

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

*Blockchain* adalah jaringan perangkat lunak *peer to peer* terdistribusi penuh dengan memanfaatkan kriptografi dalam menyimpan dan mengirim data[1], data dalam *Blockchain* disimpan dalam bentuk blok dan setiap blok memiliki *hash* dari blok sebelumnya[2][3]. *Blockchain* sudah banyak dimanfaatkan di berbagai bidang, seperti *Supply Chain*, Transportasi, dan Logistik karena kecepatan, kebenaran, dan keamanannya[4]. Teknologi *Blockchain* juga digunakan untuk *e-voting* karena keamanan dan keterbukaan akan datanya[5][6].

Tanda-tangan merupakan fitur biometrik yang dapat digunakan untuk memverifikasi identitas seseorang[7]. Di Departemen Teknik Komputer Universitas Andalas sendiri, tanda tangan sering digunakan untuk melegalisasi atau menyetujui suatu dokumen, seperti kartu ujian akhir semester yang perlu persetujuan dosen pembimbing akademik. Namun penanda tangan dokumen dengan cara menanda tangan secara langsung dan basah tidak dapat di rekam. Kemudian seiring berkembangnya teknologi, tanda tangan dapat dilakukan secara digital melalui suatu aplikasi seperti SignNow[8] dan PSrE[9]. Namun cara tersebut bersifat terpusat dimana perlu mempercayai penyedia aplikasi/layanan dalam merekam data transaksinya, sehingga ada kemungkinan manipulasi data transaksi tanda tangan di pihak penyedia layanan. Untuk mengatasi kedua masalah diatas, dibutuhkan suatu sistem yang dapat merekam data dan mendistribusikannya tanpa memerlukan pihak ketiga(desentralisasi) seperti *Blockchain*[1], [10], [11].

*Bitcoin* adalah jaringan *Blockchain* pertama yang digunakan untuk mengirim dan menerima uang kripto[12], kemudian hadir lah *Ethereum* yaitu salah satu platform jaringan *Blockchain* hasil dari pengembangan *Bitcoin* yang dapat melakukan banyak proses selain bertukar uang kripto yang mendukung *Proof of Authority Consensus Mechanism*[13] dan juga dapat ditanamkan *smart contract*[11]. *Smart contract* adalah suatu program komputer atau peraturan yang berjalan di dalam jaringan *Ethereum*[1][11], *smart contract* dapat diibaratkan seperti Vending Machine dimana minuman akan keluar hanya jika koin sudah dimasukkan. Dengan

*smart contract* inilah logika-logika mengolah data dapat diimplementasikan secara distributif, seperti menanda tangani pesan dan dokumen, mengatur otoritas, dan lain-lain. *Peer* atau *Node* dapat dijalankan dengan menggunakan *Raspberry Pi 3+*, seperti proyek *Managing Smart Home Appliances with Proof of Authority and Blockchain*[3] dan *Blockchain Technology Implementation In Raspberry Pi For Private Network*[2]. *Raspberry Pi* adalah komputer yang berukuran kecil dan tertanam pada satu papan tunggal yang memiliki hampir semua fungsi pada komputer biasa[2][14]. Kemudian untuk membuat pengguna dapat berkomunikasi dengan jaringan, dapat menggunakan aplikasi android dengan perantara sebuah rest API server.

Dari uraian masalah dan teknologi diatas, penulis tertarik untuk membuat sebuah sistem terdistribusi tanpa ada server pusat, yang dapat mencatat transaksi tanda tangan yang sah dan terpercaya. Sistem akan menggunakan *Raspberry PI* sebagai *node*, dan menggunakan aplikasi mobile sebagai antar muka pengguna. Oleh karena itu, akan dirancanglah Tugas Akhir dengan judul **Transparansi Tanda Tangan Menggunakan Jaringan Ethereum Pribadi Berbasis Single Board Computer Studi Kasus di Departemen Teknik Komputer Universitas Andalas.**

## 1.2 Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah:

1. Bagaimana mempermudah transaksi tanda tangan di Departemen Teknik Komputer Universitas Andalas
2. Bagaimana merekam transaksi tanda tangan secara desentralisasi dan terdistribusi di Departemen Teknik Komputer Universitas Andalas
3. Bagaimana memvalidasi suatu tanda tangan di Departemen Teknik Komputer Universitas Andalas

## 1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Jumlah maksimal *Node* adalah 3 buah *Node(Fixed Node)*
2. Aplikasi pengguna hanya tersedia dalam versi Android
3. *Raspberry Pi* yang digunakan minimal generasi tiga

## 1.4 Tujuan Penelitian

Tujuan yang akan dicapai dari penelitian ini adalah:

1. Terciptanya jaringan *Blockchain* pribadi
2. Menjalankan Node-node pada *Raspberry Pi*
3. Menggunakan *Proof of Authority* untuk mengesahkan blok
4. Terekamnya transaksi tanda tangan di jaringan *Blockchain* pribadi
5. Terciptanya rancangan data untuk transaksi tanda tangan menggunakan *smart contract*
6. Terciptanya aplikasi end user dan block explorer yang terintegrasi dengan sistem

