**­­BAB II**

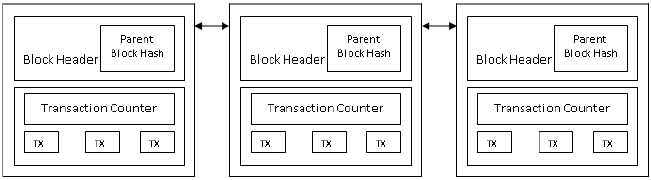
**TINJAUAN PUSTAKA DAN DASAR TEORI**

1. **Tinjauan Pustaka**
   * 1. 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 terbatas.
     2. Penggunaa *blockchain* untuk *Internet of Things* pernah diteliti oleh 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 sebagaian besar keuntungan keamanan dan privasi yang dihasilkan oleh *blockchain*. Peneliti menggunakan konteks *smart home*, *overlay network*, dan *cloud storage*, 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.
     3. 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 arsiktektur 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 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*.

1. **Dasar Teori**
   * 1. **Teknologi *Blockchain***

*Blockchain* adalah sebuah rangkaian blok data yang berisikan informasi unik dan dilengkapi dengan kode *hash* sebagi bukti keterkaitan tiap blok yang dihasilkan. *Blokchain* berhasil dipopulerkan oleh sebuah mata uuang digital atau *cryptocurrency* yang bernama Bitcoin. Meskipun bermula dari permasalahan pada Bitcoin, *blockchain* dapat berdiri sendiri tanpa penggunaan *cryptocurrency* (Christidis and Davetsikiotis, 2016).

Pada gambar dibawah dapat dilihat bahwa setiap blok memiliki hash dari blok sebelumnya pada header blok tersebut dan setiap blok hanya memiliki satu *parent* *block*. Untuk blok yang pertama kali dibuat disebut blok *genesis*, yaitu blok yang tidak memiliki *parent block*.



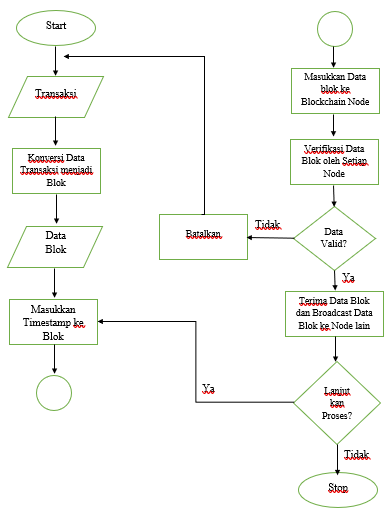
Block i+1

Block i

Block i-1

Gambar 2. Arsitektur Blockchain

*Blockchain* dapat diasumsikan sebagi arsip transaksi yang dikumpulkan pada blok-blok dengan penanda waktu atau *timestamp*. Setiap blok teridentifikasi dengan nilai hash. Namun, setiap blok tersebut mereferenskan nilai hash dari blok yang ada sebelumnya. Oleh karena itu, ikatan antar blok akan terjadi dan membuat sebuah rantai blok atau *blockchain* seperti pada gambar diatas. Skema tersebut akan berulang untuk blok-blok selanjutnya, tetapi pengecualian terjadi pada blok pertama dari rantai tersebut, yang dinamakan *genesis*. Blok *genesis* ini akan menjadi penanda secara umum pada seluruh jaringan *blockchain*, dan tanpa memiliki blok penduhulu.



Gambar Diagram alur proses *Blockchain* secara umum

Teknologi *blockchain* memiliki beberapa karakteristik sebagai berikut (Novo, 2018) :

1. Kendali yang terdesentralisasi. Sebuah desentralisasi yang tidak ada sebuah otoritas yang mengatur secara mutlak, seperti pada gambit dibawah.
2. Data yang trasnparan dan mudah untuk diaudit. Setiap *node* yang terhubung ke dalam jaringan *blockchain* memilki Salinan lengkap dari *blockchain* (publik), sejak blok *genesis* hingga blok terkini.



Gambar 1. Konsep desentralisasi pada *blockchain*.

