**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 Stake* adalah protokol yang lebih ramah energi dibandingkan dengan *Proof of Work* (PoW). *Miner* dalam PoS harus membuktikan kepemilikan dengan memiliki sejumlah uang (*cryptocurrency* yang dibuat pada *blockchain* tertentu). Pemilihan dengan melihat jumlah saldo cukup tidak adil karena orang yang paling kaya di jaringan tersebut akan mendominasi. Oleh karena itu, terdapat beberapa solusi yang diajukan untuk mengombinasi jumlah saldo dan hal lain untuk menambah blok baru pada jaringan. Contoh, pada *blockchain*, dimana membuat blok selanjutnya akan diacak dengan menggunakan rumus yang mencari nilai *hash* uang paling kecil lalu dikombinasikan dengan saldo orang tersebut (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

