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

**LAPORAN INTERNSHIP II**

Diajukan untuk memenuhi kelulusan matakuliah Internship II

Tahun akademik 2022/2023

Disusun Oleh:

Nama: Muhammad Rizal Supriadi

NPM: 1194059



**PROGRAM DIPLOMA IV TEKNIK INFORMATIKA**

**UNIVERSITAS LOGISTIK & BISNIS INTERNASIONAL**

**BANDUNG**

**2023**

***SECURITY AND INTEGRITY OF MILITARY INTELLIGENCE DATA BASED ON PRIVATE BLOCKCHAIN USING PRACTICAL BYZANTINE FAULT TOLERANCE AND PROOF OF AUTHORITY METHODS***

***INTERNSHIP REPORT II***

*Submitted to fulfill Internship II course graduation*

*Academic year 2022/2023*

*Created By:*

*Name*: Muhammad Rizal Supriadi

NPM: 1194059



APPLIED BACHELOR PROGRAM OF INFORMATICSENGINEERING

***UNIVERSITY OF INTERNATIONAL LOGISTICS & BUSINESS***

***BANDUNG***

***2023***

# **LEMBAR PENGESAHAN**

**Keamanan dan Integritas Data Intelijen Militer Berbasis *Private Blockchain* Menggunakan *Metode Practical Byzantine Fault Tolerance* Dan *Proof Of Authority***

**LAPORAN INTERNSHIP II**

Program Studi DIV Teknik Informatika

**Oleh**

**1.19.4.059** - **Muhammad Rizal Supriadi**

Telah disetujui dan disarankan

Di Bandung pada tanggal

**Pembimbing**

**Roni Andarsyah, S.T., M.Kom., SFPC**

**NIK : 115.88.193**

**Koordinator Internship II**

**Mohamad Nurkamal Fauzan, S.T., M.T., SFPC**

**NIK : 113.80.159**

# **SURAT PERNYATAAN TIDAK MELAKUKAN PLAGIARISME**

Yang bertanda tangan di bawah ini:

|  |  |  |
| --- | --- | --- |
| Nama | : | Muhammad Rizal Supriadi |
| NPM | : | 1.19.4.059 |
| Program Studi | : | DIV Teknik Informatika |
| Judul | : | Keamanan dan Integritas Data Intelijen Militer Berbasis *Private Blockchain* Menggunakan *Metode Practical Byzantine Fault Tolerance* Dan *Proof Of Authority.* |

Menyatakan bahwa:

1. Laporan Internship2 ini asli dan belum pernah diajukan sebagai kelulusan matakuliah Proyek di Program Studi DIV Teknik Informatika, baik di Universitas Logistik dan Bisnis Internasional (ULBI) maupun di Perguruan Tinggi lain.
2. Laporan Internship2 ini tidak mengandung karya atau pendapat dari orang lain, kecuali jika secara jelas disebutkan sebagai acuan dengan mencantumkan nama pengarang dan daftar pustaka.
3. Pernyataan ini dibuat dengan jujur, dan jika terdapat penyimpangan atau ketidakbenaran, saya bersedia menerima sanksi akademik, termasuk pencabutan gelar yang telah diperoleh, dan sanksi lain sesuai norma perguruan tinggi.

Bandung, 16 April 2023

Penulis

**Muhammad Rizal Supriadi**

# **ABSTRAK**

Keamanan dan integritas data intelijen militer menjadi hal yang sangat penting dalam menghadapi ancaman dan konflik di era modern saat ini. Oleh karena itu, diperlukan suatu sistem yang dapat menjaga kerahasiaan, integritas, dan ketersediaan data intelijen militer. Dalam penelitian ini, dikembangkan suatu solusi yang menggunakan teknologi *blockchain* berbasis *private blockchain* dengan menerapkan metode *Practical Byzantine Fault Tolerance (*PBFT*)* dan *Proof of Authority (*PoA*)*.

*Private blockchain* digunakan untuk memastikan hanya pihak yang berwenang yang dapat mengakses data intelijen militer, sedangkan PBFT digunakan untuk menjaga integritas dan konsistensi data dalam kondisi serangan dari pihak yang tidak berwenang. Selain itu, PoA digunakan untuk memberikan otoritas kepada partisipan yang dipercaya untuk validasi transaksi dalam blockchain, sehingga mengurangi risiko serangan dari pihak yang tidak berhak. Namun, dalam pengembangan sistem ini terdapat batasan penggunaan algoritma PoA. Untuk PBFT, hanya diberikan contoh pada penggunaan tiga organisasi dalam satu komputer dengan menggunakan docker container dan implementasi IPFS serta integrasi *Hyperledger Explorer*.

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

# ***ABSTRACT***

*Security and integrity of military intelligence data are very important in dealing with threats and conflicts in today's modern era. Therefore, a system is needed that can maintain the confidentiality, integrity, and availability of military intelligence data. In this study, a solution was developed that uses private blockchain-based blockchain technology by applying Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) Methods.*

*Private blockchains are used to ensure only authorized parties can access military intelligence data, while PBFTs are used to maintain data integrity and consistency in conditions of unauthorized attacks. In addition, PoA is used to give trusted participants authority for the validation of transactions in the blockchain, thereby reducing the risk of attacks from unauthorized parties. However, in the development of this system there are limitations to the use of the PoA algorithm. For PBFT, only examples are given on the use of three organizations in one machine using docker containers and IPFS implementation and Hyperledger Explorer integration.*

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

# **KATA PENGANTAR**

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan  
penyusunan Laporan Intership dengan lancar dan tepat pada waktunya. Laporan  
program Internship 2 ini penulis susun sebagai salah satu syarat untuk kelulusan Internship II.

Semoga Laporan yang berjudul “KEAMANAN DAN INTEGRITAS DATA INTELIJEN MILITER BERBASIS *PRIVATE BLOCKCHAIN* MENGGUNAKAN METODE *BYZANTINE FAULT TOLERANCE* DAN *PROOF OF AUTHORITY* METHODS” dapat menjadi laporanyang sempurna beserta dengan hasil peneliatan yang selanjutnya dan dapat bermanfaat bagi para pembacanya.

Saya menyadari dalam laporan ini masih banyak kekurangan, oleh karenaitu perlu kritik dan saran untuk penyempurnaan laporan selanjutnya.

Bandung, 16 April 2023

Penulis

Muhammad Rizal Supriadi

# **DAFTAR ISI**

[LEMBAR PENGESAHAN i](#_Toc133945442)

[SURAT PERNYATAAN TIDAK MELAKUKAN PLAGIARISME ii](#_Toc133945443)

[ABSTRAK iii](#_Toc133945444)

[*ABSTRACT* iv](#_Toc133945445)

[KATA PENGANTAR v](#_Toc133945446)

[DAFTAR ISI vi](#_Toc133945447)

[DAFTAR GAMBAR viii](#_Toc133945448)

[DAFTAR TABEL ix](#_Toc133945449)

[BAB I PENDAHULUAN 1](#_Toc133945450)

[1.1 Latar Belakang 1](#_Toc133945451)

[1.2 Identifikasi Masalah 2](#_Toc133945452)

[1.3 Tujuan dan Manfaat 2](#_Toc133945453)

[1.4 Ruang Lingkup/ Batasan Penelitian 3](#_Toc133945454)

[1.5 Penelitian Sebelumnya 4](#_Toc133945455)

[1.6 Sistematika Penulisan 6](#_Toc133945456)

[BAB II](#_Toc133945457) [LANDASAN TEORI 7](#_Toc133945458)

[2.1 State of The Art 7](#_Toc133945459)

[2.1.1 Teknologi Utama 7](#_Toc133945460)

[2.1.2 Use-Cases 8](#_Toc133945461)

[2.1.3 Konsensus Terdistribusi *Blockchain* 12](#_Toc133945462)

[*2.1.3.1* *Permissioned Blockchain* 12](#_Toc133945463)

[*2.1.3.2* *Permissionless Blockchain* 16](#_Toc133945464)

[2.2 Taksonomi (Taxonomy) 18](#_Toc133945465)

[BAB III](#_Toc133945466) [METODOLOGI PENELITIAN 26](#_Toc133945467)

[3.1 Analisis Kebutuhan 26](#_Toc133945468)

[3.1.1 Tujuan Penelitian 26](#_Toc133945469)

[3.1.2 Tujuan Bisnis 26](#_Toc133945470)

[3.1.3 Kebutuhan Teknis 27](#_Toc133945471)

[3.2 Desain Sistem 32](#_Toc133945472)

[*3.2.1* *Network Blockchain* 32](#_Toc133945473)

[*3.2.2* *User Flow* 35](#_Toc133945474)

[*3.2.3* *Organization* 37](#_Toc133945475)

[3.3 Pengembangan 39](#_Toc133945476)

[*3.3.1* *Private Blockchain* 39](#_Toc133945477)

[3.3.2 *Practical Byzantine Fault Tolerance* (PBFT) 40](#_Toc133945478)

[3.3.3 *Proof of Authority* (PoA) 41](#_Toc133945479)

[3.3.4 Keamanan dan Integritas Data 41](#_Toc133945480)

[3.4 Implementasi 42](#_Toc133945481)

[3.4.1 Organisasi 42](#_Toc133945482)

[*3.4.2* *Data Field* 43](#_Toc133945483)

[*3.4.3* *Hyperledger Explorer* 45](#_Toc133945484)

[3.4.4 IPFS 46](#_Toc133945485)

[3.4.5 CouchDB 47](#_Toc133945486)

[BAB IV](#_Toc133945487) [PENUTUP 48](#_Toc133945488)

[4.1 Kesimpulan 48](#_Toc133945489)

[4.2 Saran 48](#_Toc133945490)

[DAFTAR PUSTAKA 49](#_Toc133945491)

# **DAFTAR GAMBAR**

[Gambar 3.1 Network Blockchain 33](#_Toc133945442)

[Gambar 3.2 User Flow 36](#_Toc133945442)

[Gambar 3.3 Arsitektur Organisasi 37](#_Toc133945442)

# **DAFTAR TABEL**

[Tabel 1. Taksonomi 18](#_Toc133945442)

# **BAB I PENDAHULUAN**

* 1. **Latar Belakang**

Dalam 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. 28].

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].

