Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.20241116676
Vol. 11, No. 1, Februari 2024, hlm. 27-36 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

CFPCHAIN: OPTIMALISASI SISTEM SELEKSI PENDANAAN RISET BRIN MENGGUNAKAN PENDEKATAN BERBASIS KONSORSIUM *BLOCKCHAIN*

Taufik Iqbal Ramdhani[*1], Ninon Nurul Faiza[2], Marini Wulandari[3], Dian Nastiti[4], Hartanto Kurniawan[5]

[1,2,3,4,5]National Research and Innovation Agency, Bandung, Indonesia
[2,3,4]Bandung Technology University, Bandung, Indonesia
[5]Keimyung University, South Korea
Email: [1]tauf022@brin.go.id, [2]ninon.nurulfaiza@students.itb.ac.id, [3]marini.wulandari@brin.go.id, [4]arti.dian.nastiti@brin.go.id, [5]hartanto.kurniawan@brin.go.id
[*]Corresponding Author

(Naskah masuk: 9 November 2022, diterima untuk diterbitkan: 7 Agustus 2023)

Abstrak

Badan Riset dan Inovasi Nasional, Indonesia, menyediakan sistem seleksi pendanaan riset. Penelitian ini bertujuan untuk melakukan optimalisasi sistem seleksi pendanaan riset yang menggunakan teknologi blockchain untuk meningkatkan keamanan dan interoperabilitas sistem seleksi pendanaan penelitian. Saat ini, sistem pendanaan penelitian yang menggunakan sistem terpusat memiliki kekurangan dalam hal keamanan dan interoperabilitas. Masalah utama yang dihadapi sistem saat ini adalah modifikasi data, akuntabilitas transparan, dan kurangnya interoperabilitas. Pendekatan *blockchain* dapat memecahkan masalah ini dengan menyediakan keamanan tinggi, kemampuan audit, dan integritas data. Penelitian ini menggunakan *Hyperledger Fabric* (HLF) sebagai platform blockchain karena efisiensi tinggi dan kemampuan keamanannya. Arsitektur sistem pendanaan penelitian menggunakan skenario bisnis, koleksi buku besar, dan kebijakan jaringan. Implementasi sistem ini dilakukan dengan memanfaatkan fitur-fitur *blockchain* seperti imutabilitas, auditabilitas, dan interoperabilitas. Hasil penelitian menunjukkan bahwa penggunaan *blockchain* dalam sistem pendanaan penelitian dapat meningkatkan integritas data, memungkinkan audit yang jelas, dan memfasilitasi pertukaran data antar sistem. Penelitian ini memberikan kontribusi ilmiah dalam menyediakan arsitektur sistem yang aman, akuntabel, dan interoperabel untuk pendanaan riset dengan hasil peningkatan kemampuan keamanan dengan pengurangan kinerja secara minimal. Penelitian selanjutnya dapat fokus pada keamanan dokumen dan kerahasiaan dalam sistem *blockchain*.

Kata kunci: *consortium blockchain, smart contract, Hyperledger fabric*

CFPCHAIN: ENHANCING THE EFFICIENCY OF RESEARCH FUNDING SELECTION SYSTEM THROUGH THE IMPLEMENTATION OF A CONSORTIUM BLOCKCHAIN

Abstract

The National Research and Innovation Agency, Indonesia, provides a research funding selection system. This research aims to optimize the research funding selection system using blockchain technology to improve the security and interoperability of the research funding selection system. Currently, research funding systems that use a centralized system have deficiencies in terms of security and interoperability. The main problems facing the current system are data modification, transparent accountability and lack of interoperability. The blockchain approach can solve this problem by providing high security, auditability and data integrity. This research uses Hyperledger Fabric (HLF) as a blockchain platform because of its high efficiency and security capabilities. The research funding system architecture uses business scenarios, ledger collections, and network policies. Implementation of this system is carried out by utilizing blockchain features such as immutability, auditability, and interoperability. The research results show that the use of blockchain in research funding systems can improve data integrity, enable clear audits, and facilitate data exchange between systems. This research makes a scientific contribution in providing a secure, accountable and interoperable system architecture for research funding with the result of increasing security capabilities with minimal performance reduction. Future research can focus on document security and confidentiality in blockchain systems.
Keywords: *consortium blockchain, smart contract, Hyperledger fabric*

1. PENDAHULUAN

Sistem seleksi pendanaan penelitian merupakan wadah bagi peneliti untuk mengajukan permohonan dana penelitiannya. Melalui Badan Riset dan Inovasi Nasional (BRIN), Indonesia memberikan dana bagi para peneliti dengan istilah *call for proposal*. Sebagai pengelolaan dana penelitian dengan berbagai skema pendanaan, maka diperlukan suatu sistem yang aman baik dari serangan dari luar maupun dari pengguna internal. Saat ini, sistem pendanaan penelitian yang dibangun menggunakan sistem terpusat memiliki kekurangan, yaitu tertutup dan terpisah. Tertutup artinya sistem tidak dibuka secara umum, memungkinkan admin untuk mengubah data tanpa diawasi oleh pihak lain (Khan, Chrysostomou, & Nazir, 2020), sehingga memungkinkan untuk pengubahan data secara rahasia. Selanjutnya yaitu terpisah, yang berarti data yang disimpan tidak memiliki format yang seragam untuk interoperabilitas yang mudah.

Masalah utama yang muncul dari skema sistem saat ini adalah: 1) modifikasi data (Li dkk, 2018): Proposal yang telah dinilai oleh reviewer sesuai dengan jenis keahliannya menentukan persetujuan proposal. Selain itu, penilaian pendanaan dilakukan verifikasi oleh verifikator keuangan agar dana penelitian sesuai dengan komponen yang diusulkan. Kedua hal ini membutuhkan integritas data yang tinggi. Hal ini untuk memastikan bahwa pihak tidak berwenang tidak dapat mengubah data. 2) akuntabilitas transparan (Graf, Küsters, & Rausch, 2020): sistem tertutup membutuhkan metode yang memastikan setiap tindakan yang dilakukan pada sistem dicatat dan dapat dibuktikan valid. Dengan demikian, data tersebut dapat digunakan untuk referensi lembaga audit keuangan pemerintah. 3) kurangnya interoperabilitas (Kumar, & Chand, 2021): data yang dihasilkan oleh sistem ini digunakan oleh sistem lain, seperti sistem pendanaan Lembaga Pengelola Dana Pendidikan, yang mendukung skema pendanaan tertentu, sistem kepegawaian internal BRIN, dan tidak menutup kemungkinan berkomunikasi dengan sistem lainnya.

