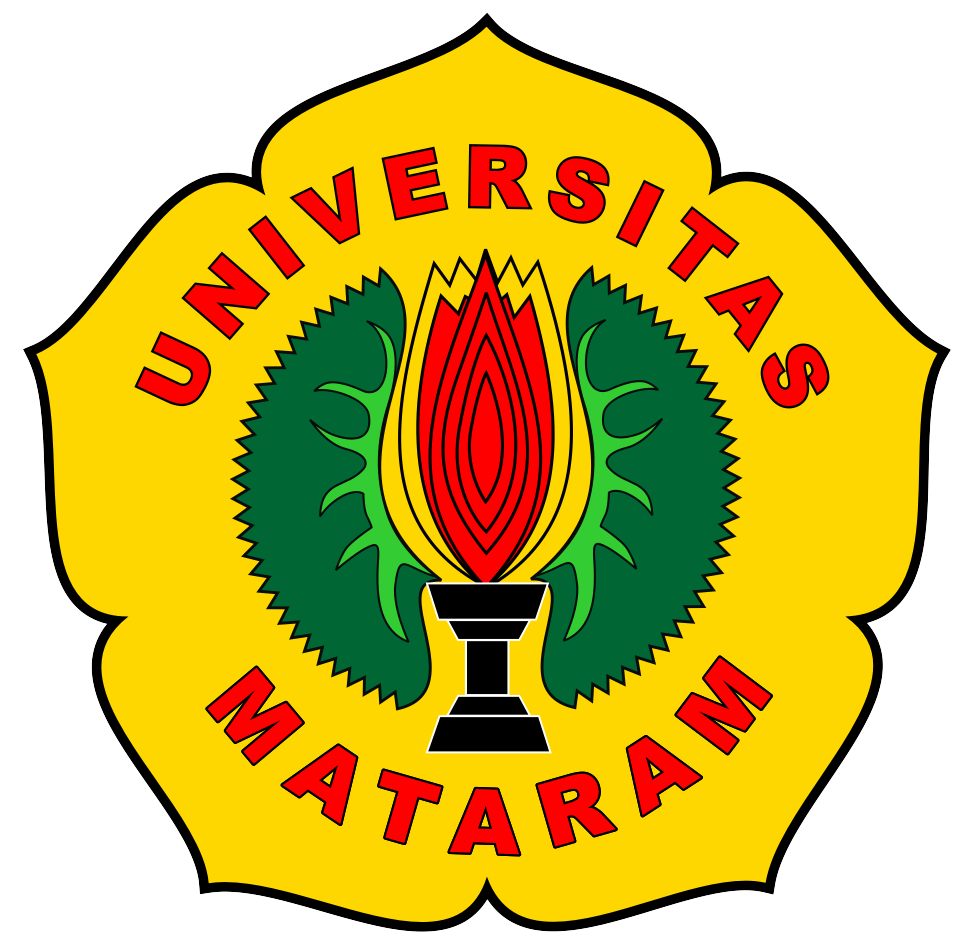
**USULAN TUGAS AKHIR**

**Implementasi *Blockchain* Sebagai Sistem Keamanan IoT dalam Mengirim, Mendistribusikan dan Menjaga Privasi Data**



**Oleh :**Lalu Ocky Saktiya Luhung  
F1B019079

**JURUSAN TEKNIK ELEKTRO**

**FAKULTAS TEKNIK**

**UNIVERSITAS MATARAM**

**DAFTAR ISI**

**DAFTAR GAMBAR**

**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Dengan kemajuan teknologi komunikasi dan pengenalan jaringan 5G di mana-mana, teknologi *Internet of Things* mulai berkembang pada tingkat yang eksponensial. *Smart Home*, *Smart City*, *e-Health*, dan *Internet of Things* untuk perusahaan industri, intelijen terdistribusi, dan sistem lainnya adalah cara yang efektif dan akrab bagi masyarakat untuk meningkatkan banyak proses, misalnya, proses untuk monitoring keadaan rumah berdasarkan sensor dan proses lain yang dapat menjadi otomatis. Pendekatan proses seperti itu mengurangi pengaruh faktor manusia dan berkontribusi pada peningkatan efisiensi perusahaan, di mana ada semua prasyarat untuk penggunaan teknologi IoT. Terlepas dari semua efektivitas dan prevalensinya, teknologi *Internet of Things* memiliki banyak tantangan dan masalah yang terkait dengan keamanan dan konfigurasi perangkat IoT yang aman. Keberadaan sejumlah besar perangkat semacam itu penuh dengan bahaya, karena penyerang dapat mengendalikannya dan mengatur serangan DDoS dan manipulasi lalu lintas lainnya menggunakan perangkat IoT, yang mengirim perangkat ini ke *server*. Salah satu contoh serangan terpadu pada beberapa perangkat IoT adalah botnet. Botnet adalah kumpulan perangkat yang disusupi di bawah kendali penyerang. Mirai adalah worm dan botnet yang dibentuk oleh perangkat yang diretas (disusupi) seperti *Internet of Things* (pemutar video, webcam pintar, dll.). Botnet ini meretas perangkat dengan menebak kata sandi untuk port 23 (telnet). Dalam sistem IoT terpusat, terkadang cukup untuk meretas server atau mikrokontroler yang bertanggung jawab untuk komunikasi antara sekelompok besar perangkat agar dapat mengontrol semua perangkat yang berkomunikasi melalui protokol terpusat dengan *server* yang dikompromikan (Nesterenko dan Maslova: 2022).