* 1. **Identifikasi Masalah**

Berdasarkan latar belakang diatas, maka dapat di identifikasi beberapa masalah yaitu sebagai berikut:

1. Masalah keamanan: Data sensitif dan rahasia sangat rentan terhadap ancaman keamanan, seperti hacking dan kebocoran data. Dalam hal ini, *blockchain* dapat memberikan keamanan yang lebih baik karena memiliki sifat transparan, terdesentralisasi, dan tahan terhadap perubahan data.
2. Masalah integritas data: Dalam beberapa kasus, data dapat diubah atau dimanipulasi dengan mudah, seperti data akuntansi dan data kesehatan. Dalam hal ini, *blockchain* dapat memastikan integritas data karena memiliki sistem pencatatan yang tidak dapat diubah dan transparan.
   1. **Tujuan dan Manfaat**

Berdasarkan identifikasi masalah diatas, maka tujuan pembuatan penelitian ini adalah sebagai berikut:

1. Untuk menunjukkan pentingnya penggunaan teknologi *blockchain* sebagai solusi untuk mengatasi masalah tersebut. Dengan menunjukkan masalah tersebut, maka diharapkan penggunaan *blockchain* dapat diterapkan sebagai solusi untuk memastikan keamanan dan integritas data yang lebih baik.
2. 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.
3. 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.
   1. **Ruang Lingkup/ Batasan Penelitian**

Untuk menghindari bahasan ini terlalu luas, maka ruang lingkup dari penelitian ini adalah sebagai berikut:

1. Memenuhi matakuliah Internship II.
2. Analisis sistem keamanan data dengan menggunakan teknologi *blockchain*, baik yang bersifat public maupun private.

Dalam penelitian ini, akan dilakukan analisis terhadap aspek keamanan data dalam implementasi *private blockchain* dengan menggunakan metode PBFT dan PoA. Penelitian ini akan memeriksa potensi masalah yang mungkin timbul, seperti skalabilitas, privasi dan kerahasiaan data, serta ancaman keamanan dan serangan yang mungkin terjadi dalam implementasi *private blockchain*. Tujuan akhir dari penelitian ini adalah menghasilkan rancangan sistem yang dapat memastikan keamanan data dalam penggunaan *private blockchain* menggunakan metode PBFT dan PoA, sebagai aplikasi konkret dalam konteks matakuliah Internship II.

* 1. **Penelitian Sebelumnya**

Berikut merupakan jurnal-jurnal dengan topik yang sama pada penelitian sebelumnya:

1. **Peneliti:** Mamun Ahmed, Akash Roy Pranta, Mst. Fahmida Akter Koly,

Farjana Taher, and Mohammad Asaduzzaman Khan

**Judul:** *Using IPFS and Hyperledger on Private Blockchain to Secure the Criminal Record System*

**Hasil Penelitian:** Dalam pendekatan kami, kami memanfaatkan IPFS dan *Hyperledger* untuk meningkatkan keamanan, integritas, dan keandalan sistem. Sifat *permissioned* dan sensitif dari *Hyperledger* memastikan konsistensi sistem di seluruh area. Selain itu, karena tidak diizinkannya penggunaan *cryptocurrency*, sistem kami menjadi lebih aman. Kami menggunakan IPFS untuk menyimpan setiap file media sebagai bukti kejahatan, sehingga transparansi dan pelacakan data dapat dilakukan melalui jaringan. Di sisi lain, *Ethereum* tidak cocok untuk digunakan dalam mengembangkan sistem pelacakan aktivitas kriminal karena catatan kriminal sangat sensitif dan *Ethereum* merupakan *blockchain* publik yang dapat diakses oleh siapa saja. Oleh karena itu, *Hyperledger* menjadi platform yang ideal untuk basis data sejarah kriminal kami [3, p. 5].

1. **Peneliti:** Prof. Reema Roychaudhary, Mercy Gill ,Aditya Chahande

**Judul:** *Integrating Blockchain and the Interplanetary File System, a resilient platform for storing students’ file*

**Hasil Penelitian:** Dalam model yang diusulkan, setelah proses autentikasi, siswa yang memasukkan rincian *login* yang benar akan diarahkan ke halaman unggah file di mana mereka dapat mengunggah *file* pdf yang berisi detail biaya. Setelah file tersimpan di *Interplanetary File* *System* (IPFS), *hash* yang dihasilkan akan dikirimkan kepada siswa dan disimpan dalam kontrak pintar *blockchain*. Pendekatan ini menggabungkan keamanan, transparansi, dan penyimpanan terdesentralisasi yang tidak dapat diubah dari *Interplanetary File System* (IPFS) dengan keuntungan dari teknologi *blockchain*. Model yang diusulkan ini dapat diterapkan di masa depan untuk menyimpan data perguruan tinggi dalam skala besar, seperti detail biaya dan kertas-kertas soal dalam aplikasi terdesentralisasi. Selain itu, integrasi teknologi *blockchain* dan *Interplanetary File System* (IPFS) dapat diterapkan dalam berbagai bidang untuk menggantikan sistem konvensional yang bergantung pada pusat pengendalian [4, p. 1096]

1. **Peneliti:** Purwono, Khoirun Nisa, Sony Kartika Wibisono, Bala Putra Dewa

**Judul:** *Private Blockchain in the Field of Health Services*

**Hasil Penelitian:** *Blockchain* semakin diminati dalam sektor kesehatan, seperti yang terbukti dengan semakin banyaknya peneliti yang memanfaatkan teknologi ini. Dalam menghadapi kebutuhan pengembang akan *toolkit* yang lengkap untuk mengimplementasikan standar privasi dan keamanan dengan cepat, *Hyperledger* menjadi pilihan yang tepat untuk aplikasi kesehatan. *Hyperledger* memberikan kontrol penuh terhadap *smart contracts* yang dapat dieksekusi dalam berbagai bahasa pemrograman, termasuk *Node.js* dan *Javascript*. Salah satu perbedaan utama antara *Hyperledger* dengan platform lain, seperti *Bitcoin* dan *Ethereum*, adalah penggunaan yang lebih banyak dalam membangun jaringan *blockchain* pribadi/berizin. Sementara itu, *Ethereum* dan *Bitcoin* dikenal lebih sebagai *blockchain* publik. Karena penggunaannya yang luas dalam pembuatan jaringan *blockchain* pribadi, pengguna/peserta dalam platform *Hyperledger* juga lebih terkontrol dan terawasi dengan baik [5, p. 14].

* 1. **Sistematika Penulisan**

Penyajian program laporan internship akan dibagi menjadi beberapa bab untuk mempermudah pencarian data dan informasi yang dibutuhkan, serta menunjukkan penyelesaian pekerjaan secara sistematis. Pembagian bab tersebut akan diatur sebagai berikut:

**BAB I PENDAHULUAN**

Bab ini akan membahas latar belakang, identifikasi masalah, tujuan, ruang lingkup, penelitian sebelumnya, dan sistematika penulisan. Pada bagian ini, pembaca akan diajak untuk menganalisis latar belakang serta mengidentifikasi masalah dari sistem yang akan diteliti, serta memahami tujuan penelitian yang dilakukan.

**BAB II LANDASAN TEORI**

Bab ini akan membahas uraian serta sumber tentang penjelasan mengenai sistem yang menjadi objek penelitian. Dalam bab ini, akan dijelaskan teori-teori yang relevan dan menjadi dasar dalam pengembangan sistem pada penelitian ini.

**BAB III METODOLOGI PENELITIAN**

Pada bab ini, akan dijelaskan metode yang digunakan dalam proses penyelesaian program penelitian internship, serta tahapan dan alur metode penelitian yang diterapkan dalam penelitian ini. Bab ini akan memberikan gambaran tentang bagaimana penelitian ini dilakukan dan langkah-langkah yang diambil dalam mengumpulkan dan menganalisis data.

**BAB IV PENUTUP**

Bab ini akan membahas pencapaian tujuan dari hasil penelitian yang dilakukan, serta memberikan saran konstruktif berdasarkan kesimpulan yang diperoleh dari sistem yang telah dibuat. Bab ini akan menjadi penutup dari laporan internship ini dan merangkum hasil penelitian serta rekomendasi untuk pengembangan lebih lanjut.

# **BAB II**

# **LANDASAN TEORI**

* 1. **State of The Art**

Di bagian ini, kami akan memperkenalkan implementasi terkini dari teknologi *Blockchain*. Pertama-tama, kami akan membahas teknologi kunci yang saat ini digunakan dalam *Blockchain*. Selanjutnya, kami akan melakukan survei terhadap kasus penggunaan dan aplikasi Blockchain yang populer.

* + 1. **Teknologi Utama**

Berikut merupakan beberapa teknologi yang mendasari *blockchain*

yang mendasari berbagai aspek tertentu dalam *blockchain.*

* **Teknologi *Distributed Ledger* (DLT)** memegang peran penting dalam perdagangan untuk mencatat informasi seperti nilai, pelacakan properti, transaksi keuangan, dan lainnya. Dalam pendekatan tradisional, *ledger* telah menjadi sangat penting. Seiring dengan penggunaan komputer dan digitalisasi yang semakin meluas, *ledger* telah beralih dari kertas ke bentuk digital [6]. Semua peserta dalam jaringan dapat memiliki salinan *ledger* yang sama. Setiap perubahan atau pembaruan pada *ledger* tercermin dalam semua salinan dalam interval waktu yang telah ditentukan. *Ledger* dijaga aman dan akurat melalui penggunaan algoritma kriptografi seperti tanda tangan digital dan fungsi *hash*. Kontrol atas *ledger* untuk modifikasi atau pembuatan didefinisikan oleh kesepakatan mutual yang disebut konsensus. Ini akan menentukan siapa yang dapat melakukan apa dalam *ledger* yang dibagi bersama.
* ***Smart contract*** merupakan sebuah algoritma komputer yang memungkinkan terjadinya pemahaman bersama dalam bentuk kesepakatan antara beberapa pihak tanpa adanya intervensi dari

pihak ketiga. Kontrak pintar ini merupakan sebuah perjanjian di mana ketentuan antara pembeli dan penjual ditulis dalam bentuk kode yang dapat dieksekusi sendiri sesuai dengan persyaratan yang telah ditentukan sebelumnya [7, p. 6798]. Dalam kata sederhana, *smart contract* merupakan baris kode yang dapat menjalankan dirinya sendiri dan diimplementasikan serta diatur berdasarkan persyaratan dan kesepakatan yang dibuat oleh dua atau lebih pihak. Teknologi *distributed ledger* dapat diterapkan dan dieksekusi melalui *smart contract*. Selain itu, teknologi *Blockchain* juga mengandalkan smart contract untuk mengimplementasikan logika bisnis pada *ledger* bersama.

* + 1. **Use-Cases**

Setelah terjadi revolusi dan popularitas *Bitcoin*, banyak industri yang tertarik untuk menggunakan teknologi *blockchain* dalam membangun sistem terdistribusi dan aman untuk berbagai keperluan seperti inventaris, manufaktur, rantai pasok, IoT, keuangan, tata kelola, dan banyak lagi. Pada bagian ini, kita akan membahas berbagai aplikasi dan kasus penggunaan dari Blockchain publik/*permission-less* dibandingkan dengan *blockchain* pribadi/*permissioned*.

* ***Public*/ *Permission-less Blockchain***

Sejak munculnya *Bitcoin* pada tahun 2008, konsep *ledger* terdistribusi di dalam *blockchain* publik telah menjadi populer dan menarik perhatian para peneliti karena dianggap sebagai teknologi revolusioner setelah internet. *Blockchain* publik dapat diakses oleh siapa saja dan siapa saja dapat berpartisipasi dalam proses konsensus untuk menentukan blok mana yang dapat ditambahkan ke dalam rangkaian [5, p. 11].