Pendekatan *blockchain* dapat memecahkan masalah ini. *Blockchain* yang merupakan dasar dari teknologi *Bitcoin*, memiliki keamanan yang tinggi dan memiliki sifat auditabilitas (Ahmad dkk, 2021), pelacakan (Mitani, & Otsuka, 2020), dan integritas (Tarkhanov, Fomin-Nilov, & Fomin, 2019). Auditabilitas properti memiliki kemampuan untuk menyimpan data pada setiap transaksi yang dilakukan sehingga setiap transaksi yang dilakukan dapat dengan mudah diverifikasi (Monrat, Schelén, & Andersson, 2019). Integritas properti menjamin keaslian dan konsistensi data dari waktu ke waktu (Xu dkk, 2019). *Blockchain* adalah basis data terdistribusi yang memanfaatkan blok yang saling berhubungan menerapkan ilmu kriptografi. Setiap blok data membawa nilai *hash* blok sebelumnya yang membentuk skema rantai, membuat data yang disimpan di setiap blok memiliki integritas yang tinggi karena mengubah satu blok data memerlukan perubahan blok berikutnya. Oleh karena itu, setiap transaksi dapat dipertanggungjawabkan. Penerapan skema keamanan ini memastikan integritas, kemampuan audit, dan ketertelusuran data.

Penelitian ini menambahkan skema arsitektur keamanan ke sistem seleksi pendanaan riset menggunakan *blockchain* yang diizinkan. *Hyperledger Fabric* (*HLF*) dipilih dalam penelitian ini karena penerapan *crash-fault-tolerance* (*CFT*) sebagai metode konsensus yang memiliki efisiensi tinggi (Huang, Ma, & Zhang, 2019). Selain itu, *HLF* menyediakan opsi mode *channel* untuk menyediakan komunikasi privat antar anggota, memastikan kerahasiaan pertukaran data (Bettayeb, Nasir, & Talib, 2021). Selain itu, HLF berjalan melalui arsitektur kontainer yang mengisolasi setiap lapisan aplikasi untuk mekanisme keamanan yang lebih baik.

Tujuan utama dari penelitian ini adalah membangun platform pendanaan riset yang memanfaatkan teknologi *blockchain* konsorsium yang memungkinkan peneliti dari lembaga publik, universitas, dan perusahaan untuk berkolaborasi dengan pendanaan yang disediakan oleh organisasi keuangan. Sedangkan kontribusi ilmiah untuk penelitian ini adalah untuk menyediakan arsitektur sistem yang *tamper-proof*, akuntabel, dan *interoperable* untuk pendanaan riset, *sponsorship*, penilaian, dan kolaborasi penelitian yang bermanfaat bagi peneliti, reviewer, auditor, penyandang dana, dan perusahaan.

Penelitian ini disusun dengan sistematika penulisan sebagai berikut. Pada bagian 1 menjelaskan mengenai latar belakang penelitian. Pada bagian 2 mencakup penelitian terkait mengenai penerapan teknologi blockchain di beberapa bidang. Bagian 3 menyajikan pemilihan tinjauan teknologi untuk penelitian ini. Pada bagian 4 terdiri dari desain arsitektur sistem pendanaan penelitian nasional. Bagian 5 meliputi implementasi desain sistem. Terakhir pada bagian 6 meliputi kesimpulan dan pembahasan penelitian.

2. PENELITIAN TERKAIT

Sistem seleksi pendanaan riset saat ini memerlukan keamanan tambahan untuk melindungi data yang tersimpan. *Blockchain* adalah salah satu teknologi yang memungkinkan keamanan tambahan pada data. Bagian ini akan menjelaskan penggunaan teknologi *blockchain* di berbagai sistem yang memecahkan masalah keamanan data dan interoperabilitas.

E-Government merupakan efek transformasi digital terhadap pelayanan publik dan perkembangan pelayanan publik yang memanfaatkan teknologi informasi. Perubahan tersebut mendorong layanan publik untuk meningkatkan kualitas pelayanannya

dengan mengadopsi teknologi baru. *Blockchain* merupakan salah satu teknologi yang bisa menjadi terobosan untuk pelayanan publik yang lebih baik (Singh, Hosen, & Yoon, 2021). Beberapa negara telah mengimplementasikan teknologi *blockchain* di lingkungan pemerintahan, seperti Estonia (Martinson, 2019), Uni Emirat Arab (Petratos, Ljepava, & Salman, 2020), China (Hou, 2017), dan Korea Selatan (Wang, & Yang, 2021). Penerapan *blockchain* di tingkat pemerintah didasarkan pada peningkatan kualitas layanan publik, peningkatan keterbukaan layanan, dan memfasilitasi pertukaran informasi antar organisasi (Hou, 2017). Di sisi keamanan informasi, teknologi *blockchain* dapat mengurangi modifikasi data, memberikan akuntabilitas, dan memfasilitasi interoperabilitas data.

Modifikasi data oleh pihak yang tidak berwenang dan tidak sesuai prosedur merupakan salah satu permasalahan dalam keamanan data. Zhou dkk. (2021) membangun *ArchivesChain*, yang memanfaatkan teknologi *blockchain* untuk melindungi arsip elektronik dari gangguan berbahaya Jing, Liu, dan Sugumaran (2021) memprakarsai sistem manajemen hak cipta kode berdasarkan *blockchain* yang melindungi kode yang diunggah. Hassija dkk. (2021) menerapkan sistem *blockchain* untuk pemilihan tender pemerintah yang dapat mengurangi korupsi dalam proses pemilihan tender dengan memberikan imutabilitas dalam data transaksi. Hang, Ullah, dan Kim (2020) mengusulkan penelitian di sektor pertanian untuk mengamankan platform peternakan ikan yang memanfaatkan teknologi *blockchain* dengan memastikan integritas data.

Akuntabilitas data adalah komponen keamanan penting dalam audit dan penelusuran transaksi, atau proses perubahan data. Penelitian yang dilakukan oleh Pu dan Lam (2021) mengadopsi teknologi blockchain di industri maritim, termasuk ketertelusuran untuk melacak dan melacak pergerakan kargo logistik. Pawlak dan Maranda (2021) menerapkan teknologi blockchain dalam sistem pemungutan suara, yang memberikan kemampuan audit sambil menjaga anonimitas pemilih. Dengan fitur imutabilitas yang disediakan oleh blockchain, log memastikan validitas setiap transaksi.

