun PoA memiliki kelemahan dalam hal ketidak adilan. |
| 8 | [2] | *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains* | *Fabric* adalah sistem operasi terdistribusi modular dan dapat diperluas untuk menjalankan *blockchain* berizin. |
| 9 | [15] | *Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain- Based Applications* | Teknologi *blockchain hyperledger fabric* untuk solusi kontrol akses berbasis IoT dan *blockchain*. |
| 10 | [16] | *Implementasi Teknologi Blockchain pada Sistem Presensi Staff VM LePKom*  *Berbasis Web* | Implementasi *blockchain* pada aplikasi Asisten VM LePKom memberikan kelebihan pada sisi ketersediaan dan keamanan. |
| 11 | [17] | *Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and*  *Litecoin* | *Crypto-currencies* pada *Etherium* memiliki nilai yang lebih besar sedangkan *Litecoin* memiliki nilai yang lebih kecil. |
| 12 | [18] | *A look into the future of blockchain technology* | Pada penelitian ini menjelaskan tentang pemahaman yang lebih baik tentang masa depan berbasis *blockchain*. |
| 13 | [19] | *Blockchain Based Warehouse Supply Chain Management using Hyperledger*  *Fabric and Hyperledger Composer* | Integrasi *blockchain* dalam rantai pasok dengan menggunakan *hyperledger fabric* dan *hyperledger composer* sebagai kerangka *blockchain*. |
| 14 | [3] | *Private Blockchain in the Field of Health Services* | Platform *hyperledger* menjadi pilihan yang tepat untuk digunakan dalam kesehatan karena mampu mengimplemtasikan privasi dan keamanan yang lebih cepat. |
| 15 | [6] | *Integrating Blockchain and the Interplanetary File System, a resilient platform for storing students' file* | IPFS digunakan untuk menyimpan *file* besar yang tidak efisien disimpan pada *blockchain*. |
| 16 | [10] | *Orphanage Management Using IPFS and Hyperledger Fabric* | *Hyperledger fabric* membantu manajemen panti asuhan menyediakan sistem pencatatan data anak yatim yang aman, transparan dan bebas dari pemalsuan. |
| 17 | [20] | *Using IPFS and Hyperledger on Private Blockchain to*  *Secure the Criminal Record System* | Pemanfaatan IPFS dalam teknologi *blockchain* membuat sistem lebih aman, tidak dapat diubah sebagai media bukti kejahatan. |

Jika merujuk pada Tabel 1, dapat dilihat bahwa penelitian terkait blockchain memiliki dominasi yang dapat diidentifikasi dengan jelas. Dari hasil analisis tabel tersebut, dapat diketahui bahwa jenis penelitian yang mendominasi adalah yang terkait dengan teknologi protokol konsensus, yang mencakup tujuh artikel:

1. Publikasi terkait *Consensus Protocols* sebanyak 41,2%.
2. Publikasi terkait *Security and Privacy* sebanyak 5,9%.
3. IoT, IIoT sebanyak 5,9%.
4. Publikasi *General Applications* sebanyak 11,8%.
5. Publikasi terkait Bidang *Industry, Healt, Education* sebanyak 17,6%.
6. Publikasi *File System* sebanyak 17,6%.
   1. Hasil Studi Literatur

Setelah dilakukan proses klasifikasi terhadap sekumpulan artikel yang dianalisis terkait teknologi *blockchain*, ditemukan beberapa temuan menarik yang dapat memberikan gambaran tentang bagaimana teknologi ini sedang berkembang dan digunakan di berbagai bidang.

Sebanyak 17 artikel teridentifikasi memiliki topik yang beragam. Dari jumlah tersebut termasuk 7 tentang protokol konsensus, 1 tentang keamanan dan privasi, 1 tentang IoT, 2 artikel umum, 3 tentang industri/kesehatan/pendidikan, dan 3 tentang sistem file.