1. ***Ethereum***

*Ethereum* adalah platform *blockchain* *open-source* yang memungkinkan penggunaan *smart contract*. Sebagai *token* di *Ethereum*, *Ether* diberikan sebagai hadiah kepada para penambang yang melakukan komputasi untuk mengamankan konsensus *blockchain*. *Ethereum* berjalan pada mesin virtual terdesentralisasi (EVM) *Ethereum*, di mana skrip dijalankan pada jaringan yang terdiri dari *node* *Ethereum* publik. *Ethereum* 2.0 adalah versi yang ditingkatkan berdasarkan *Ethereum* asli. Peningkatan meliputi transisi dari PoW ke *Proof-of-Stake* (PoS), dan peningkatan *throughput* berdasarkan teknologi *sharding* [8].

1. ***Litecoin***

Litecoin adalah sebuah *cryptocurrency* baru yang memiliki kemampuan transaksi yang cepat. Seperti namanya, *Litecoin* lebih ringan dalam pemrosesan dan dapat ditambang di komputer desktop dengan kekuatan pemrosesan yang lebih rendah. *Litecoin* diperkenalkan oleh Charles Lee pada Oktober 2011. Berbeda dengan *Bitcoin* yang menggunakan algoritma *hash kriptografis* SHA-256, *Litecoin* menggunakan algoritma yang lebih baru yang disebut *Scrypt*. Saat ini, terdapat sekitar 84 juta *Litecoin* beredar di pasar, sementara *Bitcoin* hanya sekitar 21 juta. Waktu pemrosesan transaksi *Litecoin* sekitar 2,5 menit dibandingkan dengan sekitar 10 menit untuk transaksi *Bitcoin* [9, p. 134].

1. ***Cardano***

*Cardano* adalah lingkungan *blockchain* tanpa izin. Pertukaran mata uang di platform ini memerlukan dompet khusus dan antarmuka karena melibatkan banyak transaksi. Platform ini memfasilitasi mata uang kripto terdesentralisasi *open-source* yang disebut Ada (ADA), yang dapat digunakan untuk mengirim dan menerima dana digital. Ada digunakan di platform *Cardano*, seperti halnya mata uang '*ether*' yang digunakan di platform *Ethereum*. Selain itu, *Cardano* juga menyediakan lingkungan terdistribusi untuk aplikasi terdesentralisasi dan kontrak cerdas seperti *Ethereum*. *Cardano* didirikan dengan visi untuk meningkatkan keamanan, skalabilitas, dan interoperabilitas dengan sistem dan regulasi keuangan konvensional dengan memahami, belajar, dan menganalisis *Bitcoin* dan *Ethereum* [7, p. 6799].

1. ***Bitcoin Cash***

*Bitcoin Cash* adalah mata uang *kripto* yang diperkenalkan pada bulan Agustus 2017. Dibandingkan dengan *Bitcoin*, *Bitcoin Cash* meningkatkan ukuran blok dan memungkinkan lebih banyak transaksi untuk meningkatkan skalabilitas. Seperti *Bitcoin*, *Bitcoin Cash* juga menggunakan mekanisme konsensus yang sama, algoritma hash, dan teknis lainnya [7, p. 6799].

1. ***Polkadot***

*Polkadot* adalah *cryptocurrency* dengan mekanisme *proof-of-stake* yang berbeda. Peran utamanya adalah menyediakan interoperabilitas di antara *blockchain* lainnya. Protokol dan mekanisme *Polkadot* dirancang untuk menghubungkan *blockchain* berizin dan tidak berizin. *Polkadot* memungkinkan *blockchain-paralel* bekerja sama dengan *token* mereka sendiri untuk aplikasi tertentu. Di *Ethereum*, pengembang hanya dapat menciptakan aplikasi terdesentralisasi dengan langkah-langkah keamanan mereka sendiri, sedangkan di *Polkadot*, pengembang dapat membuat *blockchain* mereka sendiri dengan fasilitas keamanan internal [7, p. 6799].

* ***Private* *Permissioned Blockchain***

Sebuah *blockchain privat* adalah jenis jaringan *blockchain* yang dibatasi oleh suatu entitas. Jenis jaringan ini hanya terbatas bagi mereka yang memiliki izin akses. Selain itu, *blockchain privat* biasanya menggunakan sistem verifikasi terpusat dan dikendalikan oleh pencipta jaringan. Keuntungan menggunakan *blockchain* *privat* adalah kontrol yang lebih besar atas data dan transaksi yang terjadi di dalam jaringan. Hal ini membuat *blockchain privat* menjadi pilihan yang lebih cocok untuk perusahaan atau organisasi yang memerlukan keamanan dan privasi yang lebih tinggi [5, p. 11].

1. ***Hyperledger Fabric***

*Hyperledger Fabric* adalah contoh *blockchain* berizin yang dapat berperan dalam mengimplementasikan sistem kesehatan yang berorientasi pada pasien dan interoperabel. Ini adalah platform teknologi buku besar terdistribusi (DTL) sumber terbuka yang mendukung fitur keamanan dan privasi yang kuat. Karena *Hyperledger Fabric* dilisensikan dan menyediakan dukungan untuk *smart contract (chain code)*, maka semakin populer untuk banyak aplikasi di berbagai domain. *Fabric* memungkinkan peserta di konsorsium untuk mengembangkan dan menerapkan aplikasi menggunakan *Blockchain*. *Hyperledger Fabric* memiliki desain dan arsitektur modular sehingga memiliki tingkat fleksibilitas dan skalabilitas yang tinggi.

*Hyperledger Fabric* dapat dibagi secara horizontal menjadi empat komponen: manajemen identitas, manajemen buku besar, manajemen transaksi, dan *smart contract*; dan vertikal. *Hyperledger Fabric* dapat dibagi menjadi lima komponen: manajemen anggota, layanan konsensus, layanan *chain code*, keamanan, dan layanan kriptografi [5, p. 12].

* + 1. **Konsensus Terdistribusi *Blockchain***

Konsensus terdistribusi pada *blockchain* adalah proses di mana semua node atau peserta dalam jaringan *blockchain* harus sepakat pada keputusan transaksi yang dibuat. Konsensus diperlukan untuk memastikan bahwa transaksi yang dicatat pada *blockchain* benar dan valid, serta mencegah terjadinya duplikasi transaksi dan penipuan dalam jaringan.

Konsensus pada *blockchain* terdistribusi dapat dicapai melalui berbagai macam mekanisme, seperti *Proof of Work* (PoW), *Proof of Stake* (PoS), *Delegated Proof of Stake* (DPoS), dan lainnya. Setiap mekanisme konsensus memiliki keunggulan dan kelemahan masing-masing, dan dipilih berdasarkan kebutuhan dan tujuan jaringan *blockchain* tersebut.

Konsensus terdistribusi pada *blockchain* juga memungkinkan transaksi dapat diproses secara otomatis tanpa harus melalui pihak otoritas atau perantara. Ini mempercepat waktu pemrosesan transaksi dan mengurangi biaya transaksi, sehingga membuat *blockchain* menjadi lebih efisien dan terjangkau untuk digunakan dalam berbagai macam aplikasi dan industri.

* + - 1. ***Permissioned Blockchain***

*Consensus mechanism* pada *Permissioned Blockchain* dibagi menjadi dua kategori besar berdasarkan lingkungan kerja mereka yaitu (i) *synchronous* dan (ii) *asynchronous*. Sebelum kita memahami protokol di bawah lingkungan *synchronous* atau *asynchronous*, kita perlu memahami ide *State Machine Replication* (SMR) yang sangat membantu untuk mencapai konsensus dalam *permissioned blockchain*. Kontrak pintar dapat direpresentasikan melalui mesin keadaan terbatas (*finite state machine*/FSM).

1. ***Synchronous Network Environment***

Lingkungan jaringan sinkron, atau *synchronous network environment*, merujuk pada lingkungan di mana setiap node atau komputer dalam jaringan memberikan respons dalam waktu yang diketahui dan terbatas. Komunikasi antara node dalam lingkungan ini teratur dan terjadwal, sehingga waktu respons antar node dapat diukur dan diatur dengan baik. Lingkungan jaringan sinkron ini sering digunakan dalam sistem konsensus pada jaringan terdistribusi.

Kategori ini memiliki beberapa protokol yang berbeda. Berikut ini adalah penjelasan tentang protokol tersebut satu per satu.

* **PAXOS**

Terdapat beberapa jenis kegagalan dalam konsensus terdistribusi, seperti kegagalan *crash*, jaringan atau partisi, dan kegagalan *Byzantine* yang lebih lanjut terbagi menjadi kegagalan perangkat lunak, perangkat keras, dan perilaku jahat. Untuk menangani kegagalan *crash* dan jaringan, digunakan PAXOS. Dari total node dalam jaringan, satu atau lebih node mengajukan nilai (dalam bentuk proposal dengan nomor unik dan konstan yang terus bertambah) yang disebarkan ke seluruh jaringan. Node ini dikenal sebagai *proposer*. Node lainnya (yang dikenal sebagai *acceptor*) menerima atau menolak proposal berdasarkan perbandingan nomor yang terkait dengan proposal saat ini dengan nomor proposal yang diterima. Kategori ketiga dari node yang dikenal sebagai *learner*, mempelajari nilai yang dipilih oleh *acceptor* melalui prinsip mayoritas suara [7, p. 6801].

* **RAFT**

Dirancang sebagai alternatif Paxos, RAFT terutama bekerja pada faktor-faktor seperti toleransi kesalahan dan kinerja. Ide dasarnya adalah membagi masalah utama menjadi sub-masalah dan menangani masing-masing sub-masalah secara independen. Bersama-sama, semua node dalam sistem memilih pemimpin dan *node* lain menjadi pengikut pemimpin. Saat memilih pemimpin, konsep pemungutan suara mayoritas diterapkan di antara kandidat yang tersedia untuk kepemimpinan. Pemimpin menjaga dan mereplikasi transisi status (misalnya, *log*) di antara pengikut [7, p. 6801].

* **BFT (Byzantine Fault Tolerance)**

BFT atau *Byzantine Fault Tolerant* adalah 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. Salah satu kelemahan kriptografi adalah memerlukan infrastruktur yang terpercaya untuk mendistribusikan kunci publik dan pribadi secara awal, sehingga jika infrastruktur ini gagal, seluruh jaringan juga akan terganggu. Karena itu, beberapa solusi non-kriptografi telah diusulkan untuk memperbaiki kelemahan ini [10, p. 52].

1. ***Asynchronous Network Environment***

Lingkungan jaringan asinkron adalah lingkungan di mana pesan atau data dapat tiba dengan waktu yang tidak pasti atau tidak teratur. Waktu respons pesan dapat bervariasi karena faktor-faktor seperti jarak geografis, kepadatan lalu lintas, atau masalah teknis pada jaringan. Oleh karena itu, algoritma dan protokol jaringan harus dirancang untuk dapat berfungsi di lingkungan asinkron yang tidak dapat diandalkan.

