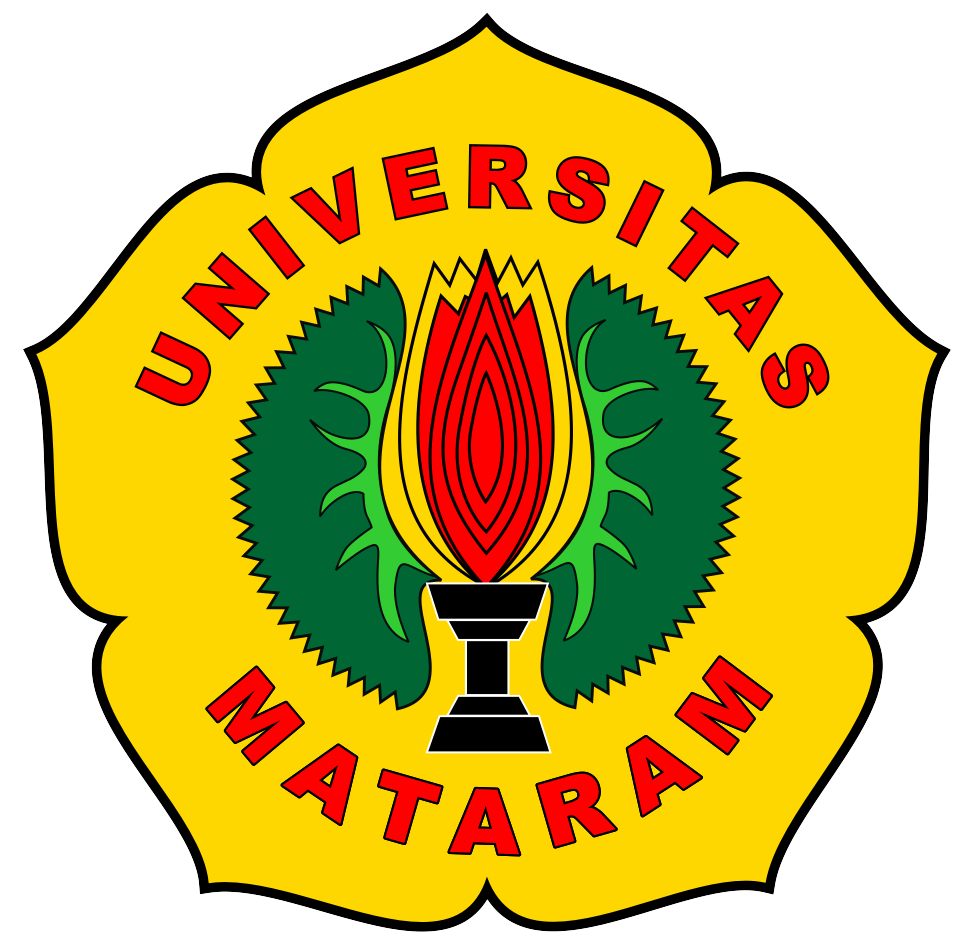
**USULAN TUGAS AKHIR**

**Implementasi Teknologi Blockchain Sebagai Sistem Keamanan pada Teknologi IoT**



**Oleh :**Lalu Ocky Saktiya Luhung  
F1B019079

**JURUSAN TEKNIK ELEKTRO**

**FAKULTAS TEKNIK**

**UNIVERSITAS MATARAM**

**DAFTAR ISI**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

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 computer*) menuju *embedded and cyber-physical system*.

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 terget menarik dari serangan *cyber*. Keamanan dan privasi dianggap sebagai hambatan utama agar paradigma IoT dapat diterima secara penuh. 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 yang membutuhkan banyak memori dan sumber daya komputer (Dorri, dkk, 2016).

