Implementasi Multichain sebagai Alternatif Solusi Keamanan dan Privasi Data pada Komunikasi Perangkat Pintar Rumah

Dimas Yoan Rizaldi[1], Ibnu Febry Kurniawan[2],

[1] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]dimasrizaldi@mhs.unesa.ac.id
[2]ibnukurniawan@unesa.ac.id

***Abstrak*— IoT berkembang dengan cepat dan diperkirakan akan tumbuh hingga 26 miliar perangkat di tahun 2020. Keamanan dan privasi dianggap sebagai hambatan utama agar paradigma IoT dapat diterima secara penuh. Keterbatasan pada perangkat IoT dan jaringan juga mengakibatkan sulitnya menerapkan solusi keamanan yang ada secara langsung, khususnya protokol keamanan tradisional dan kriptografi primitif yang membutuhkan banyak memori dan sumber daya komputer. Pada penelitian ini menerapkan teknologi yang menopang sistem *cryptocurrency* bitcoin yaitu *blockchain*, untuk memberikan keamanan dan privasi data pada arsitektur IoT dalam konteks *smart home*. Jenis *blockchain* yang digunakan adalah *private blockchain* dengan menggunakan *platform* MultiChain. Dengan menggunakan MultiChain maka hanya perangkat yang memiliki izin saja yang dapat bergabung ke dalam jaringan *blockchain*. Dari pengujian yang telah dilakukan didapatkan hasil bahwa teknologi *private blockchain* dapat diterapkan dengan baik dengan menggunakan *platform* MultiChain. Hasil dari pengujian keamanan menunjukkan bahwa *permissionless device* tidak dapat menyimpan data ke dalam *blockchain* ataupun mencari dan membaca data yang berasal dari dalam *blockchain* tanpa seizin *node admin* baik melalui API yang dimiliki MultiChain atau melalui aplikasi yang bertindak sebagai perangkat *smart home* yang mengirimkan data sehingga data di dalam *blockchain* menjadi aman dan kerahasiaannya terjaga.**

***Kata Kunci*— *Blockchain*, *Smart Home*, Keamanan, Privasi, *Internet of Things*.**

I. PENDAHULUAN

Semakin banyak inovasi baru yang muncul guna memudahkan pekerjaan manusia, khususnya di bidang teknologi jaringan dan komputer. *Internet of Things* (IoT) menggambarkan salah satu teknologi yang paling menyita perhatian abad ini. Hal tersebut merupakan sebuah evolusi alami dari *Internet (of computers)* menuju *embedded and cyber-physical systems* [1]. *Smart Home* merupakan bagian dari IoT. *Smart Home* merupakan istilah untuk rumah yang menjadi semakin "pintar" karena didorong oleh munculnya peralatan yang terhubung ke *internet*. Hal ini memungkinkan konsumen untuk memantau dan mengelola lingkungan rumah mereka dari jarak jauh misalnya mengunci atau membuka kunci pintu, alarm asap dapat mengingatkan ponsel anda ketika kebakaran terdeteksi, dan sistem pencahayaan dapat dikontrol dari jarak jauh. Survei di AS menunjukkan bahwa keamanan pribadi atau keluarga, perlindungan properti, manajemen pencahayaan / energi, dan pemantauan hewan peliharaan sebagai motivasi utama untuk menggunakan perangkat *smart home*, dengan 51% dari mereka yang disurvei bersedia membayar lebih dari $ 500 untuk perangkat *smart home* yang lengkap [2].

Keamanan dan privasi data pada lingkungan IoT perlu diperhatikan karena IoT terdiri dari perangkat yang menghasilkan, memproses, dan bertukar sejumlah besar data keamanan dan kritis terhadap keselamatan serta informasi sensitif yang sifatnya pribadi, dan karenanya merupakan target menarik dari berbagai serangan *cyber* [3]. Perangkat IoT semakin dilengkapi dengan sensor dan aktuator yang meningkatkan masalah privasi dan keamanan pada skala yang belum pernah terjadi sebelumnya [2]. Keamanan dan privasi dianggap sebagai hambatan utama agar paradigma IoT dapat diterima secara penuh. Di dunia masa depan dengan miliaran perangkat heterogen, area ini perlu ditangani dengan baik agar manfaat yang berasal dari lingkungan baru ini dapat dimanfaatkan dengan baik oleh manusia. Sementara dalam *internet* yang sekarang ini ada banyak sekali teknologi dan protokol standar untuk mengatasi banyak ancaman keamanan yang menghadang, namun keterbatasan pada perangkat IoT dan jaringan juga mengakibatkan sulitnya menerapkan solusi keamanan yang ada secara langsung. Khususnya, protokol keamanan tradisional dan kriptografi primitif membutuhkan banyak memori dan sumber daya komputer [4].