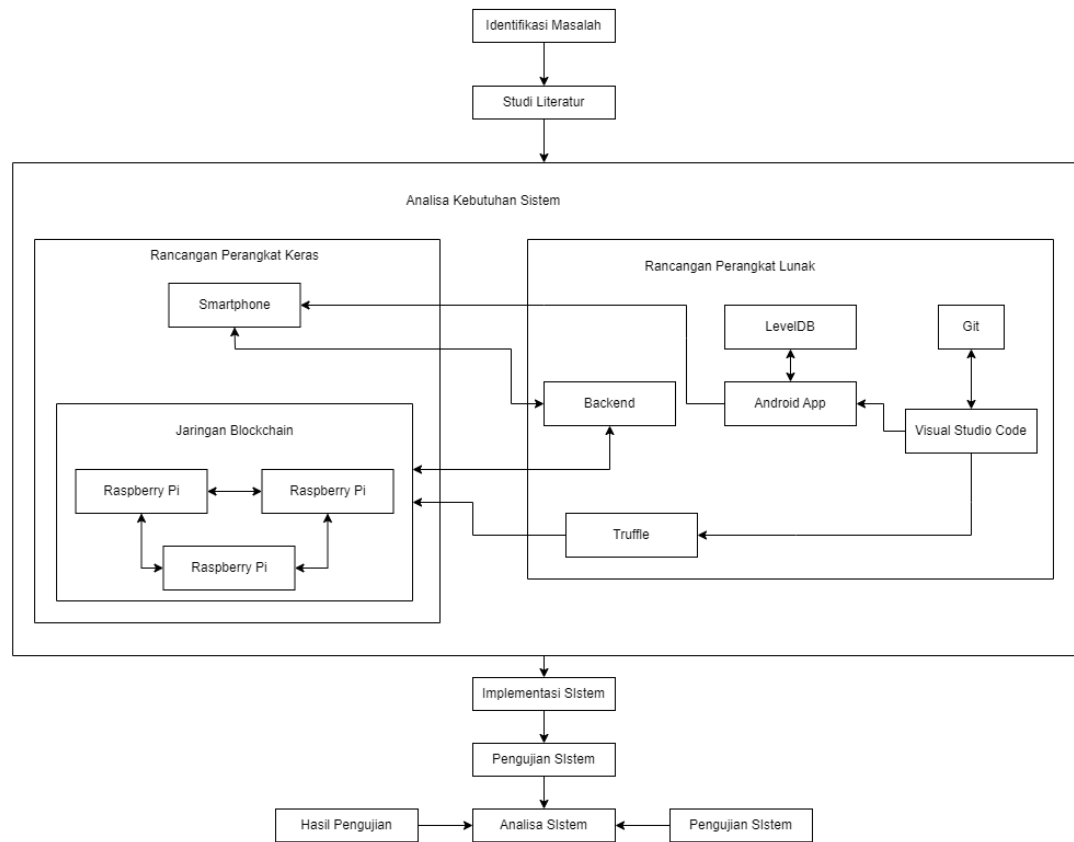
## 1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Terekamnya transaksi tanda tangan yang dilakukan di Departemen Teknik Komputer, Universitas Andalas
2. Menjamin kebenaran tanda tangan
3. Meningkatkan kepercayaan antar pihak yang terlibat dalam transaksi tanda tangan
4. Mencegah pemalsuan dan manipulasi tanda tangan
5. Mempermudah penanda tangan dokumen di Departemen Teknik Komputer, Universitas Andalas

## 1.6 Jenis dan Metodologi Penelitian

Penelitian Tugas Akhir ini menerapkan metode penelitian eksperimental (Experimental Research). Penelitian eksperimental yaitu penelitian yang dilakukan atas dasar pengaruh suatu kejadian dan tingkah laku terhadap subjek penelitian. Metode penelitian eksperimental ini memiliki tujuan untuk mempelajari suatu parameter masukan yang akan menghasilkan keluaran berbeda berdasarkan parameter-parameter yang telah ditetapkan. Penelitian ini dilakukan dengan menghubungkan beberapa komponen yang akan saling berhubungan satu sama lain, seperti pada penelitian ini terdapat beberapa komponen seperti Raspberry Pi,



**Gambar 1. 1 Diagram Rancangan Penelitian**

Berdasarkan diagram rancangan penelitian pada gambar diatas maka tahapan-tahapan dari perancangan sistem sebagai berikut :

**A. Identifikasi Masalah**

Pada tahapan ini, akan dilakukan identifikasi permasalahan yang diangkat menjadi penelitian pada tugas akhir. Proses identifikasi dilakukan melalui penelusuran permasalahan yang terjadi di Departemen Teknik Komputer Universitas Andalas yaitu kasus-kasus dalam aktifitas penanda tangan dokumen. Kemudian, dari permasalahan tersebut dirancang sebuah sistem untuk mengatasi permasalahannya.

