Implementasi *Private Blockchain* Menggunakan Multichain Sebagai Sistem Keamanan Data IoT

Lalu Ocky Saktiya Luhung [1], Misbahuddin [1] Giri Wahyu Wiriasto [1]
[1]Jurusan Teknik Elektro – Universitas Mataram, Jalan Majapahit 62, Kota Mataram - 82115, Indonesia

ARTICLE INFO

Article history (8 pt):

Received
Revised
Accepted

Keywords (8 pt):

Blockchain
Internet of Things(IoT)
Private Blockchain;
Hashing
Multichain

ABSTRACT

Integrasi teknologi blockchain dengan Internet of Things (IoT) untuk meningkatkan keamanan dan privasi data menjadi solusi yang semakin relevan di era digital. Dengan fokus pada keamanan IoT saat mendistribusikan data, risiko manipulasi data dapat dikurangi karena blockchain memungkinkan struktur terdesentralisasi dan terenkripsi. Integritas data ditingkatkan melalui verifikasi transaksi dan penyimpanan data yang diotorisasi dengan hash value dan bukti transaksi (txid). Penggunaan jaringan private blockchain mengontrol akses data, meningkatkan keamanan, privasi, dan memastikan akses terbatas pada pihak yang diizinkan.Percobaan dilakukan dan didapatkan nilai kemungkinan komulatif berdasarkan jumlah block dengan nilai kemungkinan komulatif dihasilkan dari nilai block yang bertambah setiap 15 detik sampai mendapatkan jumlah 6 konfirmasi dari prinsip blockchain sehingga suatu block dinyatakan valid dalam jaringan blockchain, yang mengartikan setelah block ditambahkan ke rantai dibutuhkan 6 block tambahan untuk memastikan keamanan transaksi. Kemudian didapatkan juga nilai kemungkinan komulatif berdasarkan jumlah waktu yang dibutuhkan membuat block di dalam blockchain, dengan nilai kemungkinan komulatif dihasilkan dari nilai block yang bertambah setiap 15 detik sampai mendapatkan jumlah 6 konfirmasi dari prinsip blockchain sehingga suatu block dinyatakan valid dalam jaringan blockchain. Kemudian hingga suatu block dinyatakan valid saat waktu mencapai 60 detik sampai 165 detik. Hasilnya menunjukkan bahwa blockchain dapat meningkatkan keamanan data IoT serta menjaga integritas data dengan lebih baik, memperkuat otorisasi, dan mengontrol akses data secara lebih selektif

corresponding Author:

Lalu Ocky Saktiya, Jurusan Teknik Elektro – Universitas Mataram, Jalan Majapahit 62, Kota Mataram – 83115, Indonesia
Email: laluocky450@gmail.com

1. INTRODUCTION

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[14].

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 terdapat 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, terdistribusi 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* [13]. Algoritma *Proof of work* adalah algoritma yang paling banyak digunakan. Algoritma ini digunakan oleh mata uang kripto seperti bitcoin dan ethereum, masing-masing memiliki perbedaan tersendiri. Algoritma PoW digunakan untuk mengkonfirmasi transaksi dan menghasilkan *block* baru di *blockchain* [10]. *Blockchain* menampilkan *database* yang terdesentralisasi dan tidak dapat rusak yang memiliki potensi tinggi untuk beragam penggunaan. *Blockchain* adalah *database* terdistribusi yang banyak digunakan untuk mencatat transaksi yang berbeda, setiap data yang dimasukkan akan di-*encrypt* sehingga tidak memudahkan orang lain untuk memanipulasi dan menggandakan sertifikat tersebut. Setelah konsensus tercapai di antara *node* yang berbeda, transaksi ditambahkan ke *block* yang sudah menyimpan catatan beberapa transaksi. Setiap *block* berisi nilai *hash* dari pasangan terakhirnya untuk koneksi sehingga *node* menjaga *database* bersama-sama. Di bawah *blockchain*, sebuah *block* menjadi tervalidasi hanya setelah diverifikasi oleh banyak pihak. Selain itu, data dalam *block* tidak dapat dimodifikasi secara sewenang-wenang [8]. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [2]. 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 *hash* ing 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 [13].

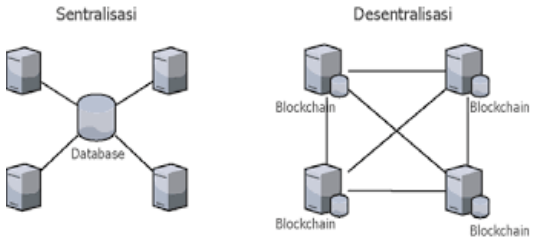
1. Internet of Things *(IoT)*

Internet of Things (IoT), merupakan sebuah konsep yang bertujuan untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus menerus 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.Misalnya sebuah *Smart Home* yang dapat dikelola lewat *smartphone* dengan bantuan koneksi internet. Pada dasarnya IoT bila mendapatkan sambungan internet sebagai media komunikasi dan *server* sebagai pengumpul informasi yang diterima untuk dianalisa [6].