Di lain sisi, perkembangan teknologi yang cukup maju memungkinkan untuk mengurangi dampak dari masalah yang ada, bahkan ada kemungkinan dapat menyelesaikan masalah yang ada. Teknologi yang dimaksud adalah *blockchain*.

Pendekatan penyimpanan yang terdesentralisasi untuk menyediakan penyimpanan data terdapa pada teknologi *blockchain* dan layanan berbagi. Untungnya, sifat teknologi *blockchain* dapat memberikan solusi yang baik untuk sistem penyimpanan yang terdesentralisasi. *Blockchain* terdiri dari blok-blok individual yang dihubungkan oleh fungsi hash, dan setiap blok berisi nilai hash dari blok sebelumnya, *time-stamp*, dan data transaksi. *Blockchain* dapat dianggap sebagai *database* buku besar terdistribusi, yang terdesentralisasi, terbuka dan transparan, anti-rusak, dan dapat dilacak, serta menyediakan metode penyimpanan yang aman dan andal untuk data ().

Pada dasarnya *Blockchain* adalah buku besar basis data yang terdesenralisasi, terdistribusim saling berbagi dan sangat sulit untuk diubah yang menyimpan daftar aset dan transaksi di jaringan *peer-to-peer*, serta telah merantai blok data yang telah diberi cap waktu dan divalidasi oleh *miners*. Teknologi *blockchain* telah diramalkan oleh industri dan komunitas penelitian sebagai teknologi yang sangat menyita perhatian yang siap memainkan peran utama mengelola, mengendalikan, dan yang paling penting mengamankan perangkat IoT. *Blockchain* menggunakan algoritma *hashing* SHA-256 untuk memberikan bukti kriptografi yang kuat untuk otentikasi dan integritas data. *Blockchain* memiliki riwayat penuh dari semua transaksi dan memberikan kepercayaan terdistribusi global. Salah satu tujuan penggunaan *blockchain* adalah untuk menghilangkan pihak ketiga atau *Trusted Third Parties* (TTP). TTP atau otoritas dan layanan terpusat dapat diganggu, ditembus kemanannya, dan diretas. Mereka juga dapat berbuat jahat dan berprilaku korup di masa depan, meskipun mereka dapat dipercaya sekarang (Khan, dkk, 2018).

* 1. **Rumusan Masalah**

Berdasarkan latar belakang diatas dapat diidentifikasi beberapa permasalahan yaitu :

1. Bagaimana cara menjaga keamanan data dalam sistem IoT dengan menggunakan *blockchain*?
2. Bagaimana *blockchain* dapat diimplemetasikan pada sistem keamanan IoT untuk meningkatkan keamanan dan privasi data?
3. Bagaimana *blockchain* dapat memfasilitasi proses autentikasi dan otorisasi pada sistem keamanan IoT?
4. Bagaimana cara mengintegrasikan teknologi *blockchain* pada infrastruktur dan arsitektur yang sudah ada pada sistem keamanan IoT?
   1. **Ruang Lingkup**

Penelitian yang dilakukan memiliki batasan masalah dan ruang lingkup sebagai berikut :

1. Menjaga keamanan dan privasi data dalam sistem IoT berfokus dengan menggunakan jaringan *private* *blockchain*.
2. Perancangan dan pengembangan sistem keamanan IoT berbasis *blockchain*.
3. Analisis keamanan dan privasi data pada sistem keamanan IoT berbasis *blockchain*.
4. Analisis kinerja sistem keamanan IoT berbasis *blockchain*.
   1. **Tujuan Penelitian**