Interoperabilitas data berarti kemampuan untuk berbagi, menggunakan, dan menafsirkan data dalam sistem heterogon (Ali, & Chong, 2019). Imanto dan Yazid (2021) meneliti pelacakan rantai pasokan makanan halal berbasis teknologi *blockchain* dengan memanfaatkan interoperabilitas antara beberapa sistem *blockchain*. Penelitian Rashideh (2020) memungkinkan teknologi *blockchain* di sektor pariwisata dengan menyediakan sistem konsorsium *blockchain* untuk berkomunikasi antara mitra yang saling terhubung. Antal, Cioara, Antal, dan Anghel (2021) membuat *platform* yang memanfaatkan teknologi *blockchain* untuk mengelola penyediaan vaksin yang memungkinkan rantai distribusi antara produsen vaksin dan pusat kesehatan. Pajooh dkk. (2021) meneliti *edge-computing* untuk meningkatkan keamanan *blockchain* pada perangkat *IoT* yang saling berhubungan.

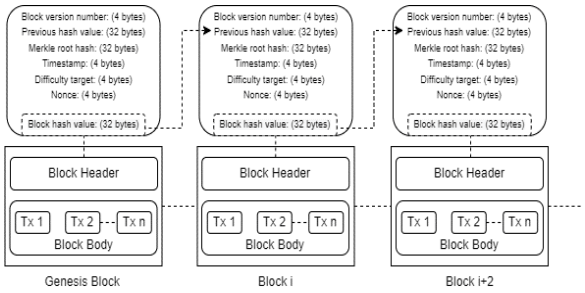
3. TINJAUAN TEKNOLOGI

Pada bagian ini menjelaskan mengenai teknologi yang digunakan pada penelitian ini. Terdapat dua teknologi utama yang digunakan pada penelitian ini yaitu teknologi *blockchain* dan juga *Hyperledger Fabric*. Tinjauan diawali mengenai penjelasan singkat mengenai teknologi *blockhain*. Selanjutnya penjelasan mengenai *Hyperledger Fabric* sebagai teknologi konsorsium *blockchain* yang digunakan pada penelitian ini.

3.1 Blockchain Technology

3.1.1 Ikhtisar

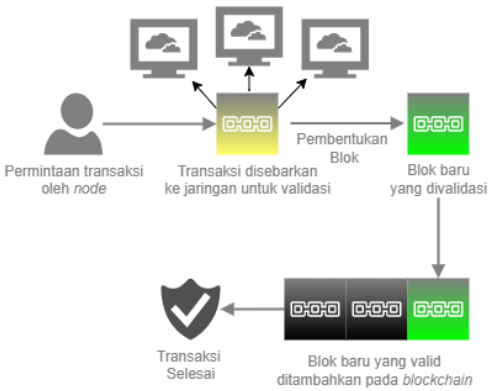
Teknologi *blockchain* menggunakan basis data, di mana data direpresentasikan dalam satu blok (Li, Deng, Cai, & Souri, 2022). Suatu blok dibentuk seperti rantai dengan memanfaatkan teknik kriptografi agar informasi blok tertentu dibentuk berdasarkan informasi blok sebelumnya, membuat *blockchain* tidak dapat diubah (Loy, Lim, How, & Yoo, 2021). Karena blok tidak dapat diubah, blok juga direpresentasikan sebagai buku besar. Buku besar terdistribusi adalah istilah *blockchain* di mana semua *node* memiliki salinan buku besar yang tepat. Pada setiap blok terdiri dari *header* dan *body* (Rajasekaran, Azees, & Al-Turjman, 2022) yang digambarkan pada Gambar 1. *Header* blok berisi informasi seperti nomor versi blok, nilai *hash* dari blok sebelumnya, nilai *hash* dari *Merkle root*, *timestamp*, kesulitan blok, blok *nonce*, dan nilai *hash* blok (Rajasekaran dkk, 2022). Sebagai perbandingan, blok *body* mengakomodasi catatan detail transaksi.



Gambar 1. Arsitektur *blockchain*

Kriptografi memainkan bagian penting dalam pembentukan *blockchain*. Gambar 2. menunjukkan pembuatan *blockchain*. Pemohon akan menandatangani transaksi dan kemudian menyebarkan ke jaringan untuk dilakukan verifikasi. Transaksi yang terverifikasi akan ditambahkan dengan transaksi sebelumnya. Setelah jumlah blok

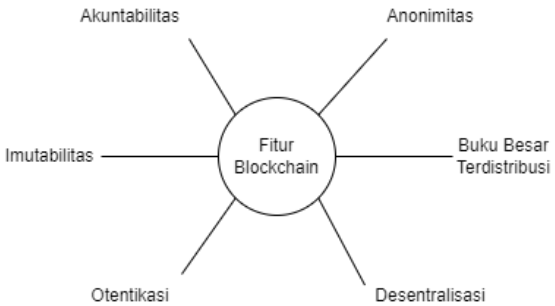
mencapai nilai atau waktu tertentu, transaksi dibungkus menjadi blok baru. Hash dari semua transaksi dihasilkan di blok baru menggunakan algoritma *hash* yang telah ditentukan. *Root hash* terbentuk dari *hash* yang dihasilkan, menghasilkan pembuatan pohon *Merkle*. Dalam protokol konsensus *proof of work*, penambang akan menghitung *nonce* untuk blok baru berdasarkan tingkat kesulitan blok. Blok baru yang divalidasi dilampirkan ke blok yang ada dengan menautkan *hash* blok sebelumnya ke *hash* blok baru yang divalidasi. Transaksi dianggap selesai setelah bloknya dipasang ke *blockchain*.



Gambar 2. Proses pembentukan *blockchain*

3.1.2 Fitur

Teknologi blockchain menyediakan beberapa teknologi kunci yang memungkinkan imutabilitas (Sapra, & Dhaliwal, 2021), akuntabilitas (Rizal Batubara, Ubacht, & Janssen, 2019), keaslian (Basu, Dimitrakos, Nakano, & Kiyomoto, 2019), anonimitas (Sapra, & Dhaliwal, 2021), buku besar terdistribusi [30], dan desentralisasi (Sapra, & Dhaliwal, 2021) yang digambarkan pada Gambar. 3.



Gambar 3. Fitur *blockchain*

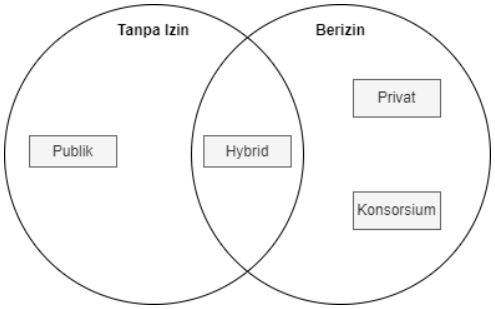
Imutabilitas memberikan perlindungan semua transaksi dari perubahan (Sapra, & Dhaliwal, 2021). Catatan transaksi ditandatangani secara digital dengan melibatkan mitra terkait, menghasilkan nilai *hash* transaksi yang relevan. *Hash* akan digunakan dalam transaksi berikutnya yang membuat rantai tertaut. Mekanisme ini merupakan properti imutabilitas yang membuat transaksi secara komputasi tidak dapat diubah dan dihapus.