1. Informasi yang terdistribusi. Setiap node menyimpan salinan dari *blockchain* untuk menghindari adanya ototritas terpusat yang menyimpan informasi tersebut sendiri.
2. Konsensus yang terdesentralisasi. Transaksi-transaksi yang direkam ke dalam *blockchain* divalidasi oleh setiap *node* yang terhubung ke dalam jaringan *blockchain*. Hal ini mematahkan paradigma konsesensus terpusat.
3. Aman. *Blockchain* kebal terhadap kerusakan yang disengaja dan tidak dapat dimanipulasi secara sengaja oleh pihak tidak bertanggung jawab.

Beberapa karakteristik penting yang dimiliki oleh jaringan *blockchain* adalah sebagai berikut (gupta):

1. **Konsensus**: Sebuah transaksi dapat dinyatakan valid ketika semua partisipan setuju dengan validitasnya.
2. **Asal**: Patisipan mengetahui sumber datangnya aset dan perubahan kepemilikannya sepanjang waktu.
3. **Kekekalan**: Tidak ada partisipan yang dapat mengubah sebuah transaksi setelah tercatat di penyimpanan utama atau *ledger*. Jika sebuah transaksi sedang terjadi kesalahan, transaksi baru harus digunakan untuk membalikkan kesalahannya, dan kedua transaksi akan terlihat.
4. **Penutup**: Sebuah *ledger* umum dapat menjadi satu tempat tujuan untuk menentukan kepemilikan sebuah aset atau penyelesaian sebuah transaksi.
   * 1. **Arsitektur *Blockchain***
     2. **Algoritma Konsensus**

Konsensus adalah problematika mendasar pada suatu sistem terdistribusi yang memerlukan dua atau lebih agen untuk mencapai kesepakatan pada sebuah nilai tertentu untuk menjalankan sebuah kompuasi. Pada pelaksanaannya, beberapa agen bisa jadi tidak andal dan proses untuk mencapai kesepakatan bersama (konsensus) harus mempertimbangkan hal ini. *Blockchain* menerapkan beberapa algoritma konsensus seperti berikut (Jakobsoson, 1999):

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 bloko 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. *Delegated Proof of Stake* (DPoS)

Protokol DPoS ini serupa dengan PoS. Pada *blockchain* dengan konsensus DPoS para pemangku kepentingan akan melakukan *voting* untuk memilih siapa yang akan melakukan keamanan jaringan demi kepentingan mereka. Delegat yang dipilih juga dapat dianggap sebagai saksi dan mereka bertanggung jawab dalam pencapaian konsensus slama pembuatan dan validasi blok baru (Vasin, 2014).

1. Ripple

Algoritma konsensus ripple menggunakan sub jaringan yang terpercaya dalam suatu jaringan yang lebih besar. Dalam jaringannya, *node* dibagi menjadi dua yaitu: *server* untuk partisipasi dalam proses konsensus dan terdapat *client* hanya unutuk mengirimkan uang digital dalam jaringan tersebut. Setiap *node* memiliki *Unique Node List* (UNL). UNL ini sangat penting untuk *server* ketika menentukan transaki akan dimasukkan ke blok untuk disimpan di *blockchain*. Ketika melakukan hal ini, *server* akan melakukan *query node* yang melakukan transaksi dalam UNL, dan jika kesepakatan yang diterima sudah lebih 80%, transaksi akan dimasukkan ke blok. Hal ini dikarenalan blockchain akan tetap benar selama transaksi berasal dari *node* yang memiliki persentase *faulty node* dalam UNL lebih kecil dari 20% (Chase and MacBrought, 2019).

* + 1. ***Hashing* SHA-256**

Fungsi *hash* adalah sebuah fungsi yang masukkannya berupa pesan dengan panjang sembarang dan hasil keluarannya berupa *hash* (*hash value*) dengan panjang yang tetap dan biasa disebut *digest* atau message *digest*. Fungsi *hash* dapat digunakan untuk mewujudkan salah satu prinsip keamanan jaringan dan informasi yaitu keutuhan data (*data integrity*). Fungsi tersebut berguna sebagai parameter yang mengecek ada tidaknya perubahan terhadap data sebelum dan sesudah data itu dikirim atau disebar ke tempat lain dalam satu komputer maupun jaringan.