Teknologi *blockchain* telah diramalkan oleh industri dan komunitas penelitian sebagai teknologi yang sangat menyita perhatian yang siap memainkan peran utama dalam mengelola, mengendalikan, dan yang paling penting mengamankan perangkat IoT [5]. Sebuah catatan data publik yang tidak dapat diubah yang diamankan oleh peserta jaringan *peer-to-peer* disebut dengan *Blockchain* (BC) yang termasuk teknologi utama dibalik *Bitcoin*. BC terdiri dari blok-blok yang saling terikat bersama seperti rantai dan berfungsi sebagai buku kas induk [1]. Pada dasarnya *blockchain* adalah buku besar basis data yang terdesentralisasi, 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*. 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 keamanannya, dan diretas. Mereka juga dapat berbuat jahat dan berperilaku korup di masa depan, meskipun mereka dapat dipercaya sekarang [5].

Menggunakan *blockchain* saja yang merupakan teknologi utama dibalik Bitcoin pada lingkungan IoT tidaklah cukup dikarenakan masih memiliki kekurangan dalam hal privasi dan proses *mining* yang membutuhkan sumber daya yang tinggi. Sesuai desain, semua transaksi bitcoin dapat dilihat oleh semua peserta di dalam jaringan bitcoin sehingga para partisipan menanggung risiko identitas mereka dapat terungkap pada beberapa titik di masa depan [6]. *Blockchain* dapat dikategorikan ke dalam dua jenis berdasarkan fungsinya: *permissionless* dan *permissioned*. Sebuah *permissioned blockchain* membatasi aktor yang dapat berpartisipasi dalam konsensus dari sistem. Dalam *permissioned blockchain*, hanya beberapa pengguna saja yang memiliki hak untuk memvalidasi transaksi [7]. MultiChain merupakan sebuah *platform* untuk pembuatan dan penyebaran *blockchain* pribadi, baik di dalam atau di antara organisasi. MultiChain memecahkan masalah terkait *mining*, privasi, dan keterbukaan melalui pengelolaan izin pengguna yang terintegrasi. Terdapat 3 tujuan inti dari MultiChain, yaitu memastikan bahwa aktivitas *blockchain* hanya dapat dilihat oleh peserta yang dipilih, memperkenalkan kontrol atas transaksi yang diizinkan, memungkinkan penambangan berlangsung secara aman tanpa *proof of work* dan biaya terkait [6].

Studi ini melakukan implementasi *platform* Multichain pada konteks komunikasi IoT perangkat pintar rumah. Perangkat pintar rumah yang mengirimkan data ke *blockchain* akan disimulasikan dengan menggunakan program Python. Ada 2 jenis media yang akan mencoba untuk melakukan proses penyimpanan dan pencarian data yaitu *permissioned device* dan *permissionless device.* Dilakukan evaluasi keamanan mengenai privasi data pada *blockchain* dengan membandingkan hasil dari *permissioned device* dan *permissionless device* ketika melakukan proses penyimpanan dan pencarian data.

Pada artikel ini fokus membahas pada rancang bangun sistem MultiChain di lingkungan perangkat pintar rumah. Pada bab 2 akan membahas penelitian yang relevan untuk mengetahui penelitian ini dengan penilitian yang sudah pernah dilakukan oleh orang lain sebelumnya. Selanjutnya pada bab 3 metodologi penelitian yang membahas tentang rancangan yang digunakan untuk melakukan penelitian ini. Kemudian, rancangan eksperimen dan hasil akan dibahas secara berurutan pada bab 4 dan 5.