Dalam IoT, asosiasi dari berbagai perangkat heterogen mengurangi kemampuan jaringan sumber daya, yang menarik perhatian para peneliti ke arah bidang yang sedang berkembang ini.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 [20].

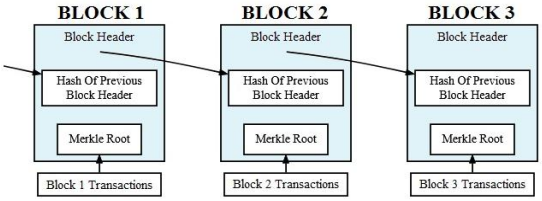
2. Blockchain

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.



Gambar 1. Blockchain dan Database

Gambar 1 merupakan gambaran perbedaan aatara penyimpanan yang bersifat sentralisasi yang digunakan pada *database* dan penyimpanan yang bersifat desentralisasi yang didigunakan pada *blockchain*. *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 [9]. *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 2 dibawah ini [17].



Gambar 2. Struktur Blockchain

Blockchain

Public Blockchain (*Blockchain* Publik) memungkinkan setiap orang untuk bisa bergabung. Sebagaimana namanya, publik, *Blockchain* ini ditujukan untuk umum/publik. *Blockchain* ini terbuka untuk semua orang, di mana setiap orang bisa menjadi simpul (*node*), bisa membaca, menulis dan melakukan *update* pada *blockchain* dengan membuat alamat pribadi (*personal address*)-nya sendiri. Dengan menggunakan kunci pribadi (*private key*) yang telah diubah menjadi kunci publik (*public key*) memungkinkan siapa saja yang memiliki koneksi internet dan perangkat komputasi yang bisa menjalankan perangkat lunak *Blockchain* untuk dapat berpartisipasi [21]. *Private Blockchain* (*Blockchain* Pribadi), pemilik *Blockchain* memiliki pengaruh yang signifikan terhadap desain dan operasi selanjutnya [21]. *Private Blockchain* adalah jenis *Blockchain* yang bersifat tertutup dan bertujuan untuk melakukan pertukaran informasi secara internal saja, sehingga pihak-pihak yang tidak bergabung tidak dapat melihat proses-proses apa saja yang dilakukan pada *Blockchain* tersebut [4]. Dalam tipe ini, jika ada yang ingin menjadi *node*, mereka harus mendapatkan ijin dari otoritas (pemilik) *Blockchain* [21].

Algoritma Consensus

Algoritma *consensus* adalah sebuah teknik untuk mencapai sebuah kesepatan bersama di dalam sebuah kelompok. 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* [15]. *Blockchain* menerapkan beberapa algoritma *consensus* seperti berikut :

Proof of Work

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. *Node*s yang menghitung nilai *hash* ini disebut dengan *miners* dan proses pengerjaan PoW ini disebut *mining* dalam Bitcoin [11].

Proof of Stake

Proof of Stake (PoS) 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 [12].

Raspberry Pi

Raspberry Pi adalah sebuah komputer kecil yang mumpuni yang memiliki ukuran sebesar kartu ATM. Perangkat ini dapat digunakan untuk proyek elektronik karena memiliki input, output, port digital dan dapat melakukan banyak hal layaknya PC desktop atau komputer. *Raspberry Pi* dapat menghubungkannya ke TV atau layar komputer dan keyboard. *Raspberry Pi* dibuat di Inggris oleh *Raspberry Pi Foundation* [7]. *Raspberry Pi* tidak menggunakan hard disk, namun menggunakan SD Card untuk proses booting dan penyimpanan data jangka-panjang. *Raspberry Pi* memiliki beberapa tipe, yaitu Model A dan Model B, dengan perbedaan spesifikasi seperti harga, SoC, CPU, GPU, RAM, dan lain-lain.[22] Pada penelitian ini, menggunakan *Raspberry Pi* 3 Model B [7].

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 [18].

Related Work

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 *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 [5].

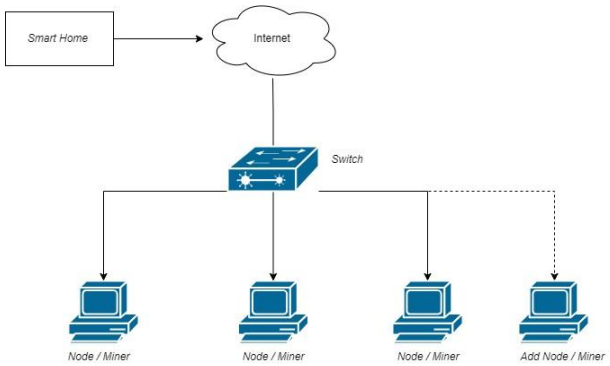
Penelitian kedua, *Blockchain* Technology *Implementation in Raspberry Pi for Private Network*. Penelitian ini mencoba membuktikan perangkat komputer yang murah seperti komputer mini dapat digunakan dalam pengembangan teknologi *blockchain*. Teknologi komputer mini digunakan karena banyaknya permasalahan yang terjadi akibat penggunaan sumber daya perangkat keras yang dibahas besar, penelitian ini menggunakan desain eksperimental. Eksperimen dilakukan dengan perangkat yang digunakan dan teknologi *blockchain*. Perangkat yang digunakan adalah komputer mini *Raspberry Pi*, dan teknologi *blockchain* adalah platform Ethereum. Hasil dari penelitian ini menunjukkan proses instalasi hingga sistem *blockchain* dapat berjalan. Hasil penelitian ditunjukkan dengan grafik evaluasi performa yang menunjukkan parameter *commulative probability* akan meningkat apabila *block number* bertambah [7].