Tujuan penelitian ini adalah mengimplementasi dan mengintegrasi teknologi IoT dengan teknologi *blockchain* dalam membangun keamanan sistem IoT dengan menggunakan *blockchain*, dan berbagai hal lainnya seperti berikut:

1. Berhasil menjaga keamanan dan privasi data pada sistem IoT dengan *blockchain*.
2. Melakukan uji coba dan evaluasi sistem keamanan IoT berbasis *blockchain* yang telah dikembangkam untuk memastikan keamanan dan efektivitasnya.
3. Menganalisis kelemahan dan tantangan keamanan pada sistem IoT dan mengidentifikasi bagaimana teknologi *blockchain* dapat digunakan untuk meningkatkan keamanan dan provasi data dalam sistem IoT.
4. Menganalisis kinerja sistem keamanan IoT berbasis *blockchain* untuk memastikan ketersediaan, integritas, dan keandalan data yang diproses dan disimpan dalam sistem.
   1. **Manfaat Penelitian**

Manfaat dari hasil pembuatan Tugas Akhir ini adalah :

1. Dapat meningkatkan keamanan sistem IoT yang sudah ada dengan mengintegrasikan dengan teknologi *blockchain*.
2. Mendapatkan pemahaman implementasi *blockchain* pada pada sistem keamanan IoT.
3. Menggunakan dan mengintegrasikan IoT dengan *Blockchain* dapat meningkatkan keamanan dan privasi data.
   1. **Sistematika Penulisan**

**BAB II**

**TINJAUAN PUSTAKA DAN DASAR TEORI**

1. **Tinjauan Pustaka**

Pada tinjauan pustaka ini akan membahas penelitian yang pernah dilakukan sebelumnya atau yang relevan dengan penelitian yang akan dilakukan sebagai acuan dalam pengerjaan penelitian.

Penelitian pertama adalah "*Blockchain for IoT Security and Privacy: The Case Study of a* Smart Home".Studi ini mempelajari penggunaan *blockchain* untuk meningkatkan keamanan dan privasi pada lingkungan Smart Home, yang merupakan salah satu aplikasi penting dari IoT. Pendekatan studi kasus untuk mengevaluasi keefektifan penggunaan *blockchain* dalam meningkatkan keamanan dan privasi pada Smart Home. Penggunaan *blockchain* pada Smart Home dapat memberikan beberapa keuntungan dalam hal keamanan dan privasi, seperti mengurangi risiko serangan peretas dan memastikan privasi data pengguna. Secara keseluruhan, penelitian ini menyimpulkan bahwa penggunaan *blockchain* dapat memberikan solusi yang efektif untuk mengatasi tantangan keamanan dan privasi pada Smart Home. Studi ini menunjukkan bahwa implementasi *blockchain* pada Smart Home dapat meningkatkan tingkat keamanan, privasi, dan pengelolaan data yang lebih efektif pada lingkungan IoT (Dorri dkk., 2017).

Penelitian kedua adalah "*A secure and private data sharing architecture for IoT based on blockchain and smart contract*".Penelitian ini bertujuan untuk memperkenalkan arsitektur berbagi data yang aman dan pribadi untuk *Internet of Things* (IoT) menggunakan *blockchain* dan smart contract.Penelitian ini mengusulkan arsitektur berbagi data yang terdiri dari beberapa komponen, yaitu penyedia layanan, pengguna, dan *blockchain*. Dalam arsitektur ini, *blockchain* digunakan untuk memastikan keamanan dan privasi data, sedangkan smart contract digunakan untuk mengatur dan mengelola data yang dibagikan.Hasil dari penelitian ini menunjukkan bahwa arsitektur berbagi data dapat memberikan tingkat keamanan dan privasi yang lebih tinggi dibandingkan dengan arsitektur yang tidak menggunakan *blockchain*. Selain itu, arsitektur yang diusulkan juga lebih efisien dalam hal penggunaan sumber daya dan waktu respons (Mingyu, dkk.,2020).