II. PENELITIAN RELEVAN

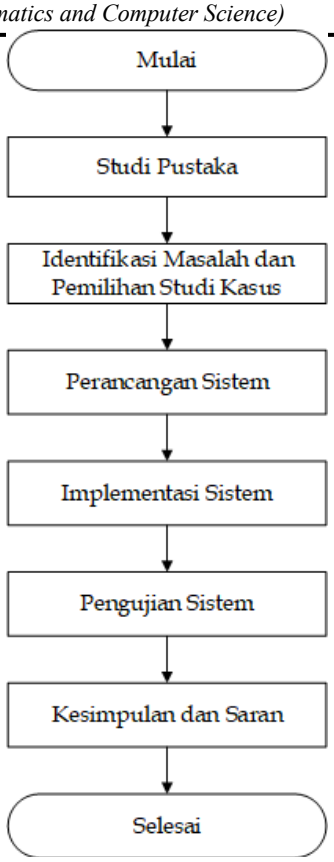
Penelitian mengenai keamanan dan privasi IoT pernah dilakukan oleh Hannes Gross, dkk pada tahun 2015 dengan judul "*Privacy-Aware Authentication in the Internet of Things*". Pada penelitian tersebut, peneliti menunjukkan bahwa keamanan dan privasi dalam IoT dapat dicapai tanpa protokol hak milik dan berdasarkan standar *internet* yang ada. Protokol otentikasi dengan pembatasan yang diberlakukan oleh standar IPsec dan TLS diterapkan untuk mengatasi masalah privasi. Tetapi, metode tersebut menghasilkan proses komputasi yang besar sehingga kurang cocok untuk peralatan IoT yang mayoritas memiliki sumber daya yang terbatas.

Penggunaan *blockchain* untuk *Internet of Things* pernah diteliti oleh Ali Dorri, dkk pada tahun 2016 dalam jurnal yang berjudul "*Blockchain in Internet of Things: Challenges and Solutions*". Peneliti mengusulkan arsitektur baru yang aman, pribadi, dan ringan untuk IoT berdasarkan teknologi *blockchain* dengan menghilangkan *overhead* yang dihasilkan *blockchain* sambil mempertahankan sebagian besar keuntungan keamanan dan privasi yang dihasilkan oleh *blockchain*. Peneliti menggunakan konteks *smart home* sebagai media pengujian metode yang diusulkan. Arsitektur yang diusulkan bersifat hierarki, terdiri atas *smart home, overlay network,* dan *cloud storages,* serta pada tiap tingkatan tersebut menggunakan jenis *blockchain* yang berbeda. Namun, pada jurnal tersebut peneliti hanya menyajikan hasil analisis kualitatif yang menunjukkan bahwa arsitektur yang dirancang peneliti memiliki performa keseluruhan kinerja pemrosesan yang konstan dalam keadaan terbaiknya.

Sedangkan pada Maret 2017 dalam jurnal "*Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*", peneliti menggali lebih dalam lagi dan menguraikan berbagai komponen inti dan fungsi dari tingkat *smart home* serta menyajikan hasil simulasi dari arsitektur yang diusulkan dengan menggunakan Cooja simulator. Dalam simulasinya, peneliti membandingkan hasil pemrosesan dari metode yang diusulkan dengan skenario lain yang tanpa menggunakan enkripsi, *hashing*, dan *blockchain.* Peneliti mensimulasikan tiga sensor z1 mote (yang meniru perilaku perangkat *smart home*) yang mengirim data langsung ke *home miner* setiap 10 detik. Setiap simulasi berlangsung selama 3 menit dan hasil yang disajikan dirata-rata selama durasi tersebut. Ada 3 hal yang dievaluasi oleh peneliti yaitu *packet overhead, time overhead,* dan *energy comsumption*.

III. METODOLOGI PENELITIAN

Berikut ini merupakan alur jalannya penelitian untuk melakukan penelitian "Impelementasi Multichain sebagai Alternatif Solusi Keamanan dan Privasi Data pada Komunikasi Perangkat Pintar Rumah" :