Penelitian ketiga, *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 [1].

2. METHOD

Pada penelitian ini menggunakan topologi jaringan, yaitu terdapat jaringan internet untuk mejadi jaringan lokal 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 dijalankan pada perangkat *Raspberry Pi* yang akan mengirimkan data kepada PC yang berperan sebagai *miner*.

Topologi Jaringan

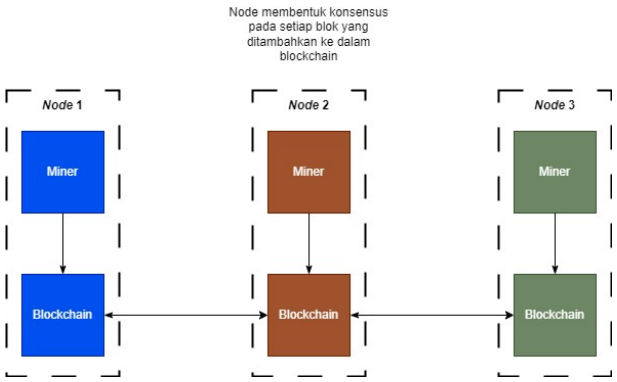


Gambar 3. Topologi Jaringan

Gambar 3 merupakan topologi jaringan yang membentuk topologi star dimana pada topologi tersebut 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.

Alur Komunikasi Blockchain

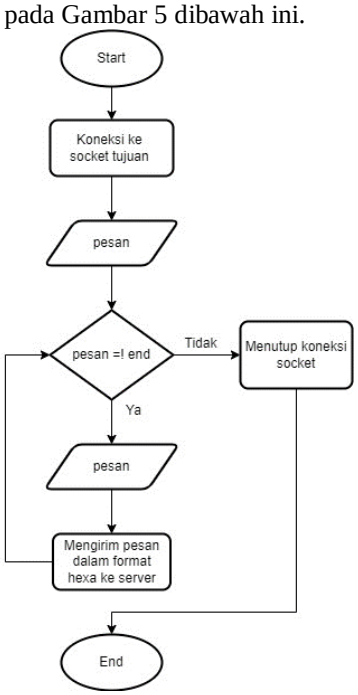


Gambar 4. Alur Komunikasi *Blockchain*

Gambar 4 merupakan alur komunikasi *blockchain* yang terjadi pada 3 buah node. Peran *node* dan *miner* dalam jaringan *blockchain* yaitu *node* dapat saling berkomunikasi dengan sesama *node* karena sudah terjadi koneksi secara *peer-to-peer* antar node, dimana masing-masing *node* terdapat *miner* untuk memvalidasi transaksi dan menambahkan ke blok baru ke dalam *blockchain*.

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 pada perangkat *Raspberry Pi* 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 kemudian digambarkan dengan diagram alir seperti pada Gambar 5 dibawah ini.



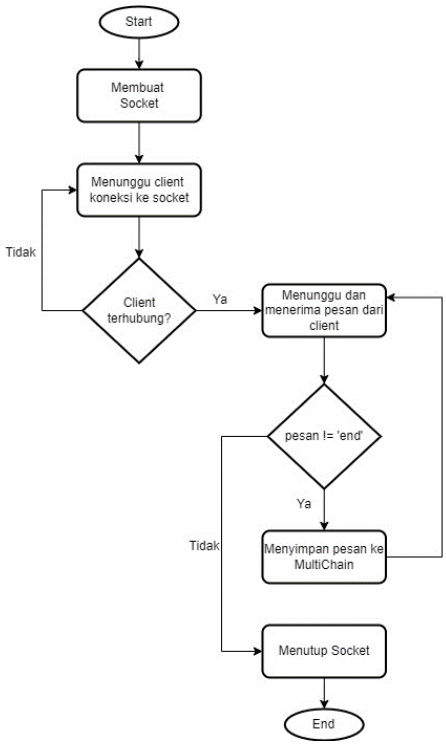
Gambar 5. Diagram Alir Perangkat Smart Home

Pengiriman Data

Data atau pesan dikirimkan dari perangkat *Smart Home* yang telah dihubungkan dengan *node* admin kemudian perangkat *Smart Home* akan disimulasikan dengan menggunakan program Python pada pernagkat *Raspberry Pi* yang mengirimkan data kepada program server pada *node* admin. Setelah terhubung, perangkat *Smart Home* dapat mengirim data ke *node* Multichain menggunakan *socket*. Data akan diserialisasi menjadi format yang sesuai *Hexadesimal* atau format khusus, lalu kirim data melalui koneksi *socket* yang sudah dibuat. Data yang dikirimkan akan memilki waktu jeda tiap pengiriman data adalah 25 detik karena harus menunggu proses *mining* dari *blockchain* terlebih dahulu.