****

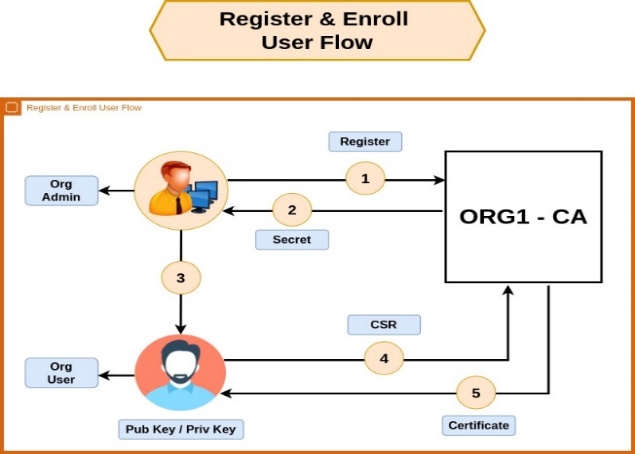
Gambar 1. Usulan Pengembangan Arsitektur Network Blockchain Pada Intelijen Militer

Pada gambar diatas merupakan skema atau arsitektur yang dibuat untuk melakukan pembuatan sistem *blockchain* dengan contoh 2 *Organizations*. Berikut merupakan tahapan yang terdapat pada gambar diatas:

1. **CA (*Certificate Authority*),** setiap organisasi memiliki CA nya tersendiri yang digunakan untuk mengelola dan menerbitkan sertifikat keamanan yang diperlukan dalam jaringan *blockchain*.
2. ***Transaction Proposal*** adalah permintaan transaksi yang dikirim oleh klien ke *endorsers* dalam jaringan *Hyperledger* *Fabric*. Ini berisi informasi tentang transaksi yang ingin dilakukan, seperti kode *Chaincode*, fungsi *Chaincode*, dan argumen.
3. ***Endorsement Response*** adalah respon dari *endorsers* setelah memverifikasi dan mengeksekusi permintaan transaksi dalam jaringan *Hyperledger Fabric*.
4. ***Invocation Request*** adalah permintaan klien kepada *endorsers* untuk menjalankan fungsi *Chaincode* pada jaringan *Hyperledger Fabric*.
5. ***Invocation*** atau pemanggilan adalah proses di mana klien mengirim permintaan untuk menjalankan fungsi *Chaincode* pada jaringan *Hyperledger Fabric*.
   1. Usulan Pengembangan

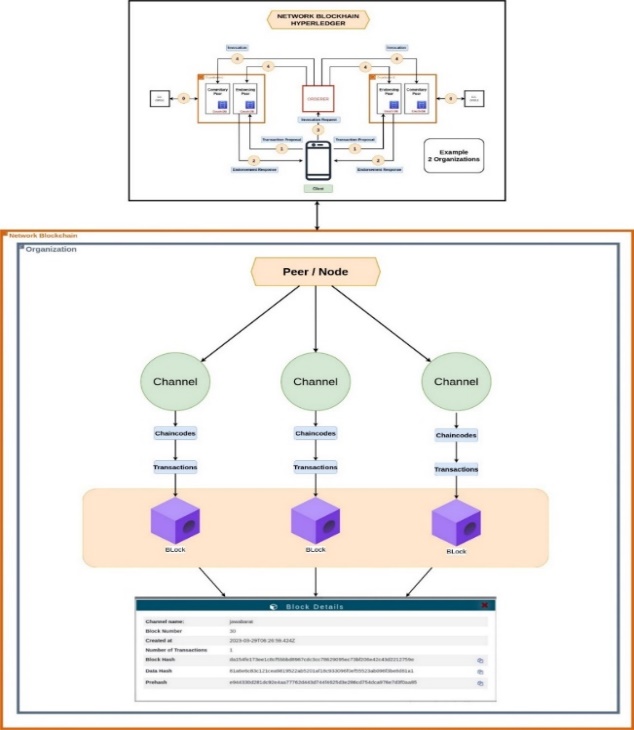
Berdasarkan tantangan yang dihadapi dalam penelitian mengenai keamanan dan integritas data pada bidang intelijen militer, diajukan usulan untuk menerapkan sistem *blockchain* pada bidang tersebut. Gambar 1 menunjukkan ilustrasi jaringan *blockchain* pada bidang intelijen militer, yang merupakan hasil dari pembahasan oleh [2]. Dimana dalam pembahasannya berfokus pada sistem *permissioned blockchain*. Usulan ini diharapkan dapat memberikan solusi yang efektif dan efisien dalam mengatasi masalah keamanan dan integritas data pada bidang intelijen militer.