Gbr. 1 Alur Proses Penelitian

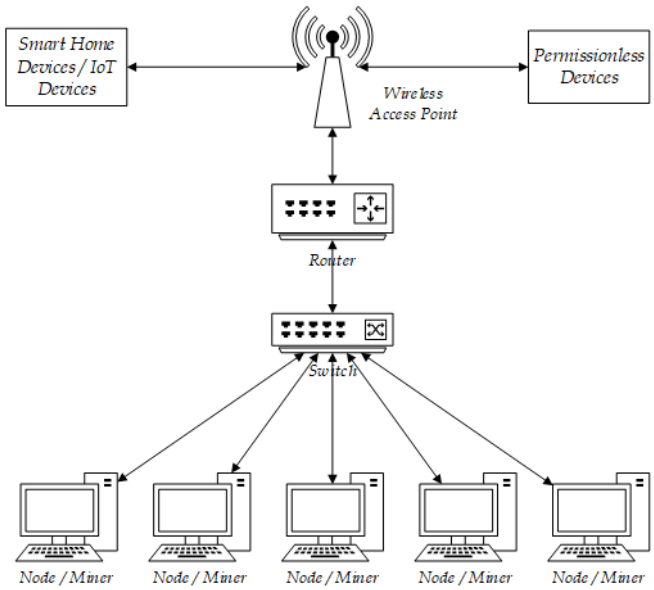
Penelitian yang telah dilakukan membahas mengenai implementasi *private blockchain* untuk keamanan dan privasi data *smart home*. Tahapan yang dilakukan pertama kali adalah melakukan studi pustaka untuk mendapatkan referensi mengenai penggunaan *platform* MultiChain, definisi *Internet of Things,* dan penggunaan *blockchain* untuk *Internet of Things* yang tepat. Kemudian melakukan identifikasi masalah dan pemilihan studi kasus untuk mengetahui masalah yang terjadi pada bidang teknologi *private blockchain* dan bagaimana keamanan data yang dihasilkan sistem pada studi kasus yang dipilih yaitu penerapan teknologi *private blockchain* pada IoT *smart home*. Pada tahap perancangan sistem yaitu penelitian ini menggunakan skema topologi jaringan yang sederhana yaitu terdapat beberapa *node* yang dapat berperan sebagai *miner* dan saling terhubung antara *node* yang satu dengan *node* yang lain, serta peralatan *smart home*. Selanjutnya yaitu implementasi sistem akan disimulasikan dalam bentuk program Python yang akan mengirimkan data kepada PC yang berperan sebagai *miner.* Pada tahap pengujian sistem dilakukan pada uji keamanan yang bertujuan untuk menganalisis keamanan sistem. Tahap terakhir adalah menarik kesimpulan atas apa yang telah dilakukan dan saran yang dibutuhkan dalam penelitian selanjutnya.

IV. RANCANGAN EKSPERIMEN

Pada penelitian ini akan membahas mengenai penggunaan *private blockchain* untuk keamanan dan privasi data *smart home*. Dengan menggunakan *platform* MultiChain, maka akan dilakukan implementasi teknologi *private blockchain* pada IoT *smart home*, simulasi perangkat *smart home* berbasis program, serta evaluasi keamanan data yang dihasilkan oleh sistem.

A. Skema Jaringan

Pada Penelitian ini menggunakan skema topologi jaringan yang sederhana, yaitu terdapat beberapa *node* yang dapat berperan sebagai *miner* dan saling terhubung antara *node* yang satu dengan *node* yang lain, serta peralatan *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 Gbr. 2 berikut ini :



Gbr. 2 Rancangan Topologi Jaringan

Ada dua jenis media yang akan mencoba mengirimkan data ke dalam *blockchain* yaitu *permissioned device* dan *permissionless device. Permissioned devices* adalah peralatan yang diizinkan oleh sistem untuk menyimpan dan melihat data. Sedangkan *permissionless devices* adalah peralatan yang berada di dalam maupun di luar sistem yang tidak memiliki izin apapun untuk melakukan aktivitas yang sama seperti *permissioned devices.* PC yang berperan sebagai *nodes* dalam jaringan dapat juga berperan sebagai *miner. Miner* bertanggung jawab untuk melakukan pengecekan dan validasi terhadap aktivitas yang terjadi di dalam sistem, misalnya sebuah *smart home devices* ada 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.

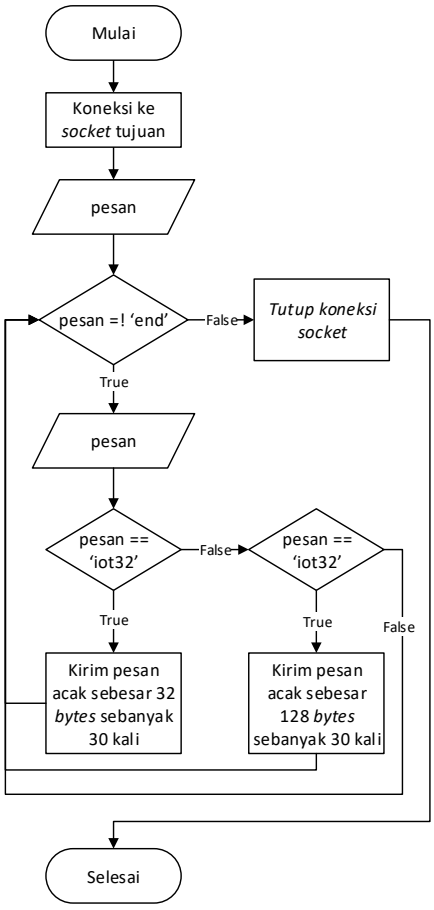
B. Node Admin

Hal pertama yang dilakukan adalah memilih satu *node* dari kelima komputer atau *node* yang digunakan dalam sistem sebagai *node admin*, dan komputer selain *node admin* akan disebut sebagai *node client.* Tugas dari *node admin* adalah