Penelitian ketiga adalah "*Security threats and solutions to IoT using Blockchain: A Review*".Penelitian ini mengevaluasi penggunaan teknologi *blockchain* sebagai solusi untuk mengatasi ancaman keamanan pada lingkungan *Internet of Things* (IoT). Penelitian ini mengidentifikasi beberapa ancaman keamanan yang dihadapi oleh lingkungan IoT, seperti serangan DDoS, pencurian data, dan manipulasi data. Kemudian, penelitian ini membahas bagaimana teknologi *blockchain* dapat membantu mengatasi masalah-masalah keamanan ini. Dengan penggunaan *blockchain*, sistem IoT dapat dilindungi dari serangan peretas dan manipulasi data. Selain itu, penelitian ini juga membahas tentang tantangan dan kelemahan penggunaan *blockchain* untuk sistem IoT, seperti keterbatasan kapasitas transaksi dan biaya operasional yang tinggi. Namun, penelitian ini menyimpulkan bahwa penggunaan *blockchain* dapat memberikan solusi yang efektif untuk mengatasi ancaman keamanan pada lingkungan IoT. Secara keseluruhan, penelitian ini memberikan informasi yang berguna tentang penggunaan teknologi *blockchain* untuk mengamankan sistem IoT. Studi ini memberikan wawasan tentang bagaimana *blockchain* dapat digunakan untuk mengatasi ancaman keamanan dan memberikan solusi yang efektif untuk mengamankan data pada lingkungan IoT (Alam dkk., 2021).

1. **Dasar Teori** 
   * 1. ***Internet of Things* (IoT)**

*Internet of Things* (IoT), merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terusmenerus yang memungkinkan kita untuk menghubungkan mesin, peralatan, dan benda fisik lainnya dengan sensor jaringan dan aktuator untuk memperoleh data dan mengelola kinerjanya sendiri, sehingga memungkinkan mesin untuk berkolaborasi dan bahkan bertindak berdasarkan informasi baru yang diperoleh secara independen. *Internet of Things* atau sering disebut IoT adalah sebuah gagasan dimana semua benda di dunia nyata dapat berkomunikasi satu dengan yang lain sebagai bagian dari satu kesatuan sistem terpadu menggunakan jaringan internet sebagai penghubung. misalnya sebuah Smart Home yang dapat dimanage lewat *smartphone* dengan bantuan koneksi internet. pada dasarnya IoT bila mendapatkan sambungan internet sebagai media komuniakasi dan *server* sebagai pengumpul informasi yang diterima untuk dianalisa (Efendy, 2018).

Dengan meningkatnya penggunaan perangkat pintar, kemampuan bertahan dan pengorganisasian mandiri jaringan menjadi sangat menantang. Namun, beberapa paradigma pengorganisasian mandiri yang diusulkan, dapat meningkatkan kekuatan jaringan. Dalam IoT, asosiasi dari berbagai perangkat heterogen mengurangi kemampuan jaringan sumber daya, yang menarik perhatian para peneliti ke arah bidang yang sedang berkembang ini.

Perkembangan IoT mengarah pada sejumlah besar pembuatan konten, yang memperoleh unit pemrosesan besar, penyimpanan konten (*cache*), dan penyediaan bandwidth. Hal ini disebabkan karena fakta bahwa jumlah *node* kecil yang terhubung ke Internet akan mencapai 27 miliar pada tahun 2021. Beberapa aplikasi membutuhkan transmisi yang aman, sementara beberapa aplikasi lainnya membutuhkan penyimpanan lokal untuk transmisi cepat dan waktu respons yang rendah. Sejumlah besar konten ini dengan pemrosesan lokal akan membutuhkan teknik yang canggih untuk administrasi local (Ikram dkk.,2019).

* + 1. ***Blockchain***

Sejak Bitcoin diperkenalkan pada tahun 2009, penggunaan *blockchain* telah meledak melalui penciptaan berbagai mata uang kripto, *decentralized finance* (DeFi) *applications*, *non-fungible tokens* (NFT), dan *smart contract*.

*Blockchain* adalah sebuah *database* terdistribusi atau buku besar yang dibagikan di antara *node*-*node* jaringan komputer. *Blockchain* terkenal dengan peran pentingnya dalam sistem mata uang digital untuk menjaga catatan transaksi yang aman dan terdesentralisasi, tetapi tidak terbatas pada penggunaan mata uang digital. *Blockchain* dapat digunakan untuk membuat data dalam industri apa pun menjadi tidak dapat diubah-istilah yang digunakan untuk menggambarkan ketidakmampuan untuk diubah. Karena tidak ada cara untuk mengubah sebuah blok, satu-satunya kepercayaan yang dibutuhkan adalah pada saat pengguna atau program memasukkan data. Aspek ini mengurangi kebutuhan akan pihak ketiga yang terpercaya, yang biasanya adalah auditor atau manusia lain yang menambah biaya dan membuat kesalahan.