* **PBFT (*Practical Byzantine Fault Tolerance*)**

PBFT merupakan konsep keamanan inovatif yang meningkatkan keamanan data di lingkungan blockchain terdesentralisasi. Metode berbasis anonimitas juga digunakan untuk memperoleh anonimitas data sensitif sebelum disimpan di dalam blockchain. Sistem ini menjamin penyimpanan data sensitif yang aman dan terlindungi, dengan IPFS sebagai alat penting yang digunakan untuk memastikan keakuratan data. Penggunaan teknologi *blockchain* membantu melindungi data sensitif di dalam lingkungan terdesentralisasi [11, p. 1].

1. ***Authority Based Environment***

Lingkungan berbasis otoritas atau *Authority Based Environment* merujuk pada lingkungan di mana hanya beberapa entitas atau individu tertentu yang memiliki hak istimewa untuk mengambil keputusan atau melakukan tindakan dalam sistem atau jaringan. Dalam konteks *blockchain*, lingkungan ini dapat merujuk pada penggunaan algoritma konsensus *Proof of Authority* (PoA).

* **PoA (*Proof of Authority*)**

*Proof of Authority* (PoA) adalah jenis algoritma konsensus berizin yang praktis dan efektif untuk sistem *blockchain* saat ini, terutama untuk konsorsium *blockchain*. Algoritma ini pertama kali diusulkan oleh Wood dan diimplementasikan oleh Ethereum pada tahun 2017. PoA mengandalkan sejumlah kecil node otoritas, disebut sebagai sealer, untuk melakukan prosedur konsensus. Dalam PoA, blok dan transaksi diverifikasi oleh node yang memenuhi syarat. Desain komite yang kecil memungkinkan konfirmasi transaksi yang cepat dan pengelolaan anggota yang mudah. Oleh karena itu, banyak proyek *blockchain* mengadopsi PoA sebagai algoritma konsensus pilihannya [12, p. 1].

* + - 1. ***Permissionless Blockchain***

*Permissionless blockchain* adalah jenis *blockchain* di mana siapa saja dapat bergabung sebagai node dalam jaringan dan berpartisipasi dalam proses validasi transaksi tanpa persyaratan khusus. Tidak ada pihak yang bertanggung jawab atas mengatur siapa yang dapat bergabung, membuat transaksi, atau mengontrol jaringan secara keseluruhan. Dalam *permissionless blockchain*, keamanan jaringan terjamin melalui konsensus mekanisme yang didesentralisasi.

* ***Proof of Work* (PoW)**

*Proof-of-Work* (PoW) adalah protokol konsensus yang digunakan dalam teknologi *blockchain* untuk memvalidasi transaksi dan menambahkan blok baru ke dalam *blockchain*. PoW membutuhkan pemecahan masalah matematis yang kompleks dan memakan waktu, yang dikenal sebagai "*mining*", oleh penambang atau miners. Setelah blok baru berhasil ditambang, mereka akan menyebarkan blok tersebut ke seluruh jaringan untuk disetujui oleh node lainnya. Dalam PoW, keamanan jaringan terjamin oleh daya komputasi yang dibutuhkan untuk menambang blok baru dan kepercayaan terhadap aturan konsensus yang ditetapkan [13, p. 4].

* ***Proof of Stake* (PoS)**

*Proof-of-stake* (PoS) adalah salah satu jenis protokol konsensus dalam jaringan *blockchain* di mana peserta mempertaruhkan sebagian dari kepemilikan mereka (stake) untuk memvalidasi transaksi dan membuat blok baru. Dalam protokol PoS, konsensus dibangun berdasarkan distribusi stake saat ini, dan diasumsikan bahwa mayoritas stake yang dimiliki oleh peserta adalah jujur dan tidak akan mencoba untuk melakukan serangan terhadap jaringan. Dalam konteks yang dijelaskan di atas, PoS digunakan untuk membangun konsensus dalam transfer nilai dan mempertahankan catatan saldo kepemilikan antara peserta di dalam jaringan *blockchain* [14, p. 3].

* ***Proof of Activity* (PoA)**

*Proof of Activity* (PoA) merupakan protokol konsensus yang menggabungkan PoW dan PoS untuk menciptakan mekanisme yang lebih tangguh dan aman. Dalam PoA, proses penambangan dimulai seperti pada PoW, di mana para penambang bersaing untuk menemukan blok baru dengan kekuatan komputasi mereka. Namun, setelah blok baru berhasil ditambang, sistem akan beralih ke PoS, di mana sekelompok validator dipilih secara acak untuk memvalidasi blok tersebut [15].

* ***Proof of Elapsed Time* (PoET)**

*Proof of Elapsed Time* (PoET) merupakan algoritma konsensus baru yang menjanjikan yang dikembangkan oleh Intel dengan dukungan teknologi *Software Guard Extension* (SGX)3, dan diimplementasikan dalam kerangka kerja *blockchain open source Hyperledger Sawtooth*. Meskipun merupakan bentuk konsensus PoW, PoET bertujuan untuk mengatasi masalah konsumsi energi yang boros yang terkait dengan algoritma aslinya [16, p. 19].

* 1. **Taksonomi (Taxonomy)**

Tabel 1. Taksonomi

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategori** | **Penulis** | **Judul** | **Hasil** |
| *Consensus Protocols* | M A Nasreen\*, Amal Ganesh, Sunitha C | *A Study on Byzantine Fault Tolerance Methods in Distributed Networks* | Untuk menjamin komunikasi yang andal bahkan dalam kondisi keberadaan kesalahan *Byzantine*, telah dipelajari solusi yang dapat disesuaikan untuk beradaptasi dengan jaringan yang jarang terhubung [17, p. 53]. |
| Amitai Porat, Avneesh Pratap, Parth Shah, and Vinit Adkar | *Blockchain Consensus: An analysis of Proof-of-Work and its applications.* | Meskipun *consensus proof-of-work* dapat menjamin konsistensi antara *node-node* yang terlibat, namun biayanya sangat mahal secara komputasi dan masih banyak tantangan teknis yang harus diatasi [18]. |
| Nilesh Gupta, Aniket Gupta, Atharva Ahirekar, Om Garg, Mrs. Aabha Patil | *Orphanage Management Using IPFS and Hyperledger Fabric* | Metode berbasis anonimitas juga digunakan untuk memperoleh anonimitas data sensitif sebelum disimpan di dalam blockchain. Sistem ini menjamin penyimpanan data sensitif yang aman dan terlindungi, dengan IPFS sebagai alat penting yang digunakan untuk memastikan keakuratan data. Penggunaan teknologi *blockchain* membantu melindungi data sensitif di dalam lingkungan terdesentralisasi [11, p. 1]. |
| Amie Corso | *Performance Analysis Of Proof-of-Elapsed-Time (POET) Consensus In The Saawtooth blockchain framework* | Tesis ini meneliti implikasi variasi interval blok dan ukuran jaringan pada throughput empiris dalam konsensus PoET. Penelitian ini menyediakan dasar untuk analisis empiris dan pembangunan model relasional formal di masa depan serta memberikan pentingnya pemahaman kuantitatif terhadap interaksi parameter sistem untuk mengoptimalkan jaringan blockchain dan memfasilitasi adopsi industry [16, p. 47]. |
| Sina Kamali, Shayan Shabihi, Mohammad Taha Fakharian, Alireza Arbabi | *RPoA: Redefined Proof of Activity* | RPoA adalah protokol konsensus yang mengatasi masalah utama dari protokol sebelumnya dan cocok untuk diimplementasikan pada sistem keuangan terdesentralisasi, khususnya pada sistem berbasis kontrak pintar seperti flash loan dan sistem likuidasi. Konsep biaya transaksi layanan yang berkontribusi pada aset yang dipertaruhkan dalam jaringan secara signifikan mengurangi ketidaklikuidan jaringan dan modal yang dipertaruhkan juga dapat diproses untuk menghasilkan pendapatan [19]. |
| Shresth Agrawal, Joachim Neu, Ertem Nusret Tas, Dionysis Zindros | *Proofs of Proof-of-Stake with Sublinear Complexity* | PoS adalah protokol konsensus blockchain yang menawarkan alternatif bagi PoW dalam hal efisiensi dan ramah lingkungan. Namun, PoS juga memiliki tantangan tersendiri yang perlu diatasi dalam penggunaannya pada jaringan blockchain yang lebih besar dan kompleks [14]. |
| Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Yang Xiang | *Exploring Unfairness on Proof of Authority: Order Manipulation*  *Attacks and Remedies* | PoA memiliki kecepatan dalam hal transaksi namun PoA memiliki kelemahan dalam hal ketidakadilan, yaitu dapat dimanipulasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, para pengembang blockchain perlu mempertimbangkan risiko ini dan mengambil langkah-langkah untuk mengurangi kerentanan PoA terhadap serangan [20]. |
| *Security and Privacy* | Elli Androulaki, Christian Cachin, Christopher Ferris, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Chrysoula Stathakopoulou | *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains* | *Fabric* adalah sistem operasi terdistribusi modular dan dapat diperluas untuk menjalankan *blockchain* berizin. *Fabric* memperkenalkan arsitektur baru yang memisahkan eksekusi transaksi dari konsensus dan memungkinkan penunjukan berdasarkan kebijakan yang mirip dengan *database* tumpang tindih *middleware*. Dengan modularitasnya, Fabric sangat cocok untuk banyak peningkatan dan penelitian di masa depan seperti meningkatkan performa dengan mengeksplorasi *benchmark* dan optimisasi, skalabilitas untuk penerapan besar, menjamin konsistensi dan model data yang lebih umum, memberikan jaminan keberlanjutan lainnya melalui protokol konsensus yang berbeda, privasi dan kerahasiaan transaksi dan data ledger melalui teknik kriptografi, dan banyak lagi [2, p. 14]. |
| IoT, IIoT | Adnan Iftekhar, Xiaohui Cui, Qi Tao and Chengliang Zheng | *Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain- Based Applications* | Teknologi *blockchain Hyperledger Fabric* untuk perangkat IoT. Dengan *Hyperledger Fabric*, dibuatlah solusi kontrol akses berbasis blockchain untuk perangkat IoT. Sistem ini menggunakan *Hyperledger Fabric* untuk memisahkan antara orang dan perangkat dengan menggunakan aturan dan manajemen akses program yang dibangun ke dalam *chaincode* itu sendiri. Dalam paper ini dijelaskan implementasi solusi dan ditunjukkan performanya pada *node Raspberry Pi* 4B. Dalam paper ini juga dibahas kebijakan *fabric*, instalasi *chaincode*, memanggil *chaincode*, dan pengujian solusi [21, p. 17]. |
| *General Applications* | Ilham Wijaya, Emy Haryatmi, Ary Bima Kurniawan | Implementasi Teknologi Blockchain pada Sistem Presensi Staff VM LePKom  Berbasis Web | Penelitian ini berhasil merancang dan menguji sistem *blockchain* pada aplikasi Asisten VM LePKom dengan beberapa rancangan yang saling berkaitan. Penerapan teknologi *blockchain* pada aplikasi ini telah diuji dan memberikan kelebihan pada sisi ketersediaan dan keamanan data. Berbagai pengujian telah dilakukan, seperti uji coba memasukkan data kehadiran ke *blockchain*, pendistribusian data ke seluruh node, dan uji coba konsensus, yang memberikan hasil yang diharapkan [22, p. 168]. |
| Jaysing Bhosale, Sushil Mavale | *Volatility of select Crypto-currencies: A comparison of Bitcoin, Ethereum and*  *Litecoin* | Proyeksi nilai *Bitcoin*, *Ethereum*, dan *Litecoin* dalam lima tahun ke depan memerlukan banyak faktor yang dipertimbangkan. Berdasarkan penelitian kualitatif, regresi linier, dan analisis Monte Carlo, *Bitcoin* diperkirakan akan mengalami pertumbuhan lebih lanjut, sedangkan *Ethereum* dan *Litecoin* memiliki potensi hasil yang berbeda. *Ethereum* memiliki variasi nilai yang lebih besar, sedangkan *Litecoin* memiliki variasi nilai yang lebih kecil [9, p. 140]. |
| *Space Industry, Healt, Education* | Daniel Levis, Francesco FontanaID, Elisa Ughetto | *A look into the future of blockchain technology* | Penelitian ini dapat berguna bagi praktisi dan manajer perusahaan untuk melihat skenario masa depan yang mungkin secara lebih rasional dan sistematis. Namun demikian, penelitian ini hanya membuka jalan untuk pemahaman yang lebih baik tentang masa depan berbasis *blockchain* [23, p. 16]. |
| Nur Hazbiy Shaffan, F. Astha Ekadiyanto, Anak Agung Putri Ratna | *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*. Hasil eksperimen menunjukkan bahwa fungsi *Read* memiliki durasi yang paling singkat dibandingkan dengan fungsi *Create, Delete*, dan *Update*. Selain itu, kami menemukan bahwa penggunaan *query* pada fungsi *Read* lebih lambat dibandingkan dengan tanpa menggunakan *query*, terutama pada kategori komoditas yang lebih banyak [24, p. 151]. |
|  | Purwono, Khoirun Nisa, Sony Kartika Wibisono, Bala Putra Dewa | *Private Blockchain in the Field of Health Services* | Platform *Hyperledger* menjadi pilihan yang tepat untuk aplikasi di bidang kesehatan karena memiliki toolkit yang lengkap dan mampu mengimplementasikan standar privasi dan keamanan dengan cepat. Selain itu, *Hyperledger* juga memiliki kendali penuh terhadap *smart contract* yang dapat dieksekusi dalam beberapa bahasa pemrograman [5, p. 14]. |
| *File Systems* | Prof. Reema Roychaudhary, Mercy Gill, Aditya Chahande, Chanchal Panjabi, Usha Kakde | *Integrating Blockchain and the Interplanetary File System, a resilient platform*  *for storing students' file* | *Blockchain* dan *Interplanetary* *File System* (IPFS) untuk menyimpan data mahasiswa telah dibuat. IPFS digunakan untuk menyimpan file besar yang tidak efisien disimpan di dalam *Blockchain*. Model ini memungkinkan mahasiswa mengunggah file pdf berisi informasi pembayaran setelah login. File tersebut disimpan di IPFS dan *hash*-nya disimpan di *smart contract* di *Blockchain* [4, p. 1096]. |
|  | *Orphanage Management Using IPFS and Hyperledger Fabric* | Menggunakan IPFS dan *Hyperledger Fabric* untuk manajemen panti asuhan menyediakan sistem pencatatan data anak yatim yang aman, transparan, dan bebas dari tindakan pemalsuan. Implementasi solusi ini memastikan bahwa data anak yatim selalu aman dan dapat diakses secara *real-time* oleh pihak yang berwenang. Selain itu, penggunaan *Ethers* untuk sistem donasi memberikan transparansi dan akuntabilitas dalam penggunaan dana [11, p. 5]. |
| Mamun Ahmed, Akash Roy Pranta, Mst. Fahmida Akter Koly,  Farjana Taher, and Mohammad Asaduzzaman Khan | *Using IPFS and Hyperledger on Private Blockchain to*  *Secure the Criminal Record System* | Memanfaatkan IPFS dan *Hyperledger* membuat sistem kami lebih aman, tidak dapat diubah, dan dapat diandalkan. Karakteristik izin dan kepekaan dari *Hyperledger* memungkinkan sistem untuk berfungsi secara konsisten di semua area. Penggunaan *cryptocurrency* tidak diperbolehkan, sehingga lebih aman. Kami menggunakan IPFS untuk file media sebagai bukti kejahatan [3, p. 5]. |