menginisiasi *blockchain,* mengatur nilai *mining diversity* pada *blockchain,* memberi izin *node* yang diperbolehkan untuk terhubung ke dalam *blockchain,* memberi izin *node* yang diperbolehkan untuk *mining* ke dalam *blockchain,* menjalankan sebuah program yang berfungsi sebagai penghubung antara *blockchain* pada MultiChain dengan perangkat *smart home* yaitu menerima paket data yang dikirim oleh perangkat *smart home* kemudian meneruskannya ke dalam *blockchain*. Untuk dapat menerima paket data yang dikirim oleh perangkat *smart home*, maka perlu dibuat jalur komunikasi dengan menggunakan teknik *socket programming* yang berfungsi sebagai penghubung antara *node admin* dengan perangkat *smart home*.

C. Perangkat Smart Home

Kemudian untuk perangkat *smart home* pada penelitian ini akan disimulasikan dengan munggunakan program Python yang akan dijalankan pada laptop dengan processor Intel core i3-5005U, CPU @ 2.00GHz (4 CPUs), RAM 4 GB, OS Windows 10 Home Single Language 64-bit. Perangkat *smart home* memiliki tugas untuk mengirimkan data atau pesan kepada *node admin*. Diagram alir dari program tersebut dapat dilihat pada Gbr. 3 :



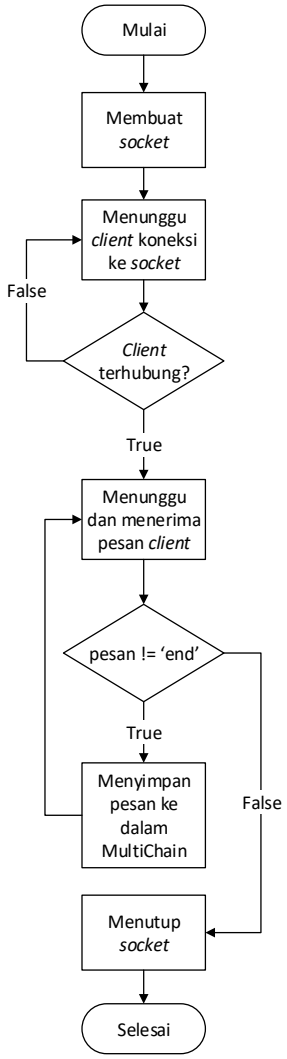
Gbr. 3 Diagram Alir Simulasi Perangkat Smart Home

D. 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*. Data yang dikirimkan berbentuk kalimat acak atau *random string* dengan dua jenis besaran data yaitu 32 *bytes* dan 128 *bytes*. Untuk mengirim pesan atau data dengan besaran 32 *bytes* maka pengguna harus mengetikkan "iot32" pada *input field* program dan menekan tombol *enter*, sedangkan untuk mengirim data atau pesan dengan ukuran 128 *bytes* maka pengguna harus mengetikkan "iot128" pada *input field* program. Data akan dikirimkan sebanyak 30 kali dengan waktu jeda tiap pengiriman data adalah 25 detik karena harus menunggu proses *mining* dari *blockchain* terlebih dahulu.

E. 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.



Gbr. 3 Diagram Alir Proses Penerimaan Data

F. Koneksi ke MultiChain API

Setelah pesan atau data diterima oleh *node admin*, maka tahap selanjutnya adalah meneruskannya 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*.

G. Penyimpanan Data

Setelah terhubung dengan API milik MultiChain, maka untuk selanjutnya data dapat diterima dan disimpan ke dalam *blockchain*. Poses penyimpanan data dalam laporan ini untuk seterusnya 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*.