*Blockchain* terdiri dari program yang disebut skrip yang melakukan tugas-tugas yang biasanya dilakukan dalam *database*: Memasukkan dan mengakses informasi serta menyimpan dan menyimpannya di suatu tempat. *Blockchain* didistribusikan, yang berarti banyak salinan disimpan di banyak mesin, dan semuanya harus cocok agar valid. *Blockchain* mengumpulkan informasi transaksi dan memasukkannya ke dalam sebuah blok, seperti sebuah sel pada *spreadsheet* yang berisi informasi. Setelah penuh, informasi tersebut dijalankan melalui algoritma enkripsi, yang menciptakan angka heksadesimal yang disebut hash. Hash tersebut kemudian dimasukkan ke dalam header blok berikutnya dan dienkripsi dengan informasi lain dalam blok tersebut. Hal ini menciptakan serangkaian blok yang dirantai bersama. (Hayes,2023).

*Blockchain* adalah sebuah inovasi yang telah menarik banyak sekali

pertimbangan dari para ahli dan *Blockchain* adalah sebuah blok catatan yang diikat Setiap blok berisi dua bagian penting yaitu pertukaran dan header blok. Dalam *blockchain*, sebuah pertukaran membentuk korespondensi penting yang mengizinkan dua hub untuk memperdagangkan data satu sama lain. Struktur esensial dari pertukaran muncul di sisi kiri. Perhatikan bahwa berbagai peluncuran *blockchain* mungkin memiliki sedikit variasi dalam struktur pertukaran seperti pada gambar dibawah ini.



Gambar 2.1 Struktur *Blockchain*

* + 1. ***Blockchain*-IoT**

*Blockchain* menyediakan penyimpanan data yang terdesentralisasi untuk sistem Teknologi Informasi (TI) umum. *Blockchain* diperkenalkan pada akhir tahun 2008 dan berfungsi sebagai platform untuk dan pemrosesan transaksi anonim menggunakan desentralisasi terdesentralisasi menggunakan jaringan komputer biasa. Biasanya, *Blockchain* dibangun sebagai sebuah daftar yang terhubung dari blok data, di mana mengubah satu bit di salah satu blok yang disimpan sebelumnya dapat segera ditemukan oleh rekan-rekan yang berpartisipasi. Dalam *Blockchain*, penambang adalah aktor utama utama yang memverifikasi validitas data yang disimpan. Kasus penggunaan yang terintegrasi dengan IoT telah meningkatkan perhatian yang tinggi dalam dekade terakhir, karena pemantauan rantai pasokan, pemantauan lingkungan, kota pintar, industri pintar, dan perawatan kesehatan berfokus pada kekekalan data dan membutuhkan sistem IoT untuk pengukuran, pengumpulan data, dan kontrol aktif. Dengan demikian, maka integrasi *Bockchain* dan IoT ke dalam aplikasi yang mendukung BIoT menanggapi tuntutan penyimpanan yang persisten dan data sangat aman, di mana pengumpulan data otomatis menjadi kunci untuk menawarkan transparansi dan keandalan. Peran aplikasi BIoT yang sangat menuntut membutuhkan elaborasi dan analisis protokol IoT yang mendasari, yang membentuk dasar komunikasi untuk sistem IoT. Dengan demikian, studi tentang jangkauan komunikasi, kecepatan data, *maximum transmission units* (MTU), keandalan protokol komunikasi dan efisiensi energi diperlukan untuk mendukung dengan tepat Penerapan IoT.

* + 1. **Algoritma *Consensus***

Algoritma *consensus* adalah sebuah teknik untuk mencapai sebuah kesepatan Bersama di dalam sebuah kelompok. Seperti sebuah kelompok yang terdiri dari sepuluh *node* yang perlu menentukan pilihan tentang tugas yang menguntungkan mereka semua. Semuanya dapat mengusulkan sebuah pemikiran, namun yang dominan dominan akan disetujui oleh salah satu yang paling mendorong mereka yang paling mendorong mereka. Yang lain perlu mengelola pilihan ini dalam hal apa pun. Namun, perhitungan konsensus tidak hanya setuju dengan bagian yang dominan memberikan suara, namun juga menyetujui yang menguntungkan semua pihak. Konsensus *Blockchain* adalah strategi untuk membuat keseragaman dan kesopanan di dunia *online*. Kerangka kerja konsensus yang digunakan untuk ini pemahaman ini dikenal sebagai hipotesis *consensus* (Pahlajani dkk., 2019). *Blockchain* menerapkan beberapa algoritma consensus seperti berikut :

1. *Proof of Work* (PoW)