Pada pengembangan sistem intelijen militer yang diusulkan, terdapat suatu *user flow* yang harus dipertimbangkan. *User flow* pada *blockchain* mencakup serangkaian langkah yang harus diambil oleh pengguna saat menggunakan aplikasi atau platform *blockchain*. *User flow* ini memiliki peran penting dalam memastikan pengguna dapat menggunakan sistem dengan mudah dan efektif, serta mengoptimalkan fungsi sistem secara keseluruhan.



Gambar 2. User Flow

Selanjutnya terdapat juga rancangan arsitektur pembuatan organisasi dalam implementasi sistem intelijen militer, berikut adalah gambaran rancangan arsitektur pembuatan organisasi dalam implementasi sistem intelijen militer, yang diusulkan dalam penelitian ini.

****

Gambar 3. Arsitektur Organisasi

Pada tahap pengembangan blockchain pada bidang intelijen militer, berikut beberapa penjelasannya:

1. *Private blockchain*

Digunakan untuk memastikan keamanan dan kerahasiaan data intelijen militer karena memiliki beberapa kelebihan dibandingkan dengan *public blockchain*. Berikut adalah beberapa alasan mengapa menggunakan *private blockchain*:

* 1. Kontrol akses: *Private blockchain* memungkinkan pengaturan level akses ke jaringan hanya untuk pihak-pihak yang telah diotorisasi. Hal ini memastikan bahwa hanya pihak-pihak yang memiliki hak akses yang dapat melihat dan memanipulasi data di dalam jaringan. Dalam konteks intelijen militer, ini penting untuk melindungi data yang sensitif dan kritikal dari pihak yang tidak berwenang.
  2. Kecepatan dan skalabilitas: Karena *private blockchain* hanya terdiri dari beberapa node yang terhubung, jaringan dapat berjalan lebih cepat dan lebih mudah untuk ditingkatkan skalanya. Hal ini memungkinkan pengolahan data yang lebih cepat dan efisien, yang sangat penting dalam lingkungan intelijen militer di mana waktu sangat berharga.
  3. Keamanan: *Private blockchain* memberikan keamanan tambahan dengan menggunakan algoritma konsensus seperti *Practical Byzantine Fault Tolerance* (PBFT) dan *Proof of Authority* (PoA). Algoritma konsensus ini memastikan bahwa transaksi di dalam jaringan diverifikasi dan diotorisasi oleh pihak yang telah ditunjuk sebelum data ditambahkan ke dalam blockchain. Hal ini memastikan keamanan dan integritas data, serta mencegah terjadinya serangan dari pihak yang tidak berwenang.
  4. Kerahasiaan: *Private blockchain* juga memastikan kerahasiaan data dengan menggunakan enkripsi dan teknologi keamanan lainnya untuk melindungi data dari pihak yang tidak berwenang. Dalam lingkungan intelijen militer, kerahasiaan data sangat penting karena data sensitif dan kritikal yang dapat membahayakan keselamatan nasional jika bocor ke tangan yang salah.

Dengan mempertimbangkan kelebihan-kelebihan di atas, penggunaan *private blockchain* dapat memberikan keamanan dan kerahasiaan data yang diperlukan dalam lingkungan intelijen militer yang kritis.

1. *Practical Byzantine Fault Tolerance* (PBFT)

Metode konsensus PBFT pada jaringan blockchain mengikuti tahapan berikut:

* 1. Membuat kumpulan pemegang kepentingan (*stakeholders*) yang terdiri dari anggota jaringan yang telah diotorisasi untuk berpartisipasi dalam konsensus PBFT.
  2. Mengirimkan transaksi proposal oleh pengirim kepada pemegang kepentingan untuk diverifikasi dan disetujui.
  3. Setiap pemegang kepentingan memvalidasi dan mengeksekusi transaksi secara terpisah dengan menggunakan algoritma PBFT.
  4. Setelah sebagian besar pemegang kepentingan menyetujui transaksi, transaksi tersebut dianggap sah dan disimpan ke dalam *ledger* *blockchain*.