H. Proses Validasi Data

Proses validasi data (dalam Bitcoin biasa disebut dengan proses *mining*) yang dilakukan oleh MultiChain berbeda dengan yang dilakukan oleh Bitcoin. Bitcoin menggunakan konsep yang bernama PoW (*Proof of Work)*, sedangkan 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*. *Miner* di dalam MultiChain dipilih secara acak. Proses validasi data dapat dijelaskan seperti berikut :

1. Menerapkan semua perubahan izin yang ditentukan oleh transaksi dalam blok secara berurutan.
2. Menghitung jumlah *miner* yang diizinkan yang ditentukan setelah menerapkan perubahan itu, misalkan jumlah *miner* = 2.
3. Mencari nilai *spacing* dengan mengalikan 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 blok ini telah melakukan validasi pada salah satu dari (nilai *spacing – 1*) blok sebelum ini, maka proses validasi tidak sah. Jika tidak, maka *miner* yang bersangkutan akan didelegasikan untuk melakukan proses validasi pada blok tersebut dan blok akan dianggap valid dan dapat disimpan ke dalam *blockchain*.

Skema ini memberlakukan teknik penjadwalan *round-robin*, di mana *miner* yang diizinkan harus membuat blok 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.

V. HASIL DAN PEMBAHASAN

A. Hasil Evaluasi Keamanan

Tahapan pengujian keamanan dalam penelitian ini dilakukan dengan cara membandingkan hasil dari proses penyimpanan data dan pencarian data dengan menggunakan *permissionless device* dan *permissioned device. Permissionless device* adalah perangkat komputer atau sejenisnya yang berada di dalam satu jaringan dengan MultiChain namun tidak mendapatkan izin dari *node admin* untuk menjadi *node client* atau bagian dari jaringan MultiChain. Tiap proses pengujian akan dilakukan dengan 2 skema pengujian. Skema pertama mengasumsikan bahwa *permissionless device* telah terhubung dengan jaringan yang sama dimana *blockchain* dijalankan namun belum mendapatkan izin oleh *node admin* untuk dapat terhubung ke dalam *blockchain*. Skema kedua adalah mencoba melakukan proses penyimpanan data dan pencarian data melalui level aplikasi yaitu mengirimkan perintah kepada *node admin* dengan cara menyamar sebagai perangkat *smart home* yang disimulasikan oleh program Python.

1) Hasil Proses Penyimpanan Data: Agar dapat melakukan penyimpanan data maka sebuah *node client* harus mendapatkan izin terlebih dahulu oleh *node admin* untuk dapat tersambung dengan *blockchain,* dan juga setelah itu harus mendapatkan izin untuk melakukan penyimpanan data dari *node admin* sehingga ada dua buah izin yang harus didapatkan terlebih dahulu. Gbr. 4 menunjukkan tampilan *node client* yang telah mendapatkan izin untuk tersambung ke dalam *blockchain* :

```
C:\Windows\System32\cmd.exe - multichaind iotchain1@10.60.101.164:2689
Microsoft Windows [Version 10.0.17134.1006]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichaind iotchain1@10.60
.101.164:2689
MultiChain 2.0.2 Daemon (Community Edition, latest protocol
20010)
Chain iotchain1 already exists, adding 10.60.101.164:2689 to
list of peers
Other nodes can connect to this node using:
multichaind iotchain1@10.60.101.163:2689

Listening for API requests on port 2688 (local only - see rp
callowip setting)

Node ready.
```

Gbr. 4 Node Client Terhubung dengan Blockchain

Gbr. 5 menunjukkan hasil dari usaha dari *permissionless device* yang berusaha untuk tersambung dengan *blockchain* :

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichaind iotchain1@10.60.
101.164:2689

MultiChain 2.0.2 Daemon (Community Edition, latest protocol
20010)

Retrieving blockchain parameters from the seed node 10.60.10
1.164:2689 ...
Blockchain successfully initialized.

Please ask blockchain admin or user having activate permissi
on to let you connect and/or transact:
multichain-cli iotchain1 grant 1DN4q11UHc7fLRCW4PEYLofLoJdF2
mKigHckDq connect
multichain-cli iotchain1 grant 1DN4q11UHc7fLRCW4PEYLofLoJdF2
mKigHckDq connect,send,receive
```

Gbr. 5 Permissionless Device Mencoba Terhubung dengan Blockchain

Dari Gbr. 5 dapat dijelaskan bahwa *permissionless device* tidak dapat tersambung ke dalam *blockchain* karena *node admin* belum memberikan izin. Kemudian dilakukan proses penyimpanan data dari *node client* yang telah mendapatkan izin untuk terhubung ke dalam jaringan *blockchain* namun belum mendapatkan izin untuk melakukan penyimpanan data oleh *node admin* dan hasilnya dapat dilihat pada Gbr. 6 :

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.1006]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 publish
 datasuhu key1 "{\"json\":{\"suhu:20C\"}}"
{"method":"publish","params":["datasuhu","key1","{\"json\":{\"su
hu:20C\"}}"],"id":"76040833-1573559234","chain_name":"iotchain1"
}

error code: -704
error message:
This wallet contains no addresses with permission to write to th
is stream and global send permission.
```