*Proof of Work* (PoW) adalah strategi konsensus yang digunakan pada Bitcoin. Jika sebuah *node* ingin mencatat sebuah blok, banyak usaha yang harus dilakukan oleh *node* tersebut untuk membuktikan bahwa *node* tersebut tidak memiliki keinginan untuk menyerang jaringan *blockchain* yang ada, hal ini yang mendasari cara kerja konsensus ini. Konsensus ini membutuhkan nilai *hash* yang dihitung tersebut untuk sama dengan atau lebih kecil dari nilai yang telah ditentukan sebelumnya. Ketika salah satu *node* dalam jaringan berhasil mencapai nilai yang ditentukan, maka blok tersebut akan disebarkan ke jaringan dan semua *node* dalam jaringan masing-masing mengkonfirmasi kebenaran nilai *hash* itu, dan setelah itu blok dinyatakan valid. Setelah itu semua *node* harus menambahkan blok ini ke *blockchain* mereka. *Nodes* yang menghitung nilai *hash* ini disebut dengan *miners* dan proses pengerjaan PoW ini disebut *mining* dalam Bitcoin (Frankenfield, 2019).

1. *Proof of Stake* (PoS)

*Proof of Work* (PoW) adalah strategi konsensus yang digunakan pada Bitcoin. Jika sebuah *node* ingin mencatat sebuah blok, banyak usaha yang harus dilakukan oleh *node* tersebut untuk membuktikan bahwa *node* tersebut tidak memiliki keinginan untuk menyerang jaringan *blockchain* yang ada, hal ini yang mendasari cara kerja konsensus ini. Konsensus ini membutuhkan nilai *hash* yang dihitung tersebut untuk sama dengan atau lebih kecil dari nilai yang telah ditentukan sebelumnya. Ketika salah satu *node* dalam jaringan berhasil mencapai nilai yang ditentukan, maka blok tersebut akan disebarkan ke jaringan dan semua *node* dalam jaringan masing-masing mengkonfirmasi kebenaran nilai *hash* itu, dan setelah itu blok dinyatakan valid. Setelah itu semua *node* harus menambahkan blok ini ke *blockchain* mereka. *Nodes* yang menghitung nilai *hash* ini disebut dengan *miners* dan proses pengerjaan PoW ini disebut *mining* dalam Bitcoin (Frankenfield, 2019).

* + 1. **Kriptografi**

Teknologi kriptografi adalah kemampuan untuk bertukar pesan yang hanya dapat dibaca oleh penerima yang dituju dan digunakan untuk beberapa tujuan untuk mengamankan berbagai transaksi yang terjadi di jaringan, untuk mengontrol pembuatan unit mata uang baru, dan untuk verifikasi transfer aset digital dan token.Mata uang digital meniru konsep tanda tangan dunia nyata dengan menggunakan teknik kriptografi dan kunci enkripsi. Metode kriptografi menggunakan kode matematika tingkat lanjut untuk menyimpan dan mengirimkan nilai data dalam format yang aman yang memastikan hanya mereka yang memiliki data atau transaksi tersebut yang dapat menerima, membaca, dan memproses data, serta memastikan keaslian transaksi dan partisipan, seperti halnya tanda tangan di dunia nyata.

Pada teknologi *blockchain* kriptografi menggunakan metode *Hashing*, yang digunakan untuk memverifikasi integritas data transaksi di jaringan secara efisien. *Hashing* menjaga struktur data *blockchain*, mengkodekan alamat akun seseorang, merupakan bagian integral dari proses enkripsi transaksi yang terjadi antar akun, dan memungkinkan penambangan blok. Selain itu, tanda tangan digital melengkapi berbagai proses kriptografi ini, dengan mengizinkan partisipan asli untuk membuktikan identitas mereka ke jaringan (Seth, 2022).

* + 1. **MultiChain**

Multichain adalah platform yang membantu pengguna untuk membangun *Blockchain* pribadi tertentu yang dapat digunakan oleh organisasi untuk transaksi. API sederhana yang disediakan MultiChain membantu untuk mengatur rantai. Tujuan MultiChain membuat visibilitas *blockchain* harus selalu secara aktif disimpan dalam peserta yang dipilih untuk menghindari kebingungan untuk memastikan stabilitas dan kontrol atas transaksi, dan proses penambangan (*mining*) dapat dilakukan dengan lebih aman. Model *blockchain* ini hanya mentransaksikan akun yang divalidasi ke peserta rantai ini. Dalam MultiChain terdapat Proses *hand-shaking* dimana terjadi ketika *node* dalam *blockchain* terhubung satu sama lain. MultiChain terjadi ketika dua *node blockchain* terhubung. Identitas setiap *node* mewakili dirinya sendiri dengan alamat dengan daftar izin. Oleh karena itu, setiap *node* yang diwakilinya mengirimkan pesan ke pengguna lain. Koneksi *Peer to Peer* (P2P) dibatalkan jika mereka tidak menerima hasil yang memuaskan dari proses tersebut.