Akuntabilitas memfasilitasi *log* transaksi yang valid untuk audit (Rizal Batubara, Ubacht, & Janssen, 2019). Sebagai perbandingan, keaslian mempromosikan verifikasi pengguna melalui sertifikat digital. Setiap transaksi menggunakan metode tanda tangan digital untuk memverifikasi validitas transaksi. Anonimitas memberikan pelestarian identitas dan privasi transaksi (Andola, Yadav, Venkatesan, & Verma, 2021).

Properti buku besar terdistribusi membuat teknologi *blockchain* dapat dibedakan dari sistem basis data lain di mana salinan persis dari basis data didistribusikan ke semua *node* (Rajasekaran dkk, 2022). Protokol konsensus menangani pembuatan blok ketika transaksi baru ditambahkan. Sebaliknya, properti desentralisasi berarti tidak ada otoritas pusat yang diperlukan dalam sistem *blockchain*, yang berarti tidak ada satu titik kegagalan (Sapra, & Dhaliwal, 2021). Oleh karena itu, semua *node* berfungsi sebagai *server*.

3.1.3 Klasifikasi

Dengan berkembangnya teknologi *blockchain*, jenis-jenis *blockchain* semakin berkembang. Jenis *blockchain* pertama adalah *blockchain* publik (Sapra, & Dhaliwal, 2021). Saat ini, jenis *blockchain* dapat diklasifikasikan sebagai *blockchain* yang memiliki izin dan tanpa izin tergantung pada tingkat izinnya (Rajasekaran dkk, 2022). Gambar 4 menggambarkan klasifikasi *blockchain* publik, privat, konsorsium, dan *hybrid*.



Gambar 4. Klasifikasi *blockchain*

Blockchain tanpa izin mencakup *blockchain* publik, di mana siapa pun dapat berpartisipasi dalam transaksi *blockchain*. Implementasi paling umum dari *blockchain* publik adalah *Bitcoin*. Sebaliknya, *blockchain* privat hanya menyediakan orang yang berwenang untuk bergabung dengan jaringan, yang umumnya menggunakan otoritas terpusat untuk mengontrol izin baca dan tulis. *Blockchain* konsorsium dapat disebut sebagai konsorsium *blockchain*, termasuk beberapa grup dalam jaringan blockchain. Alih-alih menggunakan satu otoritas terpusat seperti *blockchain* privat, konsorsium mengelola beberapa pemimpin grup untuk mengelola setiap node grup. *Hyperledger Fabric* adalah salah satu *blockchain* konsorsium yang telah banyak digunakan. *Blockchain hybrid* sebanding dengan

blockchain konsorsium, meskipun dikendalikan oleh satu otoritas yang menggabungkan beberapa proses tanpa izin.

3.1.4 Konsensus

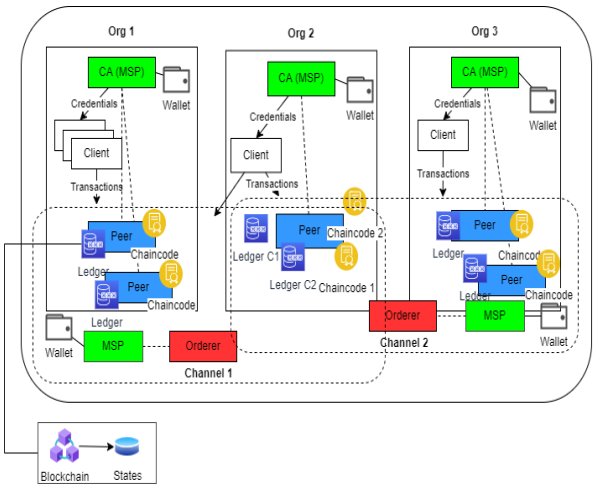
Protokol konsensus memainkan peran penting dalam sistem *blockchain* (Abdelmaboud dkk, 2022). Sebelum transaksi baru ditambahkan ke blok, itu didistribusikan ke jaringan untuk validasi. Prosedur validasi menggunakan protokol konsensus sehingga setiap salinan buku besar di semua *node* identik. Ada berbagai protokol konsensus yang tersedia di *blockchain*, seperti *proof of work*, *proof of authority*, *practical Byzantine fault tolerance (PBFT)*, dan *crash fault tolerance (CFT)*.

3.1.5 Smart contract

Smart contract adalah aturan perjanjian yang memungkinkan transaksi otomatis (Abdelmaboud dkk, 2022). Seperti dalam kontrak hukum, itu terdiri dari syarat dan ketentuan antara para pihak. Setiap transaksi secara otomatis memeriksa apakah itu memenuhi ketentuan kontrak tanpa bantuan pihak ketiga, yang merupakan tujuan mendasar dari *smart contract*.

3.2 *Hyperledger Fabric*

Hyperledger Fabric adalah salah satu proyek yang dikelola oleh *IBM* yang menggunakan teknologi blockchain. Konsep penting dari arsitektur *Fabric* adalah metode modulasi dan *extensible* di mana setiap subsistem di *Fabric* dapat dicolokkan. Tidak seperti pendekatan *blockchain* pertama yang dapat diterapkan untuk transaksi berbasis kripto, *Fabric* menyediakan solusi berbasis *non-token*. Sebagai blockchain konsorsium, kerangka *Fabric* memiliki komponen organisasi, *peer*, *orderer*, dan *channel*. Gambar 5. menggambarkan arsitektur *Fabric*. Komponen akan ditentukan di bagian berikut.



Gambar 5. Arsitektur *Hyperledger Fabric*

3.2.1 Organisasi

Setiap peserta dalam jaringan *Fabric* milik organisasi. Organisasi mengelola pembuatan identitas setiap peserta. Identitas adalah elemen penting yang digunakan untuk menandatangani setiap transaksi di dalam saluran.