Salah satu cara untuk menghasilkan *digest* adalah dengan memanfaatkan penggunaan fungsi kompresi secara berulang terhadap sebuah pesan yang telah dibagi sebelumnya menjadi sejumlah blok pesan. Salah satu fungsi *hash* yang menggunakan cara tersebut adalah SHA (*Secure Hash Algoritm*). SHA adalah fungsi *hash* satu arah yang dibuat oleh *National Intitute of Standarts and Technology* (NIST). SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest, SHA sampai saat ini memiliki 4 versi, mulai dari bebrapa varian, salah satunya adalah SHA-256.

SHA-256 adalah fungsi *hash* yang menghasilkan nilai *hash* sepanjang 256 bit dengan iterasi terhadap sejumlah blok pesan yang masing-masing panjangnya 512 bit.

Secara singkat, langkah-langkah untuk menghasilkan *digest* adalah sebagai berikut. Misalkan ada pesan P. P tersebut direpresentasikan ke bilangan biner tiap karakter pesannya. Selanjutnya adalah menambah *padding* terhadap P berupa satu bit karakter “1”, diikuti sejumlah bit karakter”0” dan repsemtasi biner dari Panjang *byte* pesan, agar Panjang P tepat berkelipatan 512 bit. Representasi pesan P ber-*padding* tersebut kemudian diubah menjadi bilangan heksadesimal. Lalu, memanggil fungsi kompresi dengan parameter masukan berupa delapan *word* nilai *digest* awal yang diambil dari bagian pecahan pada akar kuadrat delapan bilangan prima pertama dengan panjang *word* masing-masing 32 bit dan pesan P ber-*padding*. Dalam fungsi kompresi, dilakukan ekspansi *word* dari pesan P ber-*padding* tersebut dengan jumlah word sebanyak 64 yang masing-masing panjangnya 32 bit dan komputasi ronde sebanyak 64 ronde, yang mana hasilnya didapatkan dengan melakukan penjumlahan digest dikalikan dengan mod 232. Setelah tidak ada blok pesan lagi yang diproses, maka hasil dari fungsi kompresi dijadikan digest yang dicari dengan panjang 256 bit.

* + 1. **Kriptografi**
    2. ***Internet of Things* (IoT)**
    3. **Arsitektur Protokol**

**DAFTAR PUSTAKA**

Binance Academy, “Delegated Proof of Stake Explained,” Binance Academy, [Online]. Available : https://academy.binance.com/blockchain/delegated-proof-of-stake-explained. Idem

B. Chase and E. MacBrough, “Analysis of the XRP Ledger Consesnsus Protocol,” 21 February. [Online]. Available : https://arxiv.org/pdf/1802.07242.pdf. idem

Dorri A, Kanhere SS, Jurdak R. 2016, Blockchain in Internet of Things: Challenge and Solution, diakses tgl bln thn.

Dorri A, Kanhere SS, Jurdak R, Gauravaram P. 2017, Blockchain for IoT security dan privacy: The case study of a smart home, idem

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

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

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

K. Christidis dan M. Davetsikiotis 2016, “Blockchain and Smart Contracts for the Internet of Things”, idem

M. Gupta 2017, Blockchain for Dummies, IBM Limited Edition, Hoboken: John Wiley & Sons, Inc.,idem

M. Jakobsoson dan A. Juels 1999 “Process of Work and Bread Pudding Protocols (Extended Abstract),” Proc. IFTP TC6/TC11 Jt. Work. Conf. Secur. Inf. Net-work. Commun. Miltimed. Secur. Hal 258-272

O. Novo 2018, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT, ” IEEE Internet Things J.

P. Vasin, 2014, “BlackCoin’s Proof of Stake protocol v2”. idem

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

S. Nakamoto, 2009 “Bitcoin: A Peer to Peer Electronic Cash System”.

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