* + 1. **Socket Programming**

asaadakdadadadaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

**BAB III**

**METODE PENELITIAN**

1. **Alur Pengerjaan Tugas Akhir**

Perancangan alur dari pengerjaan tugas akhir ini merupakan gambaran umum dari alur penelitian yang akan dilakukan dalam pengerjaan tugas akhir mulai dari awal hingga akhir. Alur pengerjaan tugas akhir digambarkan seperti berikut:



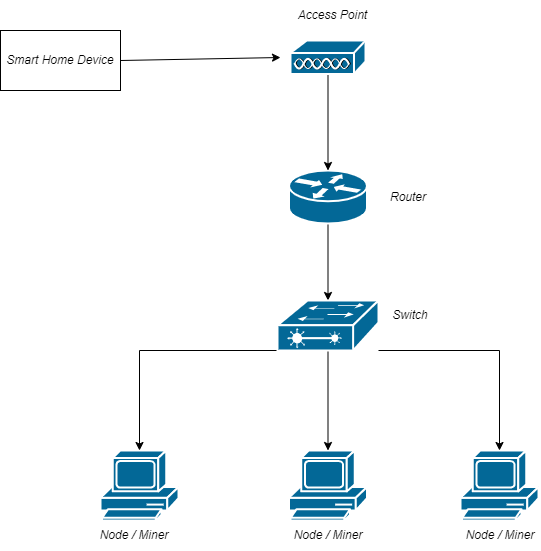
Gambar 3.1 Diagram Alir Pengerjaan Tugas Akhir

1. **Uraian Metodelogi** 
   * 1. **Studi Literatur**

Pada penelitian ini dilakukan studi literatur sebagai tahap awalan untuk melakukan penelitian, tujuan dari studi literatur ini adalah untuk memahami dasar teori dan konsep yang akan menjadi pendukung dalam melakukan penelitian yang berjudul ”Implementasi *Blockchain* Sebagai Sistem Keamanan IoT dalam Mengirim, Mendistribuskan dan Privasi Data”.

* + 1. **Topologi Jaringan**

Pada penelitian ini menggunakan topologi jaringan, yaitu terdapat *access point* untuk mejadi jaringan local antara perangkat *smart home* dengan PC (*node* / *miner*) serta terdapat 3 *node* yang dapat berperan sebagai *miner* dan saling terhubung antara *node* yang satu dengan *node* yang lain. Perangkat *smart home* yang akan disimulasikan dalam bentuk program *Python* yang akan mengirimkan data kepada PC yang berperan sebagai miner. Topologi jaringan yang dibuat dapat dilihat pada Gambar 3.2 berikut ini :



Gambar 3.2 Topologi Jaringan

PC berperan sebagai *node* dalam jaringan dan dapat juga berperan sebagai *miner*. *Miner* bertanggung jawab untuk melakukan pengecekan dan validasi terhadap aktivitas yang terjadi di dalam sistem, misalnya *smart home devices* yang hendak mengirimkan dan menyimpan data ke dalam sistem apakah diizinkan atau tidak dan apakah data yang dikirimkan merupakan data yang valid atau tidak. Penelitian ini menggunakan platform MultiChain yang akan dipasang pada semua *node* yang terdapat di dalam sistem.

* + 1. **Perangkat *Smart Home***

Pada penelitian ini dilakukan pembuatan perangkat *smart home* berbasis program yang dimana pembuatan program menggunakan Bahasa *python*. *Smart Home* berbasis program ini akan dijalankan dengan tujuan untuk dapat mengirimkan data ke *node admin* yang kemudian akan diproses dan akan didistribusikan ke blockchain apabila data sudah di dicek dan divalidasi.

* + 1. ***Node Admin***

Berdasarkan Gambar.3.2 terdapat tiga *node* yang dimana akan dipilih satu *node* yang akan berperan sebagai *node admin*. *Node admin* akan berperan untuk menginisiasi *blockchain*, seperti memberi izin *node* yang diperbolehkan untuk terhubung ke dalam *blockchain*, memberi izin *node* untuk melakukan *mining* ke dalam *blockchain*, menjalankan sebuah program yang berfungsi sebagai penguhubung antara *blockchain* pada MultiChain dengan perangkat *Smart Home* berbasis program yang akan mengirimkan paket data kemudian meneruskannya ke dalam *blockchain*. Untuk dapat menerima paket yang dikirim dari perangkat *smart home* perlu dibuat jalur komunikasi dengan menggunakan metode *socket programming* yang berfungsi sebagai penghubung antara *node admin* dengan perangkat *smart home* berbasis program *python* tersebut.