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 Multichain kemudian digambarkan dengan diagram alir seperti pada Gambar 6 dibawah ini.



Gambar 6. Alur Penerimaan Data

3. Penyimpanan Data

Setelah terhubung dengan API milik Multichain, maka untuk selanjutnya data dapat diterima dan disimpan ke dalam *blockchain*. Data yang telah diterima dan masih dalam format *hexadesimal* 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* .

4. Proses Validasi

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

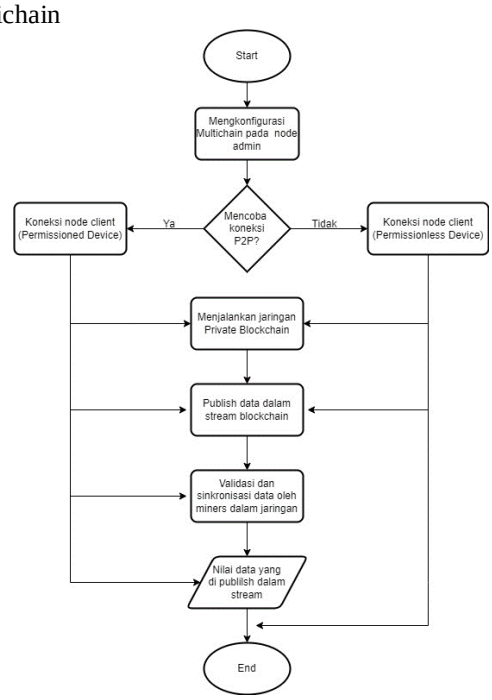
Proses validasi data dalam Bitcoin biasa disebut dengan proses *mining*. Bitcoin menggunakan konsep yang bernama PoW (*Proof of Work*). Proses vaidasi didalam multichain menggunakan skema kombinasi

antara jumlah *miner* dengan parameter bernama *mining-diversity* yang dibatasi dengan $0 \leq$ *mining diversity* ≤ 1. *Miner* adalah sebutan untuk komputer atau *node* yang bertugas untuk melakukan proses validasi data pada *blockchain*.

1. Menerapkan semua perubahan izin yang ditentukan oleh transaksi dalam blok secara berurutan.
2. Menghitung jumlah *miner* yang diizinkan yang ditentukan setelah menerapkan perubahan, misalkan jumlah *miner* adalah 2.
3. Mencari nilai *spacing* degan mengkalikan jumlah *miner* dengan nilai *mining-diversity*. Misalkan nilai *mining*-diversity = 0.3, maka diperoleh nilai *spacing* = 2 x 0.3 = 0.6. Kemudian nilai 0.6 dibulatkan ke atas menjadi 1 sehingga nilai spacing yang sebenarnya adalah 1.
4. Jika *miner* dari *block* ini telah melakukan validasi pada salah satu dari (nilai *spacing* -1) *block* sebelum ini, maka proses validasi tidak sah. Jika tidak, maka *miner* yang bersangkutan akan didelegasikan untuk melukukan proses validasi pada *block* tersebut dan *block* akan dianggap valid dan dapat disimpan ke dalam *blockchain*.

Skema ini memberlakukan teknik penjadwalan *round-robin*, dimana *miner* yang diizinkan harus membuat block secara bergiliran untuk menghasilkan *blockchain* yang valid. Parameter *mining-diversity* mendefinisikan ketatnya skema Nilai 1 pada *mining-diversity* memastikan bahwa setiap *miner* akan masuk ke dalam rotasi round-robin, sedangkan nilai 0 menunjukkan tidak ada batasan sama sekali. Secara umum nilai yang lebih tinggi akan lebih aman, namun nilai yang terlalu dekat dengan 1 dapat menyebabkan *blockchain* membeku jika beberapa *miner* menjadi tidak aktif.

- Diagram alir Pengujian Multichain



Gambar 7. Diagram Alir Pengujian

3. RESULTS AND DISCUSSION

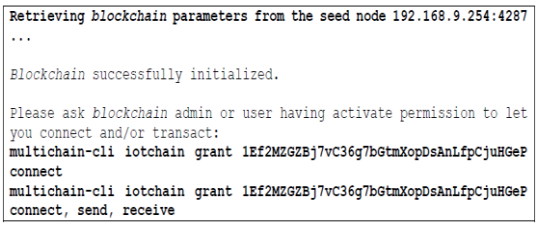
Langkah peratama pada implementasi ini adalah melakukan konfigurasi dan instalasi Multichain pada setiap *node*. Kemudian diatur 1 *node* sebagai *server* atau *node* admin dan *node* lainnya disebut sebagai *node client* yang kemudian *node client* akan dibedakan perannya yaitu sebagai *permissioned device* dan *permissionless device*. Multichain diinstal pada komputer yang berjalan dengan *operation system* (OS) menggunakan Ubuntu 22.0.4.