3.2.2 *Peer*

Peer mirip dengan *node* di *blockchain*. *Peer* memiliki lingkungan sendiri yang digunakan untuk menyimpan kode rantai dan buku besar. Oleh karena itu, ia bertanggung jawab untuk mengeksekusi, menandatangani, memvalidasi, dan menyimpan transaksi. Saat transaksi dipanggil, *peer* pengesahan akan menjalankan fungsi kode rantai berikut dan menandatangani hasil transaksi. Hasilnya disebarkan dan divalidasi dalam jaringan. Transaksi yang divalidasi akan ditambahkan ke *blockchain* dan diperbarui di basis data *state*.

3.2.3 *Orderer*

Orderer terdiri dari satu atau lebih *node* yang bertanggung jawab untuk mengumpulkan, mengurutkan, dan membungkus transaksi ke dalam blok dan mendistribusikannya ke *peer* lainnya untuk verifikasi. Pengembangan blok menggunakan *Raft* sebagai protokol konsensus. *Raft* menerapkan metode *crash fault tolerance* untuk layanan *orderer* yang tangguh, yang dapat memanfaatkan sekelompok *orderer* yang memperkenalkan pemilihan *leader* yang dinamis.

3.2.4.*Channel*

Jaringan Fabric dapat menggabungkan lebih dari satu *channel*. *Channel* mirip dengan *subnet* yang memisahkan data komunikasi dalam peserta jaringan. Transaksi di setiap *channel* disimpan dalam buku besar mereka sendiri. Oleh karena itu, ini berisi blok genesis khas di setiap buku besar *channel*.

3.2.5 *Chaincode*

Chaincode identik dengan *smart contract*. Ini adalah bagian dari kode yang berisi kesepakatan dan kebijakan yang membawa logika bisnis. Ini juga termasuk kebijakan pengesahan di mana transaksi perlu ditandatangani oleh pengesahan. Keunikannya adalah dapat menggunakan berbagai bahasa untuk membangun *smart contract* di *Fabric*, seperti *Go*, *Java*, dan *Node.js*. *Chaincode* disebarkan di rekan masing-masing organisasi di saluran yang sama.

3.2.6 *Membership Service Provider (MSP)*

Setiap peserta yang terkait dengan organisasi memiliki identitas unik yang disimpan dalam sertifikat X.509. Konfigurasi untuk membuat identitas unik dikonfigurasi di penyedia layanan keanggotaan (*MSP*). Otoritas sertifikat (*CA*)

organisasi mengeluarkan sertifikat unik peserta X.509. Sertifikat berisi kunci publik dan pribadi, yang merupakan kunci pribadi yang digunakan untuk menandatangani transaksi dan kunci publik untuk verifikasi.

3.2.7 Wallet

Dompet *Fabric* berisi identitas setiap peserta yang dibuat melalui *MSP*. Identitas tersebut digunakan untuk menandatangani dan memverifikasi transaksi. Dompet identitas biasanya disimpan di sistem *file*, tetapi bisa disimpan di memori lokal, basis data *CouchDB*, atau di Modul Keamanan Perangkat Keras (*HSM*).

3.2.8 *Ledger*

Buku besar atau *ledger* di *Fabric* dibagi menjadi dua bagian, *blockchain* dan *state*. *Blockchain* menyimpan koleksi transaksi yang tidak dapat diubah sementara *state* berisi informasi terbaru dari suatu data. Buku besar didistribusikan di setiap rekan yang divalidasi melalui mekanisme protokol *CFT*.

3.2.9 *State*

State dalam arsitektur *Fabric* mirip dengan *collection*. *State* berisikan data pasangan kunci dan nilai. Basis data *state* adalah basis data yang paling banyak diakses karena berisi informasi terkini dari objek transaksi daripada nilai objek yang lalu.

4. ARSITEKTUR SISTEM DAN DESAIN

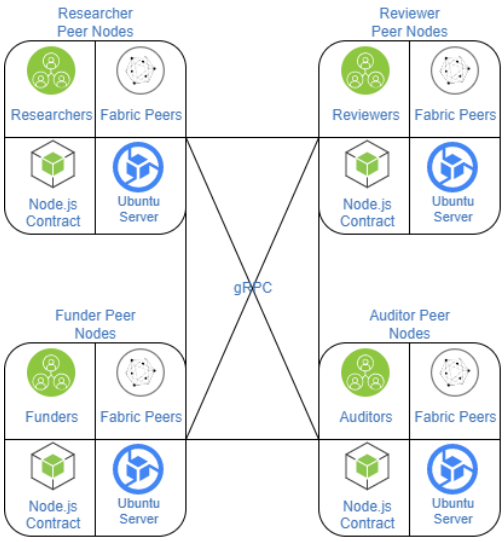
Penelitian ini berkontribusi dalam merancang konsorsium *blockchain* pada sistem seleksi pendanaan riset. Arsitektur berikut berfokus untuk mengubah sistem yang ada dengan peningkatan imutabilitas untuk memastikan integritas transaksi, akuntabilitas untuk memungkinkan audit yang jelas, dan interoperabilitas untuk menyediakan komunikasi data yang mudah. Desain terdiri dari skenario bisnis, koleksi buku besar, dan kebijakan jaringan.

4.1 Skenario Bisnis

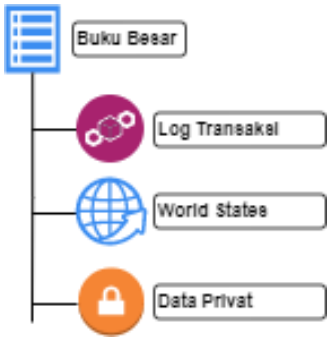
Blockchain memanfaatkan teknologi *smart contract*, yang membuat kontrak dapat dibaca oleh komputer. Hal ini membuat transaksi dapat berjalan secara otomatis tanpa bantuan pihak ketiga. Gambar 6 menggambarkan skenario bisnis sistem. Skenario bisnis terdiri dari beberapa node *peer*: peneliti, *reviewer*, penyandang dana, dan *auditor*. Transaksi antar peer dilakukan dengan remote procedure call untuk mengakomodasi transaksi yang lebih cepat. *Node* peneliti meliputi fungsionalitas pengajuan proposal, personel, dan profil peneliti. *Node reviewer* memfasilitasi penilaian proposal. Sebagai perbandingan, simpul pemberi dana mencakup pendanaan untuk setiap proposal penelitian yang diterima. Sebaliknya, simpul *auditor* menggunakan pemeriksaan penilaian proposal dan pendanaan.

4.2 Koleksi Buku Besar

Blockchain mewakili buku besar yang didistribusikan. Buku besar dalam sistem terdiri dari koleksi khusus: *log* transaksi, *world state*, dan data privat. Gambar 7 menunjukkan jenis koleksi buku besar. *Log* transaksi menyimpan semua transaksi yang dilakukan oleh setiap *peer*. Sebagai perbandingan, *world state* menyimpan status setiap koleksi saat ini. Sebaliknya, data privat mengunci informasi sensitif yang menunjukkan catatan *hash* pada *world state*.