* + 1. **Rancangan Pengiriman Data**

Data atau pesan dikirimkan dari perangkat *smart home* yang telah dihubungkan dengan *node admin*. Perangkat *smart home* yang disimulasikan dengan menggunakan program Python mengirimkan data kepada *node admin*. Setelah terhubung, perangkat *smart home* dapat mengirim data ke *node* MultiChain menggunakan *socket*. Data akan diserialisasi menjadi format yang sesuai .JSON atau format khusus, lalu kirim data melalui koneksi socket yang sudah dibuat. Dengan menggunakan perintah send() untuk mengirim data melalui *socket*. Data yang dikirimkan akan memilki waktu jeda tiap pengiriman data adalah 25 detik karena harus menunggu proses mining dari *blockchain* terlebih dahulu.

* + 1. **Rancangan Penerimaan Data**

Data yang telah dikirim oleh perangkat *smart home* kemudian akan diterima oleh sebuah program yang dijalankan pada *node admin*. Program ini memiliki fungsi untuk menerima data yang dikirim oleh perangkat *smart home* kemudian meneruskannya kepada platform MultiChain.

* + 1. **Koneksi dengan MultiChain**

Setelah pesan atau data diterima oleh *node admin*, kemudian data akan diteruskannya ke dalam *blockchain* dengan menggunakan API yang telah disediakan oleh MultiChain sehingga pesan tesebut dapat disimpan ke dalam *blockchain*. Untuk dapat berkomunikasi dengan API milik MultiChain dengan menggunakan bahasa pemrogaman *python*, maka dapat memanfaatkan library Savoir.

* + 1. **Penyimpanan Data**

Setelah terhubung dengan API milik MultiChain, maka untuk selanjutnya data dapat diterima dan disimpan ke dalam *blockchain*. Proses penyimpanan data disebut dengan proses *create*. Data yang telah diterima dan masih dalam format hexadecimal akan diteruskan ke dalam *blockchain* untuk disimpan ke dalam blok baru. MultiChain memiliki fitur *stream* yang berfungsi sebagai tempat untuk menyimpan data secara umum, dan istilah menyimpan data di dalam *stream* dikenal dengan istilah *publish*.

* + 1. **Validasi Data**

Ada dua jenis media yang akan mencoba mengirimkan data ke dalam *blockchain* yaitu *permissioned device* dan *permissionless device*. *Permissioned devices* adalah perangkat yang diizinkan oleh sistem untuk menyimpan dan melihat data. Sedangkan *permissionless devices* adalah perangkat yang berada di dalam maupun di luar sistem yang tidak memiliki izin apapun untuk melakukan aktivitas yang sama seperti *permissioned devices*.

**DAFTAR PUSTAKA**

Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P. (2017). Blockchain for IoT security dan privacy: The case study of a smart home, diakses tgl bln thn.

J. Frankenfield, 2019, “Proof of Work”: Investopedia, 28 june 2020. [online]. Available:https://www.investopedia.com/terms/p/proof-work.asp#:~:text=Proof%20of%20work%20describes%20a,launching%20denial%20of%20service%20attacks.

J. Frankenfield, 2019, “ Proof of Stake” Invetopedia, 11 Agustus 2019. [online]. Available:https://www.investopedia.com/terms/p/proof-of-stake-pos.asp.

Hayes, A., (2023). Blockchain Fact: What is it, how it works, and how it can be used. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp#what-is-blockchain

Khan, M.A., Salah, K., (2018). IoT Security: Review, blockchain solution, and open challenges. Future generation computer system, idem

Mingyu, H,, Tianyu, K., & Li, G., (2020). A Blockchain Based Architecture for IoT Data Sharing Systems. Jurnal Beijing University of Posts and Telecommunications Key Lab of Universal Wireless Communications, Ministry of Education.

Panarello A, Tapas N, Merlino G, Longo F, Puliafito A, 2018, Blockchain and IoT integration: A systematic survey. Sensors (Switzerland), idem

Rumah. (2023). [online]. Apa itu MulthiChain di Blockchain. Artikel rumah. Available:https://id.tishijie.com/10609/Apa\_itu\_MultiChain\_di\_blockchain\_

Schiller, E., Niya, S. R., Surbeck, T., & Stiller, B. (2019). Scalable Transport Mechanisms for Blockchain IoT Applications. 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium). downloaded on 2020-06-01

Seth, S., (2022) Explained Crypto in Cryptocurrence. [online]. Available: https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

Skarmeta AF, Hernandez-Ramos JL, Moreno MV, 2014, A decentralize approach for security and privacy challenges in the Internet of Things, idem