5. *Skenario Permissioned Device*

Koneksi antar *node* didalam jaringan *private blockchain* dapat terjadi dengan proses koneksi menggunakan mekanisme *hand shaking*, dimana *node* yang ingin terhubung (*Client*) akan diberi alamat

secara khusus, alamat tersebut digunakan untuk terhubung dengan *node* yang kemudian akan memberikan *permission* (admin).

1. Koneksi oleh *Node Client*



Gambar 8. Koneksi *Node Client*

Gambar 8 merupakan *node client* yang mencoba terhubung dengan jaringan *private blockchain* harus mendapatkan *permission*s oleh *Node* admin terlebih dahulu. Seperti yang terlihat dimana terdapat aksi yang dapat dilakukan *Node Client* dapat berupa *connect, send, receive*.

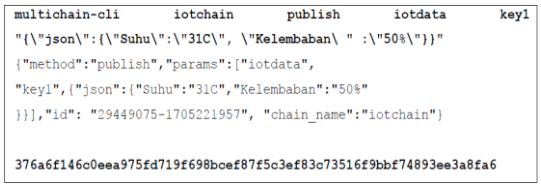
2. Pemberian Izin oleh *Node* Admin

Gambar 9. Pemberian Izin *Node* Admin

Gambar 9 merupakan proses pemberian izin oleh *node* admin kepada *node client* unutk melakukan koneksi *peer-to-peer* dan diikuti dengan perintah *grant* alamat dari *node client*, yang digunakan untuk memberikan *permission* agar *node client* dapat tergabung dalam jaringan *private blockchain* yang dikelola dan segala aksinya diatur oleh *node* admin.

Kemudian terdapat *public key* yang didapatkan dari pemberian *permission* oleh *node* admin dan menandakan proses koneksi *peer-to-peer* anatar *node* admin dan *node client* telah berhasil.

3. *Publish* Data



Gambar 10. *Publish* Data

Gambar 10 merupakan proses *publish* data ke dalam *stream* yang dilakukkan oleh *node* admin dengan menggunakan mode *write*, yang berarti dilakukan *input* data secara langsung dengan CLI pada terminal.

Kemudian didapatkan nilai txid dari proses *publish* data tersebut. Nilai txid diberikan sebagai bukti transaksi data pada setiap proses *publish* data ke dalam *stream* didalam *blockchain*.

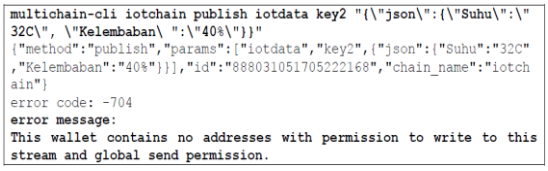
4. Melihat Data

Gambar 11. Detail Data

Gambar 11 merupakan proses melihat data yang telah di *publish* sebelumnya pada *node* admin yang kemudian dijalakan dengan perintah *multichain-cli iotchain liststreamitems iotdata*.

Didapatkan detail item yang disimpan didalam *stream* dengan *publishers* adalah alamat dari *node* admin dan jumlah *confirmation* dari aksi *publish* data ditampilkan untuk mengathui jumlah validasi pada saat proses *publish* data berlangsung beserta nilai txid yang didapatkan sesuai dengan yang diberikan pada saat proses *publish* data.

5. *Publish* Data oleh *Node Client*



Gambar 12. *Publish* Data *Node Client*

Gambar 12 merupakan aksi *publish* data pada *node client* yang ditampilkan adalah *node client* tidak dapat menyimpan data pada *stream* karena belum memiliki *permission* untuk melakukan *publish* data ke dalam *stream*. *Error massage* yang didapatkan menunjukkan bahwa alamat (*node client*) pada saat menyimpan data tidak terdapat alamat untuk disertakan sebagai bukti bahwa memiliki izin pada penyimpanan data pada *streams.*

6. *Permissions Node* Admin

Gambar 13. *Permissions Node* Admin

Gambar 13 merupakan proses pemberian izin pada *node* admin kepada *node client* agar dapat melakukan *publish* data kedalam *stream* dengan dijalankan perintah *multichain-cli blockchain*_name *grant node_client*_address *send*, dimana diberi *permissions* agar *node client* dapat melakukan *send* data ke dalam *stream*.

Kemudian pada baris kedua dijalankan perintah *multichain-cli blockchain_name grant node_client*_address *iotdata.write* untuk *node client* dapat melakukan *publish* data dengan mode *write* ke dalam *stream* iotdata. Keduanya diikuti dengan nilai *hash* dari proses pemberian izin oleh *node* admin.