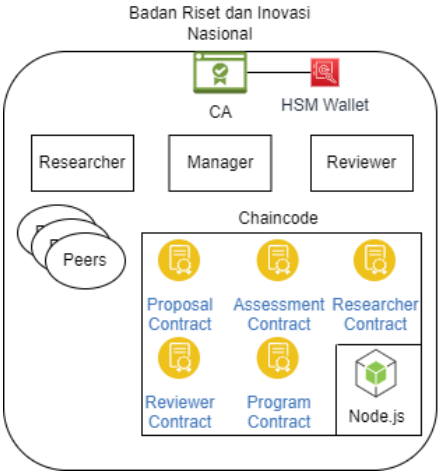


Gambar 6. Skenario bisnis



Gambar 7. Tipe koleksi buku besar

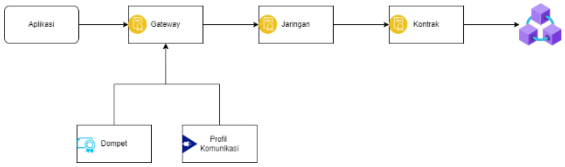
Chaincode mewakili *smart contract* dalam sistem *HLF*. Gambar 8 mencirikan pengembangan *chaincode* di organisasi BRIN. *Chaincode* membahas proposal, *assessment*, *researcher*, *reviewer*, dan kontrak program. Kontrak proposal menunjuk pengaturan transaksi yang diusulkan. Sebagai perbandingan, kontrak *assessment* mencakup penyelesaian penilaian proposal. Selain itu, kontrak *reviewer* mengelola pemilihan *reviewer*. Selanjutnya, kontrak program mencatat informasi tentang program pendanaan.



Gambar 8. Kontrak BRIN

4.3 Kebijakan Jaringan

Kebijakan jaringan menyediakan bagian penting dari sistem *HLF* sebagai benteng untuk menjalankan otentikasi dan pemeriksaan validitas. Gambar 9 menginterpretasikan kebijakan jaringan dalam sistem. Aplikasi yang mengakses sistem *HLF* akan dirutekan ke *gateway* terlebih dahulu. Identitas dan profil pengguna diautentikasi di *gateway*. Proses otentikasi terdiri dari pengecekan identitas dompet pengguna dan profil koneksi yang ditentukan oleh sistem. Setelah koneksi di *gateway*, itu akan merutekan ke koneksi jaringan, yang mengirimkan permintaan ke rekan yang ditunjuk. Dengan demikian, kontrak yang ditunjuk akan diberlakukan untuk melakukan transaksi yang diminta untuk membuat catatan *blockchain*.



Gambar 9. Arsitektur jaringan

5. IMPLEMENTASI SISTEM

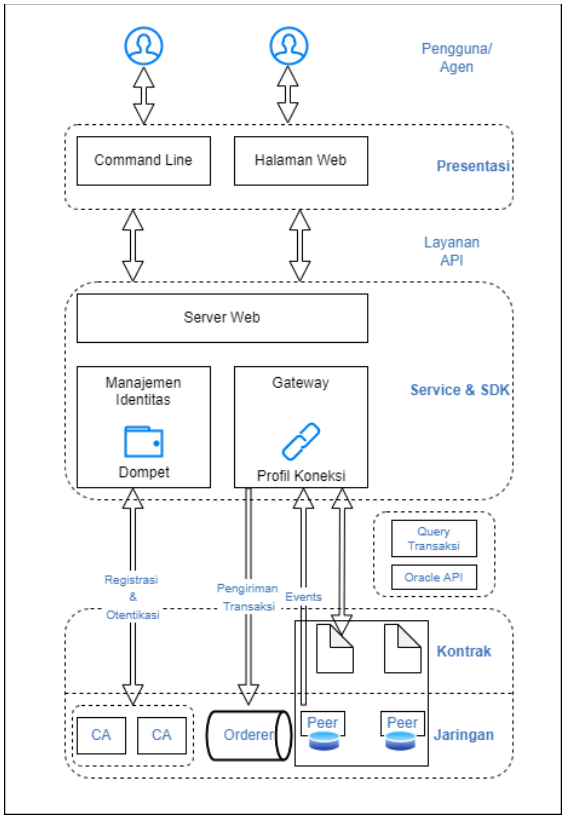
Sistem menerapkan desain *HLF* sebagai sistem inti dalam membuat sistem *CFPChain*. Gambar 10 menggambarkan implementasi sistem. Sistem ini terdiri dari tiga lapisan presentasi, layanan, dan jaringan. Fungsi dari lapisan presentasi adalah untuk menyediakan antarmuka pengguna atau agen, yang terdiri dari antarmuka baris perintah dan halaman web. Lapisan presentasi dapat diakses oleh *API* layanan untuk berkomunikasi dengan lapisan layanan. Lapisan layanan terdiri dari manajemen identitas dan profil koneksi. Manajemen identitas memasok proses pendaftaran dan otentikasi, yang didukung oleh *CA* di lapisan jaringan. Sebaliknya, profil koneksi menangani pengiriman transaksi melalui node pemesan. Komunikasi *node peer* juga berjalan menggunakan profil koneksi. Selain itu, kontrak pintar dapat mengakses *API* lain melalui koneksi *oracle*.

Algoritma tambahProposal menyediakan properti penguraian integritas. Penggunaan rantai *hash* mendukung properti imutabilitas, yang memastikan integritas transaksi. Fungsi dari set data pribadi adalah untuk memberikan kerahasiaan data sensitif.

Tabel 1. Algoritma tambahProposal

Algorithm 1: tambahProposal
Input: proposal data pD
Output: proposal id pId, proposal status pS
Actor: researcher

procedure tambahProposal(pD)
  if *valid_group = True* **and** *valid(pD)* **then**
    send_to_orderer(pD)
    prevId = last_ordering_id(transactions)
    pId = hash(pD)
    set_private_data(pD)
    pS = put(pId, prevId, pD, userId)
    return pId, pS
  else
    not in group or not valid data
  end if
end procedure



Gambar 10. Implementasi sistem

Dalam algoritma tambahProposal memberikan solusi kemampuan audit. Adopsi integritas dengan tetap menjaga transparansi data dapat dilakukan dengan menggunakan blockchain. Fungsi membaca data pribadi mengelola transparansi data,

memungkinkan entitas yang berwenang untuk membaca data.