**B. Studi Literatur**

Pada studi literatur, hal yang dilakukan yaitu mencari dan mengumpulkan jurnal dari penelitian-penelitian sebelumnya yang berkaitan dengan penelitian ini. Studi literatur ini juga mempelajari teori-teori yang berkaitan dalam pembuatan tugas

akhir. Teori-teori yang dipelajari meliputi cara kerja perangkat keras, perangkat lunak dan bagaimana sistem bekerja.

### C. Perancangan Sistem

Pada perancangan sistem ini terdapat tiga jenis yaitu perancangan perangkat keras, perancangan jaringan blockchain, dan perancangan perangkat lunak.

#### 1. Perancangan Perangkat Keras

Pada tahap perancangan perangkat keras ini, memilih perangkat keras yang dibutuhkan agar sistem yang dirancang dapat berjalan sesuai dengan tujuannya. Perangkat keras yang digunakan pada sistem ini yaitu Raspberry Pi 3 dan Raspberry Pi 4 sebagai host untuk menjalankan node.

#### 2. Perancangan Perangkat Lunak

Pada tahap perancangan perangkat lunak, dilakukan pembuatan aplikasi android, backend dan smart contract. Teknologi yang digunakan dalam pembuatan aplikasi android adalah React Native sebagai framework mobile development, web3.js sebagai library untuk terhubung ke sebuah node, levelDB sebagai local storage, visual studio code sebagai editor kode, git sebagai version control, dan github sebagai remote repository. Dan teknologi yang digunakan untuk membuat smart contract adalah Truffle sebagai framework smart contract development, Solidity sebagai bahasa pemrograman, visual studio code sebagai editor kode, git sebagai version control, dan github sebagai remote repository.

### D. Implementasi Sistem

Sistem yang telah dirancang akan diimplementasikan dalam bentuk perangkat keras dan perangkat lunak yang akan diimplementasikan kedalam sebuah jaringan blockchain agar dapat digunakan sesuai fungsinya.

### E. Pengujian Sistem

Pada tahap pengujian sistem, akan dilakukan pengujian secara end to end untuk semua fitur yang, yaitu Minta Tanda Tangan, Beri Tanda Tangan, Validasi Tanda Tangan, Akses Faucet, dan Tambah Data Ke Smart Contract.

### F. Hasil Pengujian

Setelah sistem berhasil melewati tahap pengujian sistem, selanjutnya hasil yang didapat akan diamati serta dianalisis apakah sudah sesuai dengan yang diinginkan atau tidak. Hasil dari sistem ini berupa,

1. Basis data transaksi tanda tangan yang terdistribusi dalam jaringan dan immutable
2. Data-data untuk transaksi tanda tangan dapat diimplementasikan dengan smart contract
3. Transaksi penanda tangan dokumen menjadi transparan dan dapat ditelusuri menggunakan dapp

#### G. Analisa Hasil

Pada tahap ini, terdapat hasil dari rangkaian pengujian yang telah dilakukan dan akan dilakukan analisa terhadap,

1. Basis data transaksi tanda tangan yang terdistribusi sesuai dengan yang diharapkan
2. Smart contract bekerja seperti yang diharapkan
3. Transparansi transaksi tanda tangan

#### H. Dokumentasi

Tahap dokumentasi diperlukan dalam seluruh proses penelitian. Dokumentasi digunakan untuk kebutuhan laporan dan pembuktian bahwa sistem yang telah dibuat dapat berjalan sesuai yang diharapkan. Dokumentasi meliputi seluruh proses kegiatan yang telah dilakukan pada saat perancangan sistem, pembuatan, pengujian, analisa dan hasil. Tahap dokumentasi bertujuan untuk memberikan kemudahan terhadap pengembangan maupun penelitian tingkat lanjut terhadap sistem yang telah dibuat.

### 1.6 Sistematika Penulisan

Penulisan laporan tugas akhir ini ditulis dalam beberapa bab, dengan urutan sebagai berikut :

#### **BAB I PENDAHULUAN**

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

## **BAB II LANDASAN TEORI**

Bab ini berisi tentang landasan teori dasar yang mendukung pembahasan penelitian yang didapat dari sumber-sumber yang terkait dan berhubungan dengan penelitian.

## **BAB III METODOLOGI PENELITIAN**

Bab ini membahas tentang jenis dan metodologi penelitian, analisa kebutuhan sistem, rancangan umum sistem, rancangan proses, rencana pengujian, dan analisa kebutuhan penelitian.

## **BAB IV HASIL DAN ANALISA**

Bab ini menjelaskan tentang hasil perancangan sistem yang berupa data-data dari penelitian yang dilakukan, serta analisa terhadap sistem melalui perbandingan sistem sebelum dan setelah dilakukan pengembangan dan peningkatan

## **BAB V PENUTUP**

Bab ini berisi kesimpulan yang dapat diambil dari penelitian serta saran untuk pengembangan selanjutnya.