7. Melihat Data *Node Client*

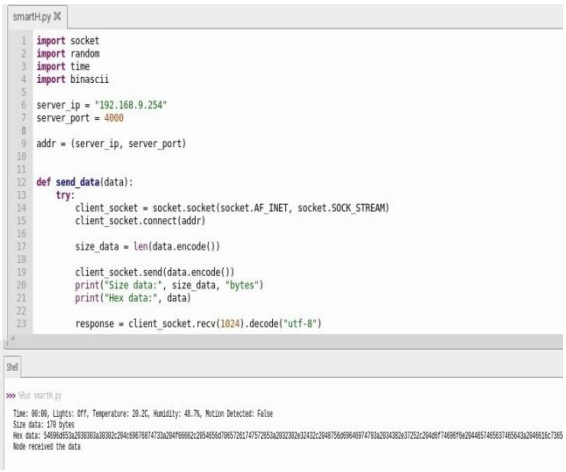
```
multichain-cli iotchain liststreamitems iotdata
{"method":"liststreamitems","params":["iotdata"],"id":"50650521-
1705222323","chain_name":"iotchain"}
{
"publishers" : ["1Ef2MZGZBj7vC36g7bGtmXopDsAnLfpCjuHGeP"
"keys" : ["key2"
"offchain" : false,
"available" : true,
"data" : {
"json" : {
"Suhu" : "32C",
"Kelembaban" : "40%"
}
},
"confirmations" : 3,
"blocktime" : 1705222279,
"txid":"432650340bc94bce322b070d491368326a0772567d201b69f42782c6bded
0dbf"
}
```

Gambar 14. Detail Data *Node Client*

Gambar 14 merupakan proses *subscribe* yang dilakukan oleh *node client* pada *stream node* admin dengan menjalankan perintah *multichain-cli blockchain_name subcribe iotdata* oleh *node client* agar dapat melihat detail item pada *stream.*

Kemudian dilakukan proses mencari detail *items* oleh *node client* dengan menjalankan perintah *multichain-cli blockchain_name liststreamitems iotdata* dan dengan kode *key2* yang merupakan hasil *publish* oleh *node client*. Terlihat publishers adalah alamat dari *node client* dan jumlah *confirmation* dari aksi *publish* data ditampilkan untuk mengathui jumlah validasi pada saat proses *publish* data berlangsung.

8. Pengiriman Data *Smart Home*

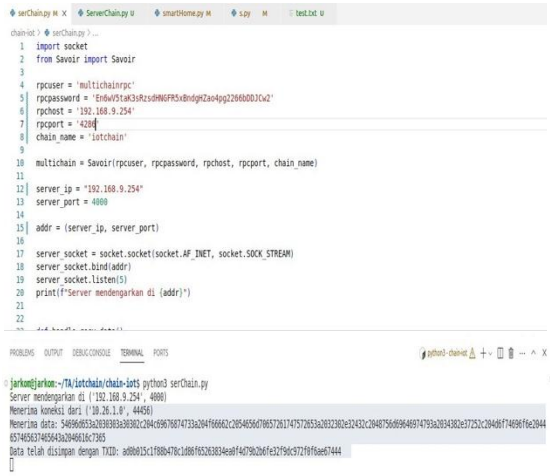


Gambar 15. Pengiriman Data *Samrt Home*

Gambar 15 merupakan program simulasi yang bertindak sebagai klien yang dijalankan pada perangkat *Raspberry Pi*. Simulasi program akan terhubung dengan program *server* dengan digunakan socket programming yang memberi nilai alamat IP dan Port dari program *server*.

Proses simulasi *Smart Home* diatur dengan data akan dikirim ke program *server* dengan *time.sleep(3600)* atau dikirim setiap jam. *Output* dari simulasi program *Smart Home* yang akan dikirim ke program *server* dimana nilai asli dari simulasi diubah terlebih dahulu kedalam format *hexadecimal* agar dapat disimpan oleh program *server* ke dalam multichain.

9. Penerimaan Data *Smart Home*



Gambar 16. Penerimaan Data *Smart Home*

Gambar 16 merupakan program *server* yang akan menerima koneksi socket dari klien untuk mendapat data hasil simulasi hasil program *Smart Home* kemudian akan dilakukan proses *publish* data ke dalam *stream* pada *node* admin.

Hasil dari program *server* yang menerima koneksi dengan program klien dan menerima data hasil simulasi dari program *Smart Home* yang nilai asli data telah di konversi kedalam format *hexadecimal*, kemudian akan di *publish* dalam stream pada multichain dengan diberi nilai txid data yang tersimpan ke dalam *stream* multichain.

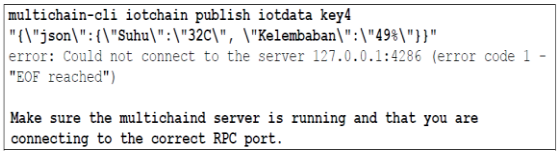
10. Melihat Data *Smart Home*

Gambar 17. Detail Data dalam *Blockchain*

Gambar 17 merupakan pencarian data atau atau detail items hasil dari simulasi *Smart Home* yang disimpan melalui program *server* yang melakukan *publish* data ke dalam *stream* pada multichain. Nilai data yang sudah dikonversi ke dalam format *hexadecimal* dengan nilai txid yang didapatkan bernilai sama seperti pada Gambar 16 dan data diberikan juga keterangan *timestamp*.