Gbr. 6 Node Client Belum Mendapatkan Izin

Terlihat bahwa *node client* tidak dapat menyimpan data karena tidak mendapatkan izin dari *node admin.* Kemudian dilakukan proses pemberian izin oleh *node admin* yang ditunjukkan oleh Gbr.7 :

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 grant 1R
GLcjo7BujQjJZ8yu8swpwdBy2GyEoee1aw2H send
{"method":"grant","params":["1RGLcjo7BujQjJZ8yu8swpwdBy2GyEoee1aw
2H","send"],"id":"22403942-1573559424","chain_name":"iotchain1"}

3030303b7852312447e5b897a266347e1646a9e54d08b458f621e3ba6438e651

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 grant 1R
GLcjo7BujQjJZ8yu8swpwdBy2GyEoee1aw2H datasuhu.write
{"method":"grant","params":["1RGLcjo7BujQjJZ8yu8swpwdBy2GyEoee1aw
2H","datasuhu.write"],"id":"91592455-1573559439","chain_name":"io
tchain1"}

79a8aff633a091de610ff93b2fd2598e250ee984b4945767c690c0a9dc955906
```

Gbr. 7 Proses Pemberian Izin oleh Node Admin

Kemudian dilakukan penyimpanan data oleh *node client* yang telah mendapatkan izin dari *node* admin yang ditunjukkan oleh Gbr. 8 :

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.1006]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 publish
 datasuhu key1 "{\"json\":{\"suhu\":\"20C\"}}"
{"method":"publish","params":["datasuhu","key1",{"json":{"suhu":
"20C"}}],"id":"78073366-1573560893","chain_name":"iotchain1"}

3ff6253c3ee4587d4b56cf3380890426d40e40154edc8f60e30ba21c2c4f978e
```

Gbr. 8 Node Client Sukses Melakukan Penyimpanan Data

Setelah itu dilakukan proses penyimpanan data pada *permissionless device*.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 publish
 datasuhu key1 "{\"json\":{\"suhu\":\"21C\"}}"

error: couldn't connect to server
```

Gbr. 9 Permissionless Device Gagal Melakukan Penyimpanan Data

Dapat dilihat pada Gbr. 9 bahwa *permissionless device* tidak dapat melakukan penyimpanan data dengan adanya pesan *error* yaitu "couldn't connect to server" karena memang syarat pertama untuk dapat melakukan proses tersebut adalah harus tersambung ke dalam *blockchain* terlebih dahulu sedangkan *permissionless device* tidak mendapatkan izin tersebut. Kemudian untuk skema pengujian kedua pada *permissioned device* didapatkan hasil bahwa perangkat *smart home* yang disimulasikan menggunakan program Python dapat melakukan penyimpanan data yang dibuktikan dengan Gbr. 10 dan Gbr. 11.

```
C:\Users\Dimas\PycharmProjects\skripsiku>py iot_device.py

connecting to 10.60.100.218 port 8882
Kirim pesan: 20c
ukuran pesan asli: 28 bytes
ukuran pesan setelah menjadi hexa: 31 bytes
hex msg: 323063
```

Gbr. 10 Permissioned Device Mengirimkan Data untuk Disimpan ke dalam Blockchain

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 listst
reamitems datasuhu false 1
{"method":"liststreamitems","params":["datasuhu",false,1],"id":
"79493392-1573565109","chain_name":"iotchain1"}

[
    {
        "publishers" : [
            "1W31H3w124wTiFi73bvvf5jFVMrmnmH4bBvEux"
        ],
        "keys" : [
            "key1"
        ],
        "offchain" : false,
        "available" : true,
        "data" : "323063",
        "confirmations" : 0,
        "txid" : "6aa216a0311acf8da9eb0b5fa2682bcd838b842b0617f
fd2abe08c2ccda862f7"
    }
]
```

Gbr. 11 Data Berhasil Tersimpan di Dalam Blockchain

Dapat dilihat pada Gbr. 10 dan Gbr. 11 data yang disimpan sama yaitu dalam bentuk hexa "323063". Sedangkan jika menggunakan *permissionless device* maka secara otomatis pesan tidak akan diterima oleh *node admin* karena program yang dijalankan oleh *node admin* hanya menerima satu koneksi saja pada satu waktu.