# **BAB III**

# **METODOLOGI PENELITIAN**

* 1. **Analisis Kebutuhan**

Tahap Analisis Kebutuhan adalah tahap awal dalam metodologi penelitian yang bertujuan untuk memahami kebutuhan dan tujuan penelitian yang akan dilakukan. Dalam tahap ini, dilakukan analisis terhadap tiga hal penting yaitu tujuan penelitian, tujuan bisnis, dan kebutuhan teknis.

* + 1. **Tujuan Penelitian**

Tujuan utama dari penelitian ini adalah untuk mengevaluasi dan menganalisis tingkat keamanan dan integritas data intelijen militer yang disimpan dalam sebuah sistem *blockchain* berbasis *private*. Penelitian ini juga bertujuan untuk menunjukkan efektivitas penggunaan metode *Practical Byzantine Fault Tolerance* (PBFT) dan *Proof of Authority* (PoA) dalam meningkatkan keamanan dan integritas data yang disimpan dalam *blockchain* tersebut. Melalui penelitian ini, diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem *blockchain* yang lebih aman dan andal untuk menyimpan data intelijen militer yang sangat sensitif dan krusial, serta dapat memberikan wawasan baru dalam bidang keamanan siber dan teknologi *blockchain*.

* + 1. **Tujuan Bisnis**

Tujuan bisnis dari proyek ini adalah untuk menyediakan solusi *blockchain* berbasis *private* yang aman dan andal untuk penyimpanan data intelijen militer yang sangat sensitif dan penting. Dalam proyek ini, metode *Practical Byzantine Fault Tolerance* (PBFT) dan *Proof of Authority* (PoA) akan digunakan untuk menjamin keamanan dan integritas data yang disimpan di dalam sistem *blockchain* tersebut. Dengan menyediakan solusi yang aman dan andal untuk penyimpanan

data intelijen militer, diharapkan dapat membantu meningkatkan efektivitas operasi militer dan melindungi data sensitif dari ancaman siber dan peretasan. Selain itu, proyek ini juga bertujuan untuk memperkuat kemampuan teknologi *blockchain* dalam bidang keamanan dan memberikan solusi yang dapat disesuaikan dengan berbagai sektor yang memerlukan tingkat keamanan yang tinggi dalam pengolahan dan penyimpanan data. Dengan demikian, proyek ini memiliki potensi untuk menjadi solusi yang sangat diperlukan dalam mengatasi tantangan keamanan data di masa depan.

* + 1. **Kebutuhan Teknis**

Kebutuhan teknis merujuk pada persyaratan teknologi atau infrastruktur yang diperlukan untuk menjalankan suatu proyek atau penelitian. Hal ini meliputi perangkat keras, perangkat lunak, dan sumber daya manusia yang dibutuhkan untuk melaksanakan suatu tugas atau proyek.

1. **Spesifikasi Perangkat Keras Mininum**

* **Sistem Operasi *Windows***
* RAM minimal 8GB, direkomendasikan 12GB
* HDD *free space* 20GB
* SSD minimal 128GB direkomendasikan 256GB
* *Processor* minimal i3 (Intel) atau setara dengan i3
* **Sistem Operasi *Linux***
* RAM minimal 8GB
* HDD *free space* 20GB
* SSD minimal 128GB direkomendasikan 256GB
* *Processor* minimal i3 (Intel) atau setara dengan i3

1. **Spesifikasi Perangkat Keras Peneliti**

Dalam pengembangan sistem ini, peneliti menggunakan spesifikasi perangkat keras sebagai berikut:

* RAM 20GB+ (20480 MB)
* HDD 1TB
* SSD 1TB Samsung
* *Processor* i5-7200U (Intel) @ 2.50GHz (4 CPUs), ~2.7GHz
* Sistem Operasi Linux (Ubuntu 22.04)

1. **Perangkat Lunak**
   * + ***Hyperledger Fabric***

*Hyperledger Fabric* adalah salah satu contoh *blockchain* berizin yang dapat memainkan peran penting dalam mengimplementasikan sistem kesehatan yang berpusat pada pasien dan interoperabilitas. Platform teknologi *ledger* terdistribusi *open-source* ini mendukung fitur keamanan dan privasi yang kuat, serta memungkinkan peserta di konsorsium untuk mengembangkan dan mendeploy aplikasi menggunakan kontrak pintar (*chain code*). Oleh karena itu, *Hyperledger Fabric* semakin populer untuk banyak aplikasi di berbagai domain [5, p. 12].

* + - ***Hyperledger Fabric* CA**

Merupakan suatu layanan sertifikat untuk melakukan pengelolaan sertifikat digital dalam jaringan *Hyperledger Fabric*. CA (*Certificate Authority*) memungkinkan pengguna untuk melakukan pengelolaan indetitas dan otorisasi, serta menyediakan fitur keamanan seperti enkripsi dan dan autentikasi pengguna.

* + - ***Hyperledger Fabric Chaincode***

*Chaincode* adalah salah satu fitur utama dari *Hyperledger Fabric* untuk mengimplementasikan kontrak pintar. Fitur ini berisi logika dari rencana bisnis yang memelihara *ledger* di dalam sistem, mengontrol keadaan dunia (yaitu nilai saat ini dari atribut sebagai ledger yang unik) dalam basis data, dan mengikuti kebijakan *endorsement*. Dengan *Chaincode*, *Hyperledger Fabric* dapat mendukung eksekusi kontrak pintar yang aman dan andal untuk berbagai aplikasi *blockchain* [24, p. 148].

* + - ***Hyperledger Fabric Peer***

Merupakan komponen inti dari jaringan b*lockchain Hyperledger Fabric* yang berfungsi sebagai node untuk memelihara dan menjaga *ledger*, serta melakukan transaksi dan validasi di dalam jaringan. Setiap *peer* memiliki salinan lengkap dari *ledger* dan dapat melakukan operasi baca/tulis di dalamnya. *Peers* di dalam jaringan *Hyperledger Fabric* bekerja sama untuk menjaga konsistensi dan keandalan data di dalam *ledger*, serta dapat berkomunikasi dengan *peers* lainnya untuk menyepakati transaksi yang akan dimasukkan ke dalam blok.