Setiap pemegang kepentingan menyimpan salinan dari ledger *blockchain*, sehingga memastikan bahwa setiap pemegang kepentingan memiliki salinan yang sama dan akurat dari ledger.

1. *Proof of Authority* (PoA)

Pada tahapan *Proof of Authority* (PoA) pada jaringan *blockchain* yaitu:

* 1. Membuat jariangan *private blockchain* dan membuat *node* *authority* yang berperan sebagai pemegang otoritas.
  2. Karena tidak memerlukan proses mining yang memakan waktu dan sumber daya komputasi yang besar. PoA sendiri dapat meningkatkan efisiensi dan kecepatan transaksi dalam jaringan *blockchain*.

1. Keamanan dan Integritas Data

Mekanisme pengamanan dan integritas data sangat penting untuk diterapkan, berikut merupakan tahapan pengembangan mekanisme tersebut.

* 1. Enkripsi Data: Data intelijen militer perlu dienkripsi agar tidak mudah dibaca oleh pihak yang tidak berwenang. Pada tahap ini, dilakukan penggunaan algoritma enkripsi yang aman dan sulit untuk didekripsi oleh pihak yang tidak berwenang.
  2. Penggunaan Tanda Tangan Digital: Tanda tangan digital digunakan untuk memverifikasi keaslian data dan keaslian identitas pengguna. Setiap transaksi pada jaringan blockchain harus memiliki tanda tangan digital dari pengirim dan penerima, sehingga memastikan bahwa transaksi tersebut valid dan sah.

# KESIMPULAN

Berdasarkan hasil klasifikasi artikel terkait teknologi *blockchain*, didapati bahwa subtopik *consensus protocols* menjadi fokus utama dalam penelitian *blockchain* dengan *persentase* tertinggi sebesar 41,2%. Hal ini menunjukkan bahwa para peneliti tidak hanya berfokus pada penggunaan teknologi *blockchain* secara umum, tetapi juga pada pengembangan algoritma konsensus yang lebih baik dan efisien untuk memperkuat keamanan dan keandalan *blockchain*. Selain itu, mayoritas artikel yang dianalisis memfokuskan pada penggunaan *blockchain* dalam berbagai bidang industri, kesehatan, pendidikan, dan lainnya, serta pada pengembangan sistem file seperti IPFS.

Penelitian tentang penggunaan *blockchain* dalam lingkungan intelijen militer menunjukkan bahwa teknologi *blockchain* dapat memberikan solusi yang efektif dan efisien dalam menjaga keamanan dan integritas data intelijen militer. Melalui penggunaan *private blockchain*, PBFT, dan PoA, serta integrasi dengan IPFS dan *Hyperledger Explorer*, dapat dipastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan memvalidasi transaksi dalam *blockchain*. Selain itu, dengan memanfaatkan IPFS, data intelijen militer dapat disimpan dengan aman dan terenkripsi secara terdesentralisasi.

# SARAN

# Penggunaan *blockchain* pada intelijen militer adalah suatu hal yang potensial untuk menjaga keamanan dan integritas data. Oleh karena itu, diperlukan pengembangan lebih lanjut untuk meningkatkan kemampuan sistem dalam menangani ancaman dan serangan cyber.

# UCAPAN TERIMA KASIH

Penulis berterima kasih kepada Program Studi D4 Teknik Informatika Universitas Logistik dan Bisnis Internasional, dosen, staff, keluarga, teman-teman, dan rekan-rekan yang memberikan dukungan dan motivasi selama masa studi.