Tabel 2. Algoritma daftarProposal

Algorithm 2: daftarProposal
Input: user MSP id userMspId
Output: proposal data pD
Actor: reviewer, funder, auditor

procedure daftarProposal()
  if *valid_group = True* **then**
    proposals = query_proposal(userMspId)
    if group = reviewer **then**
      reviews = query_review(userMspId)
      reviews = *read_private_data_review(reviews)*
      proposals = *merge_result_sets(proposals, reviews)*
    else if group = funder **then**
      proposals = *read_private_data_proposal_budget(proposals)*
    else if group = auditor **then**
      proposals = *read_private_data_proposal_budget(proposals)*
      reviews = *read_private_data_review(reviews)*
      proposals = *merge_result_sets(proposals, reviews)*
    end if
  else
    not in group
  end if
end procedure

Interoperabilitas dapat dilakukan dalam sistem blockchain konsorsium. Melalui *peer* dan pembuatan kode rantai, siklus hidup transaksi dapat diintegrasikan sebagai unit data standar. Gambar 11 menunjukkan informasi konfigurasi *node* yang menyediakan pengaturan *node* yang digunakan oleh sistem.

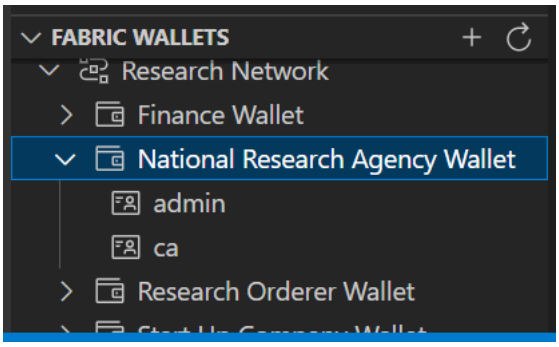
```
{
        "name": "orderer.cfpchain.com",
        "msp_id": "CfpChainOrdererOrgMSP",
        "api_url": "grpcs://localhost:7050",
        "type": "fabric-orderer",
        "ssl_target_name_override":
"orderer.cfpchain.com",
        "pem": "LS0tLS1…"
},
{
        "name": "peer0.nraorg.cfpchain.com",
        "msp_id":
"NationalResearchAgencyOrgMSP",
        "api_url": "grpcs://localhost:7051",
        "type": "fabric-peer",
        "ssl_target_name_override":
"peer0.nraorg.cfpchain.com",
        "pem": "LS0tLS1…"
}
```

Gambar 11. Konfigurasi *node*

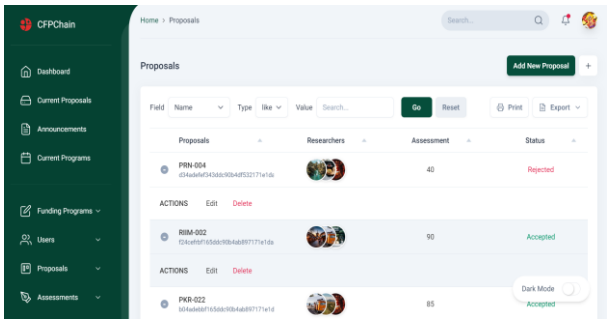
Dompet adalah istilah yang digunakan untuk menyimpan identitas digital pengguna dalam sistem *blockchain*. Gambar 12 menunjukkan dompet yang tersedia. Dompet dapat disimpan di mesin *HSM* untuk mematuhi persyaratan Standar Pemrosesan Informasi Federal (*FIPS*) untuk menyimpan kunci privat. Gambar 13 menyajikan aplikasi web untuk mengakses sistem *CFPChain*.

Pengujian yang dilakukan dalam penelitian ini adalah pengujian kinerja. Pengujian kinerja berfungsi untuk mengevaluasi sistem yang dibangun dari segi stabilitas untuk memastikan sistem yang responsif terhadap kebutuhan akses pengguna. Pengujian kinerja meliputi evaluasi waktu respon, ketersediaan layanan, dan keandalan sistem dalam melayani permintaan akses pengguna. Spesifikasi servernya:

- CPU: 8 Core
- RAM: 32 GB DDR4
- OS: Linux
- HDD: 500 GB
- Bandwidth: 100 Mbps



Gambar 12. Dompet pada *CFPChain*



Gambar 13. Tampilan sistem *CFPChain*

Pengujian ini dilakukan dengan menggunakan aplikasi Jmeter yang merupakan platform pengujian kinerja suatu sistem. Tabel IV menunjukkan rangkuman hasil pengujian kinerja pada beberapa operasi yang telah ditentukan sebelumnya. Pengujian dilakukan untuk menunjukkan evaluasi kinerja sistem yang diusulkan sehubungan dengan sistem saat ini. Hasil menunjukkan bahwa sistem yang diusulkan memberikan keamanan yang lebih baik dengan penurunan kinerja yang dapat ditoleransi.

Tabel IV. Hasil Uji Kinerja

No	Fungsi	Jumlah Permintaan	Waktu (detik)	
			Dengan Blockchain	Tanpa Blockchain
1	tambahProposal	50	5.44	3.78
		500	24.67	17.34
		5000	345.80	251.73
2	daftarProposal	50	2.35	1.11
		500	5.85	3.36
		5000	82.35	64.46

6. HASIL DAN DISKUSI

Penelitian ini mengusulkan peningkatan keamanan sistem seleksi pendanaan riset BRIN dengan melengkapi properti integritas, auditabilitas, dan interoperabilitas. Penggunaan catatan *on-chain* memberikan integritas dalam setiap transaksi. Selain memastikan integritas, auditabilitas dilengkapi dengan pemanfaatan data *on-chain*. Evaluasi transaksi dapat diperiksa secara menyeluruh karena sifat dari *blockchain*, memberikan imutabilitas dan transparansi. Selain memastikan integritas dan kemampuan audit, juga mendukung interoperabilitas pada sistem. Kriteria interoperabilitas membantu dengan memanfaatkan sistem konsorsium. Sistem konsorsium memberikan standarisasi protokol seperti data dan media komunikasi. Optimasi sistem yang dibangun memberikan tingkat keamanan yang lebih tinggi dengan pengurangan kinerja yang masih dapat diterima. Saran untuk pekerjaan di selanjutnya yaitu menyertakan keamanan dokumen untuk memastikan kerahasiaan, integritas, dan ketersediaan dokumen pengguna dalam sistem *blockchain*.

DAFTAR PUSTAKA

ABDELMABOUD, A., AHMED, A. I. A., ABAKER, M., EISA, T. A. E., ALBASHEER, H., GHORASHI, S. A., dan KARIM, F. K., 2022. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics, 11(4), 630.