* + - ***Hyperledger Fabric Orderer (Ordering Phase)***

Setelah seorang klien mengumpulkan cukup banyak *endorsement* pada sebuah proposal, klien akan menyusun transaksi dan mengirimkannya ke layanan pemesanan. Transaksi tersebut berisi *payload* transaksi (termasuk operasi *chaincode* beserta parameter), metadata transaksi, dan sejumlah endorsement. Tahap pemesanan akan mengatur urutan total pada semua transaksi yang dikirimkan *per channel*. Dengan kata lain, tahap pemesanan akan menyiarkan secara atomik *endorsement* dan dengan demikian membangun konsensus pada transaksi, bahkan jika terdapat *orderer* yang bermasalah. Hal ini memastikan keandalan dan keamanan sistem, sehingga *Hyperledger Fabric* dapat menjadi *platform blockchain* yang andal dan terpercaya untuk berbagai aplikasi [2, p. 6].

* + - ***Hyperledger Explorer***

*Hyperledger Explorer* adalah alat visualisasi open source untuk memonitor dan menganalisis jaringan *blockchain Hyperledger*. Alat ini menyediakan antarmuka web untuk menampilkan informasi tentang transaksi, blok, *peer*, dan *smart contract* secara terstruktur dan terorganisir. Dengan fitur pencarian, pemfilteran, dan pengurutan data, pengguna dapat dengan mudah mencari informasi dan melakukan analisis data untuk pengambilan keputusan bisnis dan pengembangan aplikasi *blockchain*.

* + - **VSCode**

VSCode merupakan teks editor yang digunakan dalam pengembangan *blockchian* untuk menulis setiap kode program dari *Hyperledger Fabric*, React, Node JS dan Express JS.

* + - **Docker**

Adalah sebuah platform *open source* yang digunakan untuk membuat, mengemas, dan menjalankan aplikasi dalam kontainer. Kontainer memungkinkan aplikasi diisolasi dari lingkungan sistem operasi host dan memungkinkan aplikasi berjalan di berbagai lingkungan tanpa perlu memikirkan perbedaan konfigurasi di lingkungan tersebut.

* + - ***Docker Dekstop***

Adalah sebuah aplikasi *dekstop* yang menyediakan sebuah lingkungan *Docker* yang mudah digunakan di sistem operasi *Windows* dan macOS. *Docker Desktop* memungkinkan pengembang untuk membuat dan menjalankan kontainer *Docker* secara lokal dengan mudah dan menawarkan integrasi dengan alat-alat pengembangan seperti VSCode.

* + - **IPFS**

Digunakan untuk menyimpan data dalam bentuk file media dengan aman dan terenkripsi. IPFS menawarkan keamanan dan transparansi dalam pertukaran data melalui jaringan, sehingga setiap file yang diunggah dan disimpan memiliki hash unik dan rekam jejak transaksi [3, p. 2].

* + - **IPFS *Dekstop***

Adalah aplikasi *desktop* yang menyediakan sebuah antarmuka untuk menggunakan protokol IPFS. IPFS sendiri adalah protokol yang digunakan untuk mendistribusikan file secara terdesentralisasi, mirip dengan teknologi *blockchain*. IPFS *Desktop* memungkinkan pengguna untuk mengunggah dan mengunduh file ke jaringan IPFS dengan mudah dan memungkinkan pengguna untuk menjelajahi file yang tersedia di jaringan IPFS.

* + - **CouchDB**

CouchDB adalah sebuah *database* NoSQL yang dapat digunakan sebagai database *backend* untuk aplikasi *blockchain*. CouchDB memiliki beberapa fitur yang berguna untuk pengembangan aplikasi *blockchain*, seperti replikasi data yang mudah, dukungan untuk indeks berbasis JSON, dan dukungan untuk ACID (*atomicity, consistency, isolation,* dan *durability) transactions*.

* + - **Postman**

Adalah sebuah alat pengujian API yang dapat digunakan untuk memvalidasi API backend untuk aplikasi *blockchain*. Postman memungkinkan pengguna untuk mengirim permintaan ke API dan menampilkan respons dari API. Dalam pengembangan aplikasi *blockchain*, Postman dapat digunakan untuk menguji berbagai fungsi *blockchain*, seperti transaksi dan kontrak pintar (*smart contract*).

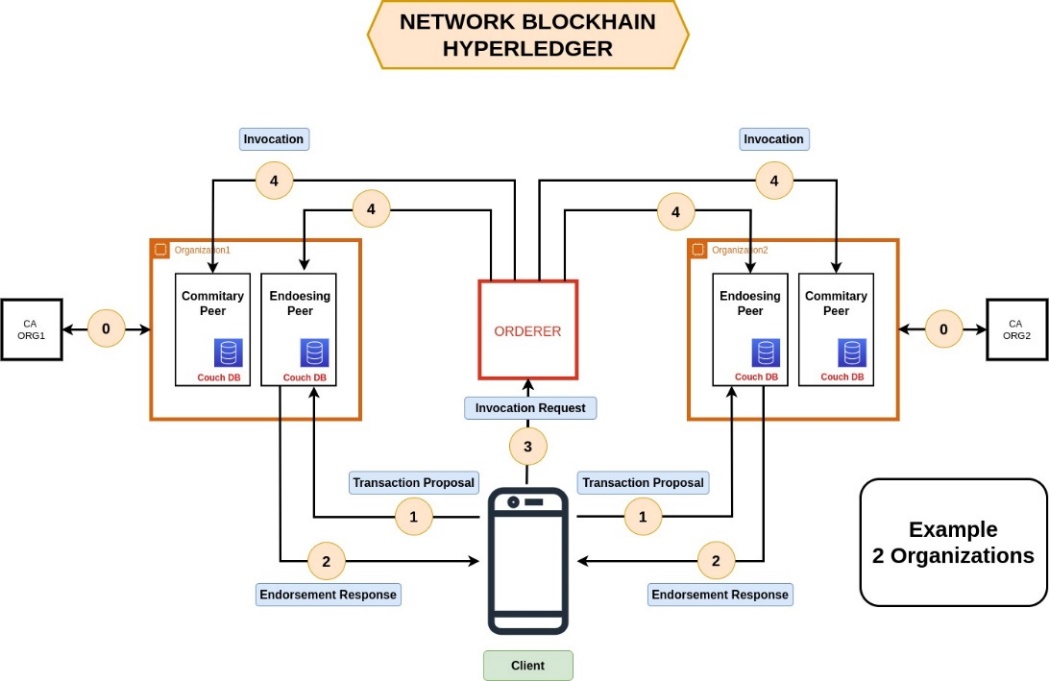
* 1. **Desain Sistem**

Desain sistem merupakan tahap awal dalam pengembangan suatu sistem yang bertujuan untuk merancang sebuah sistem yang tepat dan efektif untuk memenuhi kebutuhan dan tujuan bisnis. Tahap ini meliputi analisis kebutuhan untuk memahami masalah atau tantangan bisnis yang ingin diatasi, tujuan dari pengembangan sistem, dan sumber daya yang tersedia untuk menciptakan sistem tersebut.

* + 1. ***Network Blockchain***

*Network blockchain* merujuk pada jaringan *peer-to-peer* yang terdiri dari *node-node* komputer yang terhubung satu sama lain. Setiap *node* memiliki salinan lengkap dari seluruh data transaksi yang terjadi di jaringan. Jaringan ini memungkinkan node-node untuk bekerja sama dan memverifikasi transaksi serta menjaga keamanan data di dalam *blockchain*.

*Node-node* di dalam jaringan *blockchain* dapat bekerja sama untuk memverifikasi transaksi dan menjaga keamanan data di dalam *blockchain*. Setiap node akan memverifikasi setiap transaksi sebelum menambahkannya ke *blockchain*, dan setiap transaksi yang diterima oleh node akan dikirim ke node lain di dalam jaringan untuk diverifikasi ulang. Proses verifikasi ini membutuhkan waktu dan sumber daya komputasi yang cukup besar, namun ini adalah bagian yang sangat penting dalam menjaga keamanan jaringan *blockchain*. Karena setiap node memiliki salinan lengkap dari *blockchain*, maka jika terdapat upaya untuk memanipulasi data pada satu *node*, maka *node* lain akan segera mendeteksinya dan menolak transaksi tersebut. Dalam hal ini, jaringan *blockchain* memberikan keamanan yang lebih baik dibandingkan dengan sistem tradisional yang dapat rentan terhadap serangan dan manipulasi data.

****

*Gambar 3.1 Network Blockchain*

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*. CA berperan sebagai otoritas yang menjamin keamanan identitas dan transaksi di dalam jaringan.
2. ***Transaction* Proposal**

*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. *Endorsers* memverifikasi dan mengeksekusi transaksi, kemudian mengembalikan hasil dan tanda tangan digital mereka ke klien untuk diproses dan ditambahkan ke dalam *ledger* oleh *orderer*.

1. ***Endorsment Response***

*Endorsement Response* adalah respon dari *endorsers* setelah memverifikasi dan mengeksekusi permintaan transaksi dalam jaringan *Hyperledger Fabric*. Respons ini berisi hasil eksekusi fungsi *Chaincode* dan tanda tangan digital *endorsers* yang menjamin keaslian dan validitas transaksi. *Endorsement Response* adalah bagian kritis dari mekanisme konsensus di dalam jaringan, yang memastikan keamanan dan kevalidan transaksi. Setelah menerima respons, klien memeriksa tanda tangan digital dan melanjutkan proses pengiriman transaksi ke *orderer* untuk diproses dan ditambahkan ke *ledger*.

1. ***Invocation Request***

*Invocation Request* adalah permintaan klien kepada *endorsers* untuk menjalankan fungsi *Chaincode* pada jaringan *Hyperledger Fabric*. *Endorsers* akan memverifikasi dan menjalankan fungsi *Chaincode*, kemudian mengembalikan hasil eksekusi dan tanda tangan digital. Setelah itu, klien dapat mengirimkan hasil transaksi ke *orderer* untuk diproses dan ditambahkan ke dalam *ledger*.