# DAFTAR PUSTAKA

[1] A. Alwi, Moh. Bhanu Setyawan, and M. Munirah, “Building Private Blockchain For Recording Student Values Data in Environment Faculty of Engineering at Universitas Muhammadiyah, Ponorogo,” *IJAIT Int. J. Appl. Inf. Technol.*, p. 27, Mar. 2021, doi: 10.25124/ijait.v4i01.3122.

[2] E. Androulaki *et al.*, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proceedings of the Thirteenth EuroSys Conference*, Apr. 2018, pp. 1–15. doi: 10.1145/3190508.3190538.

[3] P. Purwono, K. Nisa, Sony Kartika Wibisono, and Bala Putra Dewa, “Private Blockchain in the Field of Health Services,” *J. Adv. Health Inform. Res.*, vol. 1, no. 1, pp. 10–15, Feb. 2023, doi: 10.59247/jahir.v1i1.14.

[4] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telemat. Inform.*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[5] B. Shrimali and H. B. Patel, “Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6793–6807, Oct. 2022, doi: 10.1016/j.jksuci.2021.08.005.

[6] R. Roychaudhary, M. Gill, A. Chahande, C. Panjabi, and U. Kakde, “Integrating Blockchain and the Interplanetary File System, a resilient platform for storing students’ file,” *J. Interdiscip. Cycle Res.*, no. 0022.

[7] F. D. Wihartiko, S. Nurdiati, A. Buono, and E. Santosa, “Blockchain dan Kecerdasan Buatan dalam Pertanian : Studi Literatur,” *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 8, no. 1, p. 177, Feb. 2021, doi: 10.25126/jtiik.0814059.

[8] M. A. Nasreen, A. Ganesh, and C. Sunitha, “A Study on Byzantine Fault Tolerance Methods in Distributed Networks,” *Procedia Comput. Sci.*, vol. 87, pp. 50–54, 2016, doi: 10.1016/j.procs.2016.05.125.

[9] A. Porat, A. Pratap, P. Shah, and V. Adkar, “Blockchain Consensus: An analysis of Proof-of-Work and its applications.”.

[10] N. Gupta, A. Gupta, A. Ahirekar, O. Garg, and M. A. Patil, “Orphanage Management Using IPFS and Hyperledger Fabric,” vol. 07, no. 04, 2023.

[11] A. Corso, “PERFORMANCE ANALYSIS OF PROOF-OF-ELAPSED-TIME (POET) CONSENSUS IN THE SAWTOOTH BLOCKCHAIN FRAMEWORK”.

[12] S. Kamali *et al.*, “RPoA: Redeﬁned Proof of Activity”.

[13] S. Agrawal, J. Neu, E. N. Tas, and D. Zindros, “Proofs of Proof-of-Stake with Sublinear Complexity”.

[14] Q. Wang, R. Li, Q. Wang, S. Chen, and Y. Xiang, “Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies”.

[15] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, “Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications,” *Entropy*, vol. 23, no. 8, p. 1054, Aug. 2021, doi: 10.3390/e23081054.

[16] I. Wijaya and E. Haryatmi, “Implementasi Teknologi Blockchain pada Sistem Presensi Staff VM LePKom Berbasis Web,” vol. 5, 2020.

[17] J. Bhosale and S. Mavale, “Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and Litecoin,” vol. 6, 2018.

[18] D. Levis, F. Fontana, and E. Ughetto, “A look into the future of blockchain technology,” *PLOS ONE*, vol. 16, no. 11, p. e0258995, Nov. 2021, doi: 10.1371/journal.pone.0258995.

[19] “Blockchain Based Warehouse Supply Chain Management using Hyperledger Fabric and Hyperledger Composer,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 3S, pp. 147–151, Feb. 2020, doi: 10.35940/ijitee.C1033.0193S20.

[20] M. Ahmed, A. R. Pranta, Mst. F. A. Koly, F. Taher, and M. A. Khan, “Using IPFS and Hyperledger on Private Blockchain to Secure the Criminal Record System,” *Eur. J. Inf. Technol. Comput. Sci.*, vol. 3, no. 1, pp. 1–6, Jan. 2023, doi: 10.24018/compute.2023.3.1.81.