6. *Skenario* Permissionless Device

1. *Publish* Data



Gambar 18. Gagal Menyimpan Data

Gambar 18 merupakan aksi *Permissionless device* mencoba *publish* data pada multichain dengan menjalankan perintah *multichain-cli blockchain_name publish Streams_name key_value data_value* dan

didapatkan *error: Could not connect to the server* karena *permission*less *device* tidak dapat terhubung dengan *server* multichain tetapi melakukan penyimpanan data.

2. Melihat Data

```
multichain-cli iotchain liststreamitems iotdata true 1
error: Could not connect to the server 127.0.0.1:4286 (error code 1
- "EOF reached")

Make sure the multichaind server is running and that you are
connecting to the correct RPC port.
```

Gambar 19. Gagal Melihat Data

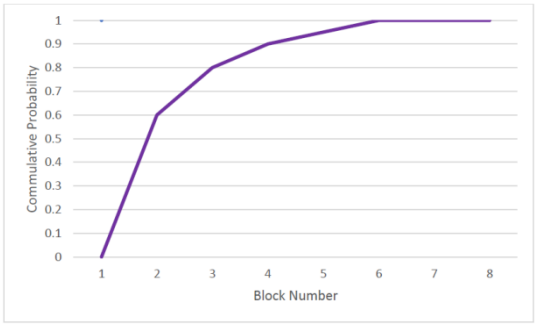
Gambar 19 merupakan aksi *Permissionless device* mencoba mendapatkan detail item dari percobaan *permissionless device* saat menyimpan data dengan menjalankan perintah *multichain-cli blockchain_name liststreamitems* dan didapatkan *error: Could not connect to the server* karena *permissionless device* tidak dapat terhubung dengan *server* multichain tetapi mencoba melakukan pencarian detail item.

7. Validasi Data

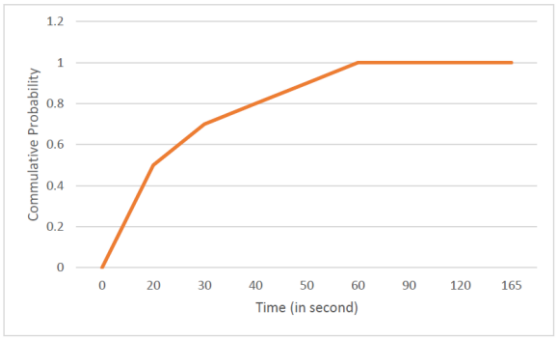
Validasi data mengacu pada proses pemberian izin *node client* untuk melakukan *mining* oleh *node* admin agar jaringan *private blockchain* yang berjalan pada sisi *node client* tidak mengalami pembekuan atau data dan jumlah *block* pada kedua *node* tidak sinkron serta tidak dapat lagi menyimpan data ke dalam stream pada jaringan *private blockchain*. Proses validasi didasarkan pada nilai *spacing* yang harus dipenuhi dengan mengkombinasikan nilai parameter *mining*-diversity dan jumlah *miners* atau nilai *spacing* = *mining-diversity*miners* .

8. Evaluasi Sistem

Evaluasi kinerja dilakukan untuk dapat mengetahui nilai yang dapat dihasilkan oleh *blockchain* yang diimplementasikan pada proses distribusi data IoT kedalam jaringan *private blockchain* dengan menggunakan platform multichain dan didapatkan nilai kemungkinan komulatif berdasarkan jumlah *block number* yang dihasilkan didalam *blockchain*.



Gambar 20. *Commulative Probability* Terhadap *Block Number*



Gambar 21. *Commulative Probability* Terhadap *Time*

Nilai kemungkinan komulatif (*commulative probability*) berdasarkan jumlah *block* pada Gambar 20 tampak dengan nilai kemungkinan komulatif (*commulative probability*) dihasilkan dari nilai *block* yang bertambah setiap 15 detik sampai mendapatkan jumlah 6 konfirmasi dari prinsip *blockchain* sehingga suatu *block* dinyatakan valid dalam jaringan *blockchain*, yang mengartikan setelah *block* ditambahkan ke rantai dibutuhkan 6 *block* tambahan untuk memastikan keamanan transaksi. Kemudian didapatkan nilai kemungkinan komulatif (*commulative probability*) berdasarkan jumlah waktu pada Gambar 21 tampak yang dibutuhkan membuat *block* didalam *blockchain*, dengan nilai kemungkinan komulatif dihasilkan dari nilai *block* yang bertambah setiap 15 detik sampai mendapatkan jumlah 6 konfirmasi dari prinsip *blockchain* sehingga suatu *block* dinyatakan valid dalam jaringan *blockchain*. Kemudian hingga suatu *block* dinyatakan valid saat waktu mencapai 60 detik sampai 165 detik.