AHMAD, D., LUTFIANI, N., AHMAD, A. D. A. R., RAHARDJA, U., dan AINI, Q., 2021. Blockchain Technology Immutability Framework Design in E-Government. Jurnal Administrasi Publik: Public Administration Journal, 11(1), 32-41.

ALI, S., dan CHONG, I., 2019. Semantic mediation model to promote improved data sharing using representation learning in heterogeneous healthcare service environments. Applied Sciences, 9(19), 4175.

ANDOLA, N., YADAV, V. K., VENKATESAN, S., dan VERMA, S., 2021. Anonymity on blockchain based e-cash protocols—A survey. Computer Science Review, 40, 100394.

ANTAL, C., CIOARA, T., ANTAL, M., dan ANGHEL, I., 2021. Blockchain platform for COVID-19 vaccine supply management. IEEE Open Journal of the Computer Society, 2, 164-178.

BASU, A., DIMITRAKOS, T., NAKANO, Y., dan KIYOMOTO, S., 2019. A framework for blockchain-based verification of integrity and authenticity. IFIP International Conference on Trust Management (pp. 196-208). Springer, Cham.

BETTAYEB, M., NASIR, Q., dan TALIB, M. A., 2021. Implementation of Hyperledger-Based Secure Firmware Update Delivery for IoT Devices. In Trust Models for Next-Generation Blockchain Ecosystems (pp. 191-223). Springer, Cham.

GRAF, M., KÜSTERS, R., dan RAUSCH, D., 2020. Accountability in a permissioned blockchain: Formal analysis of hyperledger fabric. 2020 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 236-255). IEEE.

HANG, L., ULLAH, I., dan KIM, D. H., 2020. A secure fish farm platform based on blockchain for agriculture data integrity. Computers and Electronics in Agriculture, 170, 105251.

HASSIJA, V., CHAMOLA, V., KRISHNA, D. N. G., KUMAR, N., dan GUIZANI, M., 2020. A blockchain and edge-computing-based secure framework for government tender allocation. IEEE Internet of Things Journal, 8(4), 2409-2418.

HONAR PAJOOH, H., RASHID, M., ALAM, F., dan DEMIDENKO, S., 2021. Hyperledger fabric blockchain for securing the edge internet of things. Sensors, 21(2), 359.

HOU, H., 2017. The application of blockchain technology in E-government in China. 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-4). IEEE.

HUANG, D., MA, X., dan ZHANG, S., 2019. Performance analysis of the raft consensus algorithm for private blockchains. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 172-181.

IMANTO, T., dan YAZID, S., 2021. Blockchain Based Halal Food Production Tracking. 2021 6th International Workshop on Big Data and Information Security (IWBIS) (pp. 97-102). IEEE.

JING, N., LIU, Q., dan SUGUMARAN, V., 2021. A blockchain-based code copyright

management system. Information Processing & Management, 58(3), 102518.

KHAN, N. D., CHRYSOSTOMOU, C., dan NAZIR, B., 2020. Smart FIR: securing e-FIR data through blockchain within smart cities. 2020 IEEE 91st vehicular technology conference (VTC2020-Spring) (pp. 1-5). IEEE.

KUMAR, M., dan CHAND, S., 2021. MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. Journal of Network and Computer Applications, 179, 102975.

LI, D., DENG, L., CAI, Z., dan SOURI, A., 2022. Blockchain as a service model in the Internet of Things management: systematic review. Transactions on Emerging Telecommunications Technologies, 33(4), e4139.

LI, H., ZHU, L., SHEN, M., GAO, F., TAO, X., dan LIU, S., 2018. Blockchain-based data preservation system for medical data. Journal of medical systems, 42(8), 1-13.

LOY, A. C. M., LIM, J. Y., HOW, B. S., dan YOO, C. K., 2021. Blockchain as a frontier in biotechnology and bioenergy applications. Trends in Biotechnology.

MARTINSON, P., 2019. Estonia–the Digital Republic Secured by Blockchain. PricewaterhouseCoopers: London, UK, 1-12.

MITANI, T., dan OTSUKA, A., 2020. Traceability in permissioned blockchain. IEEE Access, 8, 21573-21588.

MONRAT, A. A., SCHELÉN, O., dan ANDERSSON, K., 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

PAWLAK, M., dan PONISZEWSKA-MARAŃDA, A., 2021. Implementation of Auditable Blockchain Voting System with Hyperledger Fabric. International Conference on Computational Science (pp. 642-655). Springer, Cham.

PETRATOS, P. N., LJEPAVA, N., dan SALMAN, A., 2020. Blockchain technology, sustainability and business: A literature review and the case of Dubai and UAE. Sustainable Development and Social Responsibility—Volume 1, 87-93.

PU, S., dan LAM, J. S. L., 2021. Blockchain adoptions in the maritime industry: a conceptual framework. Maritime Policy & Management, 48(6), 777-794.

RAJASEKARAN, A. S., AZEES, M., dan AL-TURJMAN, F., 2022. A comprehensive survey on blockchain technology. Sustainable Energy Technologies and Assessments, 52, 102039.

RASHIDEH, W., 2020. Blockchain technology framework: Current and future perspectives for the tourism industry. Tourism Management, 80, 104125.

RIZAL BATUBARA, F., UBACHT, J., dan JANSSEN, M., 2019. Unraveling transparency and accountability in blockchain. Proceedings of the 20th Annual International Conference on Digital Government Research (pp. 204-213).

SAPRA, R., dan DHALIWAL, P., 2021. Blockchain: the perspective future of technology. International Journal of Healthcare Information Systems and Informatics (IJHISI), 16(2), 1-20.

SINGH, S., HOSEN, A. S., dan YOON, B., 2021. Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, 13938-13959.

TARKHANOV, I., FOMIN-NILOV, D., dan FOMIN, M., 2019. Application of public blockchain to control the immutability of data in online scientific periodicals. Library Hi Tech.

WANG, H., dan YANG, D., 2021. Research and Development of Blockchain Recordkeeping at the National Archives of Korea. Computers, 10(8), 90.

XU, X., RAHMAN, F., SHAKYA, B., VASSILEV, A., FORTE D., dan TEHRANIPOOR, M., 2019. Electronics supply chain integrity enabled by blockchain. ACM Transactions on Design Automation of Electronic Systems (TODAES), 24(3), 1-25.

ZOU, B., ZHAO, G., TANG, H., NIE, R., HUANG, R., dan TANG, J., 2021. ArchivesChain: Distributed PKI Archives System. 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE) (pp. 1009-1013). IEEE.