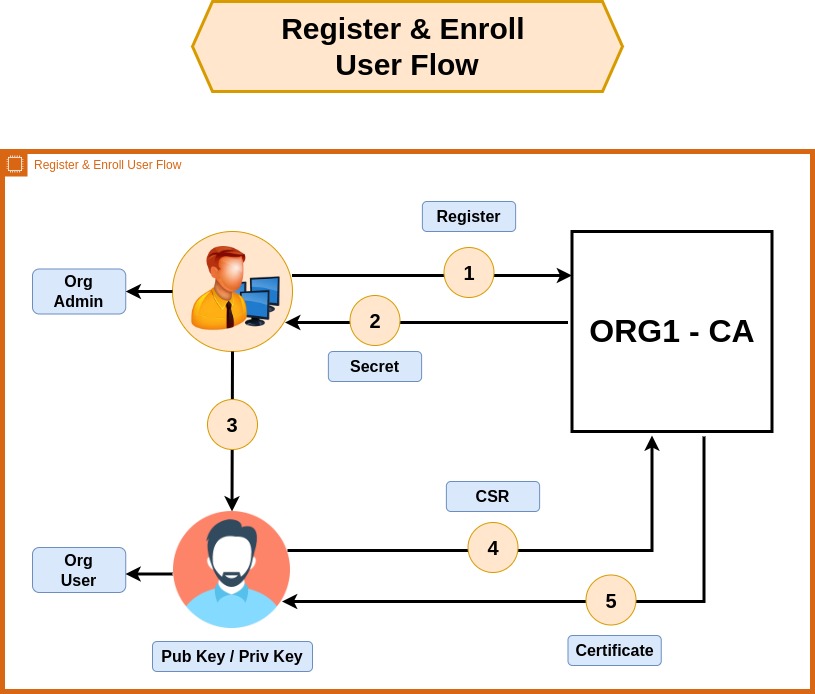
1. ***Invocation***

*Invocation* atau pemanggilan adalah proses di mana klien mengirim permintaan untuk menjalankan fungsi *Chaincode* pada jaringan *Hyperledger Fabric*. Permintaan ini akan diterima dan diproses oleh *endorsers*, yang bertugas untuk memverifikasi keaslian dan integritas permintaan transaksi, serta mengeksekusi fungsi *Chaincode* yang diminta. Setelah itu, hasil eksekusi dan tanda tangan digital *endorsers* dikirimkan kembali ke klien untuk diproses dan ditambahkan ke dalam *ledger*. Proses pemanggilan ini merupakan bagian penting dari mekanisme konsensus pada jaringan *Hyperledger Fabric* untuk memastikan keamanan dan kevalidan transaksi di dalam jaringan.

* + 1. ***User Flow***

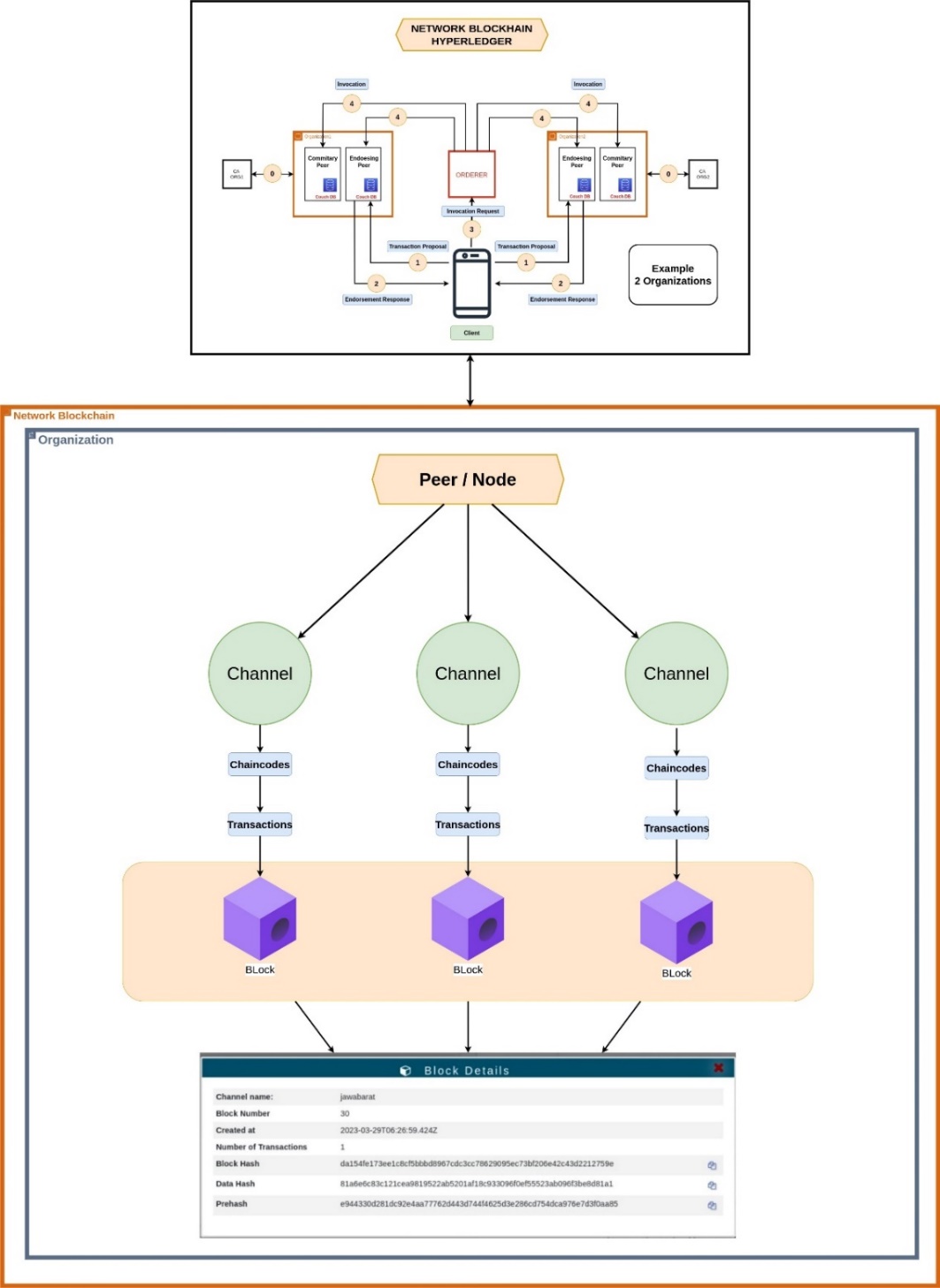
*User flow* pada *blockchain* mencakup serangkaian langkah yang diambil oleh pengguna saat menggunakan aplikasi atau platform *blockchain*. Langkah-langkah ini dapat berbeda-beda tergantung pada aplikasi atau platform yang digunakan, tetapi pada umumnya mencakup beberapa tahap sebagai berikut:

1. Registrasi: Pengguna mendaftar pada aplikasi atau platform *blockchain* dengan mengisi formulir pendaftaran dan memberikan informasi yang diperlukan, seperti nama, alamat email, dan kata sandi.
2. Membuat akun: Setelah pendaftaran, pengguna membuat akun di aplikasi atau platform blockchain dan mengatur profil pengguna dengan informasi yang relevan, seperti alamat dompet atau informasi identitas.
3. Verifikasi identitas: Pada beberapa platform *blockchain*, pengguna harus melewati proses verifikasi identitas sebelum dapat menggunakan platform sepenuhnya. Ini dilakukan untuk memastikan keamanan dan kepatuhan pada peraturan yang berlaku.
4. Melakukan transaksi: Pengguna dapat melakukan transaksi seperti mengirim atau menerima kripto aset, melakukan perdagangan, atau mengakses layanan *blockchain* lainnya.
5. Memantau transaksi: Setelah transaksi dilakukan, pengguna dapat memantau status transaksi dan melihat histori transaksi mereka di dalam aplikasi atau platform *blockchain*.



*Gambar 3.2 User Flow*

* + 1. ***Organization***

****

*Gambar 3.3 Arsitektur Organisasi*

*Organization* pada *blockchain* merujuk pada struktur organisasi dari jaringan *blockchain* yang dapat berupa organisasi terpusat atau terdesentralisasi.

* ***Node***

Node adalah entitas dalam jaringan *blockchain* yang menyimpan salinan lengkap dari seluruh data transaksi yang terjadi di jaringan. Setiap *node* juga berfungsi untuk memverifikasi transaksi dan menambahkannya ke dalam *blockchain*.

* ***Channel***

*Channel* adalah konsep dalam *blockchain* yang memungkinkan beberapa pihak untuk berinteraksi dan melakukan transaksi secara terpisah di dalam jaringan *blockchain* yang sama. Dengan adanya *channel*, setiap pihak hanya dapat melihat transaksi yang terjadi di dalam *channel* yang sama dengan mereka, sehingga privasi dan keamanan transaksi dapat terjaga.

* ***Chaincodes***

*Chaincode* adalah program yang digunakan dalam *blockchain* untuk menentukan aturan dan logika transaksi yang dilakukan di dalam jaringan. *Chaincode* ditulis dalam bahasa pemrograman tertentu dan dieksekusi pada setiap node di dalam jaringan *blockchain*.

* ***Transactions***

Transaksi adalah unit dasar dari data di dalam *blockchain* yang mencatat perubahan kepemilikan aset atau informasi lain di dalam jaringan. Setiap transaksi harus diverifikasi dan disetujui oleh seluruh *node* di dalam jaringan sebelum dapat ditambahkan ke dalam *blockchain*.

* ***Block***

*Block* adalah kumpulan dari beberapa transaksi yang terjadi di dalam jaringan *blockchain* yang telah diverifikasi dan disetujui oleh seluruh node. Setiap *block* dienkripsi dan dihubungkan dengan *block* sebelumnya untuk membentuk rangkaian data yang tak terputus, yang dikenal sebagai *blockchain*.

* ***Block Detail***

*Block Detail* merujuk pada informasi yang terkandung dalam satu *block* di dalam jaringan *blockchain*. Informasi ini mencakup hash dari *block* sebelumnya, hash dari semua transaksi yang terjadi di dalam *block*, waktu pembuatan *block*, dan informasi lain yang berguna untuk memverifikasi keaslian dan integritas data di dalam *blockchain*.

* 1. **Pengembangan**

Pada tahap pengembangan *blockchain*, berikut beberapa penjelasannya:

* + 1. ***Private Blockchain***

*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.
   1. **Implementasi**

Pada tahapan implementasi *blockchain* pada sistem intelijen militer menggunakan *private blockchain.* *Private blockchain* menjadi pilihan yang tepat karena hanya dapat diakses oleh pihak-pihak yang memiliki izin akses sehingga dapat memastikan bahwa data-data yang terdapat di dalamnya tidak mudah diakses oleh pihak yang tidak berwenang.

* + 1. **Organisasi**

Implementasi *blockchain* menggunakan 3 Organisasi didalamnya dimana organisasi intelijen militer yang bertanggung jawab untuk mengumpulkan, menganalisis, dan menyediakan informasi intelijen untuk kepentingan pertahanan dan keamanan negara. Berikut adalah tiga organisasi intelijen militer di Indonesia:

1. **Badan Intelijen Negara (BIN)**

BIN adalah lembaga intelijen yang bertanggung jawab langsung kepada Presiden RI. Tugas utama BIN adalah mengumpulkan, menganalisis, dan menyediakan informasi intelijen yang berkaitan dengan keamanan dan ketertiban nasional. BIN juga bertanggung jawab untuk melindungi kepentingan nasional dari ancaman dan gangguan dalam negeri dan luar negeri.

1. **Dewan Intelijen Nasional (DIN)**

DIN adalah lembaga intelijen yang dibentuk oleh Kepala Staf TNI untuk memfasilitasi koordinasi antara intelijen TNI dengan intelijen kepolisian dan intelijen sipil. DIN bertanggung jawab untuk mengumpulkan, menganalisis, dan menyediakan informasi intelijen yang dibutuhkan oleh TNI untuk menjalankan tugas-tugasnya dalam menjaga keamanan dan ketertiban nasional.