4. CONCLUSION

Implementasi *blockchain* sebagai sistem keamanan IoT dalam mendistribusikan dan menjaga privasi data mampu memberikan hasil pengamanan data berupa *block* yang berisi *hash block*, *miner*, *confirmation*, *previous block hash* dan *next block hash* serta *timestamp* dan masing-masing *block* saling terhubung. Hal ini membuktikan bahwa implementasi blockchain mampu menjaga keamanan dan privasi data pada saat melalui proses distribusi oleh perangkat IoT hingga sampai pada akhirnya data disimpan. Dari hasil pengujian yang dilakukan waktu dan pembuatan *block* yang membutuhkan waktu 15 detik dalam setiap pembuatan block serta dibersamai dengan proses validasi yang dilakukan saat membuat *block* hingga mendapatkan jumlah 6 konfirmasi yang sesuai dengan prinsip *blockchain* sehingga *block* dinyatakan valid dalam jaringan *blockchain*.

Acknowledgments

Diucapkan terimakasih pada Laboratorium Teknik Komputer Jurusan Teknik Elektro Universitas Mataram atas peminjaman perangkat penelitian.

2. REFERENCES (10 PT)

[1] S. R. Lam, S. Jain, and R. Doriya, (2021). Security threats and solutions to IoT using *Blockchain*: A review.Proccedings – 5th Internasional Conference on Intelligent Computing and Control System, ICICCS 2021.

[2] A. Amrulloh, E. Ujianto, (2019), *Kripto Simetris Menggunakan Algoritma Vigenere Cipher*. Jurnal CoreIT, Vol. 5, No. 2

[3] K. Andersson, LCN Symposium 2019 : 2019 IEEE 44th Local Computer Networks Symposium on Emerging Topics in Networking : Proceedings : 14 October 2019, Osnabrück, Germany.

[4] D. A. Badawi, 2019. "Investigasi Forensik Digital Berbasis Teknologi *Blockchain*." Universitas Islam Indonesia. https: // dspace.uii.ac.id/handle/123456789/16982%0Ahttps://dspace.uii.ac.id /bitstream/handle/123456789/16982/08. naskah publikasi .pdf?sequence=11&isAllowed=y.

[5] A. Dorri, S.S Kanhere, R. Jurdak, P. Gauravaram, (2017). *Blockchain* for IoT security dan privacy: The case study of a *Smart Home*, IEEE International Conference on Pervasive Computing and Communications 15. 2017 Kona, Hawaii et al. 2017 IEEE International Conference on Pervasive Computing and Communications.

[6] Y. Efendi,. 2018. "*Internet of Things* (Iot) Sistem Pengendalian Lampu Menggunakan *Raspberry Pi* Berbasis Mobile." Jurnal Ilmiah Ilmu Komputer 4(2): 21–27.

[7] E. Fernando, Meyliana, and Surjandy. 2019. "*Blockchain* Technology Implementation in *Raspberry Pi* for *Private* Network." Proceedings of 2019 4th International Conference on Sustainable Information Engineering and Technology, SIET 2019: 154–58.

[8] R. Hargude, R., Ashutosh, Ghule., A. Nawale, S. Adshure, (2021), "Verification and Validation of Certificate Using Blockchain". International Journal of Engineering Research & Technology, Departemen Komputer India, Vol.6

[9] A. Hayes, (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*

[10] Husni., (2019), *Mengenal Blockchain: Teknologi dibelakang Bitcoin*. WordPress. Tersedia di : https://komputasi.files.wordpress.com/2019/05/husni-mengenal-*blockchain*-teknologi-di-belakang-bitcoin.pdf, diakses 18 April 2023.

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

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

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

[14] R. V. Nesterenko dan M. A. Maslova (2022). Menggunakan Teknologi *Blockchain* Untuk Memastikan Keamanan. Jurnal Nasional Teknologi Komputer Vol. 2: No:1 ; Januari 2022. E-ISSN: 2808-4845; P-ISSN: 2808-7801.

[15] S. Pahlajani, K. Avinash, and P. Vinod, "Algorithms." 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT): 1–6.

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

[17] R. Premkumar, and S. P. Sathya. 2021. "A *Blockchain* Based Framework for IoT Security." In Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021, Institute of Electrical and Electronics Engineers Inc., 409–13.

[18] Rumah. (2023). [online]. Apa itu MulthiChain di *Blockchain*. Artikel rumah. Available:https://id.tishijie.com/10609/Apa_itu_MultiChain_di_*blockchain*.

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

[20] U. Ikram, 2019. "The Internet of Things: A Review of Enabled Technologies and Future Challenges." IEEE Access 7: 7606–40.

[21] T. P. Utomo, 2022. "Implementasi Teknologi *Blockchain* Di Perpustakaan: Peluang, Tantangan Dan Hambatan." Buletin Perpustakaan 4(2): 173–200.

[22] I. D. Wijaya, N. Usman., and M. A. Barata, (2018)."Implementasi *Raspberry Pi* Untuk Rancang Bangun Sistem Keamanan Pintu Ruang *Server* Dengan Pengenalan Wajah Menggunakan Metode *Triangle Face*".