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

Impelementasi *blockchain* pada peranti IoT tidak dapat dilakukan secara langsung karena karakteristik *blockchain* yang memiliki tingkat komputasi yang sangat tinggi dan berat. Solusi yang ada mengoptimasi *blockchain* agar sesuai dengan karakterisik peranti IoT dengan mengiliminasi beberapa overhead tanpa mengorbankan yang signifikan pada sisi keamanan dan privasi. Beberapa Teknik implementasi *blockchain* di IoT menghilangkan sisi *Proof of Work* (PoW), pemisahan antara lapisan data dan transaksi dan kombinasi antara *blockchain* publik dan privat. Pada Teknik implementasi ini, komunikasi pada *nodes* selalu terenkripsi dengan ,mekanisme kunci publik dan menggunakan teknik verifikasi tanpa konsensus, Sebuah node dapat mengganti kunci publiknya secara berkala untuk menjaga anominitas dan privasi (Dorri, dkk, 2016).

Pada penelitian yang dilakukan oleh Satoshi Nakamoto (2008) dengan judul *Bitcoin: A Peer-to-Peer Electronic Cash System*, terdapat konsep teknologi yang disebut dengan *blockchain*. *Blockchain* memungkinkan suatu sistem untuk dikembangkan secara terdesentralisasi (*decentralized*) sehingga otoritas dari sistem tidak dipegang oleh satu pihak saja, tetapi semua entitas di dalam sistem memiliki hak otoritas yang sama. Sifat terdesentralisasi yang dimiliki oleh *blockchain* memberikan dampak yang signifikan pada properti keamanan dan transparansi dari suatu sistem.

Pengembagan *blockchain* ini awalnya diberlakukan untuk sistem transaksi mata uang digital, atau biasa disebut dengan *cryptocurrency*. Sistem ini memungkinkan suatu transaksi dapat dilakukan tanpa adanya pihak ketiga yang bertugas untuk melakukan validasi dalam menentukan keabsahan dari suatu transaksi. Validasi dari transaksi dilakukan bersama oleh seluruh *node* berua entitas-entitas yang terhubung pada jaringan sistem.

1. **Rumusan Masalah**

Berdasarkan latar belakang diatas dapat diidentifikasi beberapa permasalahan yaitu :

1. Bagaimana *blockchain* dapat menjaga keamanan dalam sistem IoT?
2. Bagaimana cara menjaga keamanan data dalam sistem IoT dengan menggunakan *blockchain*?
3. Bagaimana cara mengetahui hasil dari *blockchain* dalam mengamankan sistem IoT?
4. Bagaimana *blockchain* dapat diimplemetasikan pada sistem keamanan IoT untuk meningkatkan kemanan dan privasi data?
5. Bagaimana *blockchain* dapat memfasilitasi proses autentikasi dan otorisasi pada sistem keamanan IoT?
6. Bagaimana cara mengintegrasikan teknologi *blockchain* pada infrastruktur dan arsitektur yangsudah ada pada sistem keamanan IoT?
7. **Ruang Lingkup**

Penelitian yang dilakukan memiliki batasan dan ruang lingkup sebagai berikut :

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

Tujuan dari tugas akhir ini adalah mengimplementasi dan mengintegrasi teknologi IoT dengan Teknologi *Blockchain* dalam membangun keamanan sistem pada IoT dengan menggunakan *Blockchain*.

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

Manfaat dari hasil pembuatan Tugas Akhir ini adalah :

1. Dapat meningkatkan keamanan sistem IoT terdahulu dengan mengintegrasikan dengan teknologi *Blockchain*.
2. Mendapatkan pemahaman implementasi *Blockchain* pada pada sistem keamanan IoT.
3. Menggunakan dan mengintegrasikan IoT dengan *Blockchain* dapat meningkatkan keamanan dan privasi data.

**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 Iternet Of Things”. Pada penelitian tersebut, peneliti menunjukkan
     2. **Asa**
2. **Dasar Teori**
   * 1. **Teknologi Blockchain**
     2. **Arsitektur Blockchain**
     3. **Algoritma Konsensus**
     4. **Algoritma Hashing SHA-256**
     5. **Kriptografi**
     6. **Internet of Things (IoT)**
     7. **Arsitektur Protokol**

**BAB III**

**METODE PENELITIAN**

**DAFTAR PUSTAKA**

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

Dorri A, Kanhere SS, Jurdak R, Gauravaram P. 2017, Toward an Optimimzed BlockChain for IoT,”*Proc. Second Int. Conf. Internet-of-Things Des. Implement*”, idem

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

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

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