1. **Badan Intelijen Strategis (BAIS)**

BAIS adalah lembaga intelijen militer yang bertanggung jawab untuk mengumpulkan, menganalisis, dan menyediakan informasi intelijen strategis bagi TNI dan pemerintah. Tugas utama BAIS adalah memberikan informasi yang dibutuhkan untuk mengembangkan strategi pertahanan dan keamanan nasional serta membantu dalam pengambilan keputusan strategis pemerintah.

Ketiga organisasi intelijen militer di Indonesia tersebut memiliki peran yang sangat penting dalam menjaga keamanan dan ketertiban nasional, serta melindungi kepentingan negara dari berbagai ancaman dalam dan luar negeri.

* + 1. ***Data Field***

1. **Lokasi musuh:** Informasi tentang lokasi musuh sangat penting untuk intelijen militer, karena dapat membantu dalam perencanaan strategi dan taktik militer. Informasi tentang lokasi musuh dapat mencakup posisi militer, posisi senjata, pangkalan udara, pelabuhan, jalan raya, dan infrastruktur lainnya yang digunakan oleh musuh. Informasi ini harus dijaga kerahasiaannya agar musuh tidak dapat mengambil tindakan untuk menghindari serangan atau melawan serangan.
2. **Kekuatan musuh**: Informasi tentang kekuatan musuh dapat meliputi jumlah personil militer, jenis senjata yang dimiliki, kekuatan udara dan laut, dan sumber daya lain yang dimiliki musuh. Informasi ini sangat penting untuk perencanaan strategi dan taktik militer, serta untuk mengevaluasi kemampuan musuh untuk melawan serangan. Informasi ini harus dijaga kerahasiaannya agar musuh tidak dapat mengetahui kelemahan dan kekuatan dari pasukan militer kita.
3. **Rencana musuh**: Informasi tentang rencana musuh dapat mencakup rencana operasi militer, taktik, dan strategi yang akan digunakan oleh musuh. Informasi ini sangat penting untuk perencanaan dan persiapan pasukan militer kita dalam menghadapi musuh. Informasi ini harus dijaga kerahasiaannya agar musuh tidak dapat mengambil tindakan untuk menghindari serangan atau melawan serangan.
4. **Teknologi musuh**: Informasi tentang teknologi musuh dapat mencakup jenis senjata, sistem pertahanan, dan teknologi militer lainnya yang dimiliki oleh musuh. Informasi ini sangat penting untuk memahami kemampuan dan kelemahan musuh, dan untuk mengembangkan strategi dan taktik militer yang efektif. Informasi ini harus dijaga kerahasiaannya agar musuh tidak dapat mengetahui teknologi yang kita miliki dan mengembangkan strategi untuk mengalahkan kita.
5. **Identitas sumber intelijen:** Identitas sumber intelijen harus dijaga kerahasiaannya agar tidak membahayakan keselamatan dan keamanan mereka. Identitas ini harus dijaga kerahasiaannya agar musuh tidak dapat mengetahui siapa yang memberikan informasi kepada intelijen militer.
6. **Rencana operasi militer:** Rencana operasi militer mencakup perencanaan dan persiapan untuk melakukan serangan atau pertahanan militer. Informasi ini harus dijaga kerahasiaannya agar musuh tidak dapat mengambil tindakan untuk menghindari serangan atau melawan serangan.
7. **Informasi tentang perlengkapan dan logistik:** Informasi mengenai perlengkapan dan logistik musuh sangat penting untuk disimpan dalam data intelijen militer karena dapat membantu dalam mengambil keputusan yang tepat dalam merencanakan serangan atau strategi militer. Informasi ini meliputi jenis senjata dan peralatan yang dimiliki oleh musuh, jumlah pasukan dan kendaraan, serta rincian logistik seperti stok makanan, amunisi, dan bahan bakar.
8. **Informasi tentang kegiatan diplomatik:** Informasi tentang kegiatan diplomatik musuh dapat membantu dalam memahami hubungan politik dan diplomasi antara negara dan dapat memberikan wawasan tentang rencana dan strategi yang dilakukan oleh musuh. Informasi ini dapat mencakup pertemuan diplomatik, perjanjian internasional, dan kunjungan resmi oleh pejabat pemerintah.
9. **Informasi tentang sasaran strategis:** Informasi tentang sasaran strategis musuh mencakup informasi tentang target yang mungkin diincar oleh musuh seperti fasilitas militer, infrastruktur penting, dan pusat pemerintahan. Informasi ini dapat membantu dalam merencanakan strategi pertahanan atau serangan untuk melindungi sasaran penting dari serangan musuh.
10. **DataHash:** Ini menyimpan informasi mengenai Hash dari IPFS dimana hasil hash yang digenerate dari IPFS akan disimpan pada kolom ini, jadi secara umum blockchain tidak langsung menyimpan dokumen kedalam blockchain melainkan melakukan penyimpanan Hash dari hasil generate IPFS.
    * 1. ***Hyperledger Explorer***

*Hyperledger Explorer* adalah aplikasi *open-source* yang sangat berguna untuk memantau, menganalisis, dan memvisualisasikan data pada jaringan *blockchain* yang menggunakan *framework Hyperledger Fabric*, terutama pada konteks intelijen militer. Penggunaannya pada *blockchain* intelijen militer akan memudahkan pengelolaan dan pemantauan data-data intelijen yang tersimpan di dalam *blockchain* tersebut, sehingga informasi yang relevan dan akurat dapat diperoleh dengan lebih mudah dan cepat.

Untuk mengimplementasikan *Hyperledger Explorer* pada *blockchain* intelijen militer, perlu dilakukan persiapan pada jaringan *Hyperledger Fabric*, seperti konfigurasi dan instalasi *peer, orderer*, serta *channel* pada jaringan *blockchain*. Selain itu, diperlukan juga konfigurasi pada *Hyperledger Explorer* agar dapat terhubung dengan jaringan *blockchain* yang telah disiapkan. Setelah semua persiapan selesai, maka *Hyperledger Explorer* dapat digunakan untuk memantau dan menganalisis data intelijen yang tersimpan di dalam *blockchain* intelijen militer dengan lebih mudah dan efektif.

* + 1. **IPFS**

*InterPlanetary File System* (IPFS) adalah sistem distribusi file *peer-to-peer* yang digunakan untuk menyimpan dan mengambil file dengan aman, terdesentralisasi, dan dapat diakses secara global. Implementasi IPFS pada *blockchain* intelijen militer dapat membantu untuk meningkatkan keamanan dan integritas data pada jaringan *blockchain*. Hal ini dapat dilakukan dengan cara menyimpan data-data intelijen pada jaringan IPFS dan menyimpan hash dari data tersebut di dalam *blockchain* intelijen militer. Dengan demikian, data dapat diamankan dengan baik karena file aslinya disimpan terdesentralisasi pada jaringan IPFS, sedangkan hash-nya yang dijamin keasliannya disimpan pada *blockchain*.

Implementasi IPFS pada *blockchain* intelijen militer dapat memberikan beberapa keuntungan, seperti mengurangi risiko kehilangan data dan memungkinkan data dapat diakses dengan lebih cepat dan efisien. Selain itu, IPFS juga memungkinkan pengguna untuk membuat versi terenkripsi dari data, yang dapat memberikan perlindungan ekstra terhadap akses yang tidak sah. Dengan demikian, IPFS dapat menjadi solusi yang tepat untuk menyimpan data-data intelijen yang sangat sensitif pada jaringan *blockchain* intelijen militer, sehingga dapat meningkatkan keamanan dan integritas data pada sistem tersebut.

* + 1. **CouchDB**

Penggunaan CouchDB pada jaringan *blockchain* intelijen militer *Hyperledger Fabric* sangat penting karena dapat meningkatkan keamanan dan kinerja sistem secara signifikan. Dalam *Hyperledger Fabric*, CouchDB digunakan sebagai *database stateful* yang dapat menyimpan data transaksi dan status dari *ledger*. Dengan memanfaatkan kemampuan CouchDB sebagai *database*, data dapat disimpan secara terdistribusi pada beberapa node yang ada pada jaringan, meningkatkan keamanan dan integritas data secara signifikan. Selain itu, CouchDB pada *Hyperledger Fabric* juga memungkinkan pengguna untuk melakukan sinkronisasi data antar node dengan mudah dan mempercepat proses *indexing* dan *querying* data, sehingga peningkatan kinerja dapat dicapai secara efektif.

# **BAB IV**

# **PENUTUP**

* 1. **Kesimpulan**

Penelitian ini membahas tentang pemanfaatan teknologi *blockchain* untuk meningkatkan keamanan dan integritas data intelijen militer dengan menerapkan metode PBFT dan PoA pada *private blockchain*. Selain itu, IPFS juga diimplementasikan sebagai sistem penyimpanan data terdistribusi, dan *Hyperledger Explorer* digunakan untuk memudahkan pengelolaan dan pemantauan jaringan *blockchain* intelijen militer. Dengan teknologi *blockchain*, metode PBFT dan PoA, serta dukungan dari IPFS *dan Hyperledger Explorer*, diharapkan data intelijen militer dapat dijaga kerahasiannya, integritasnya terjaga, dan risiko serangan dari pihak tidak berwenang dapat diminimalisasi.

Namun, perlu diingat bahwa terdapat batasan penggunaan algoritma PoA, dan contoh penggunaan PBFT hanya diberikan pada skala kecil menggunakan tiga organisasi dalam satu komputer dengan menggunakan *docker container*. Oleh karena itu, penelitian selanjutnya sebaiknya mempertimbangkan pengujian sistem dalam skala yang lebih besar dengan melibatkan lebih banyak organisasi untuk memastikan efektivitas sistem.

* 1. **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*. Selain itu, penelitian selanjutnya dapat mencoba menggunakan algoritma konsensus lainnya dan menguji performa sistem pada skala yang lebih besar dengan melibatkan lebih banyak organisasi.

# **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] 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.

[4] 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.

[5] 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.

[6] “Distributed Ledger Technology: beyond block chain”.

[7] 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.

[8] D. G. Wood, “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER”.

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

[10] 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.

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

[12] Q. Wang, R. Li, Q. Wang, S. Chen, and Y. Xiang, “Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies.” arXiv, May 01, 2022. Accessed: Apr. 18, 2023. [Online]. Available: http://arxiv.org/abs/2203.03008

[13] “Porat et al. - Blockchain Consensus An analysis of Proof-of-Work.pdf.”

[14] S. Agrawal, J. Neu, E. N. Tas, and D. Zindros, “Proofs of Proof-of-Stake with Sublinear Complexity.” arXiv, Mar. 06, 2023. Accessed: Apr. 19, 2023. [Online]. Available: http://arxiv.org/abs/2209.08673

[15] S. Kamali *et al.*, “RPoA: Redefined Proof of Activity.” arXiv, Nov. 29, 2022. Accessed: Apr. 19, 2023. [Online]. Available: http://arxiv.org/abs/2210.08923

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

[17] 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.

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

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

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

[21] 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.

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

[23] 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.

[24] “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.