2) Pengujian Proses Pencarian Data: Pengujian proses pencarian data menggunakan skema pertama dapat dijalankan dengan mengetikkan perintah *liststreamitems,* perintah tersebut mengembalikan informasi tentang data yang telah tersimpan di dalam *blockchain*. Berikut hasil pencarian dari *permissioned device* :

```
C:\Windows\System32\cmd.exe

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 listst
reamitems datasuhu false 1
{"method":"liststreamitems","params":["datasuhu",false,1],"id":
"97094027-1573192814","chain_name":"iotchain1"}

[
    {
        "publishers" : [
            "1W31H3w124wTiFi73bvvf5jFVMrmnmH4bBvEux"
        ],
        "keys" : [
            "key1"
        ],
        "offchain" : false,
        "available" : true,
        "data" : "67617378",
        "confirmations" : 0,
        "txid" : "31bf75e52d4616d7daa67632ba1f747671b06d37aa5e1
822adc19b179b29e187"
    }
]
```

Gbr. 12 Hasil Pencarian Data pada Permissionned Device

Sedangkan hasil pencarian data pada *permissionless device* adalah sebagai berikut :

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

D:\dyr\multichain-windows-2.0.2>multichain-cli iotchain1 listst
reamitems datasuhu false 1
error: couldn't connect to server
```

Gbr. 13 Hasil Pencarian Data pada Permissionless Device

Terlihat bahwa *permissionless device* gagal melakukan pencarian data karena tidak mendapatkan izin dari *node admin* untuk dapat terhubung dengan *blockchain*. Kemudian untuk skema pengujian kedua hasilnya sama dengan saat penyimpanan data, karena program hanya menerima satu koneksi saja sehingga jika ada koneksi lain yang mencoba masuk maka secara otomatis akan tertolak.

VI. KESIMPULAN

Kesimpulan yang diperoleh dari hasil penelitian adalah bahwa teknologi *private blockchain* dapat diterapkan dengan baik dengan menggunakan *platform* MultiChain pada *smart home*. Hanya *node* yang mendapatkan izin saja yang dapat berpartisipasi ke dalam jaringan *private blockchain* sehingga data yang tersimpan di dalam *blockchain* hanya dapat dilihat oleh partisipan yang telah memperoleh izin. Program yang dibuat dengan menggunakan bahasa pemrograman Python dapat mengirimkan data atau pesan kepada *node admin* dan dapat diterima dengan baik tanpa mengalami kehilangan bagian dari data atau pesan yang dikirimkan sehingga dapat dikatakan bahwa program berhasil menyimulasikan perangkat *smart home* dengan baik.

UCAPAN TERIMA KASIH

Puji syukur serta rasa terima kasih saya haturkan kepada Allah SWT yang selalu memberi kemudahan dan kelancaran dalam mengerjakan jurnal ini. Semua pihak terkait yang senantiasa memberi saran serta semangat sehingga jurnal ini dapat terselesaikan dengan baik.

REFERENSI

[1] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: Challenges and Solutions 2016:1861–2. doi:10.1145/2976749.2976756.

[2] Notra S, Siddiqi M, Gharakheili HH, Sivaraman V, Boreli R. An Experimental Study of Security and Privacy Risks with Emerging Household Appliances (Position Paper) 2014:79–84.

[3] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE Int Conf Pervasive Comput Commun Work PerCom Work 2017 2017:618–23. doi:10.1109/PERCOMW.2017.7917634.

[4] Skarmeta AF, Hernandez-Ramos JL, Moreno MV. A decentralized approach for security and privacy challenges in the Internet of Things. 2014 IEEE World Forum Internet Things, WF-IoT 2014 2014:67–72. doi:10.1109/WF-IoT.2014.6803122.

[5] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Futur Gener Comput Syst 2018. doi:10.1016/j.future.2017.11.022.

[6] Greenspan G. MultiChain Private Blockchain 2015:1–17.

[7] Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and iot integration: A systematic survey. Sensors (Switzerland) 2018;18. doi:10.3390/s18082575.