# 

**TRANSPARANSI TANDA TANGAN MENGGUNAKAN JARINGAN *ETHEREUM* PRIBADI BERBASIS *SINGLE BOARD COMPUTER***

**STUDI KASUS DI DEPARTEMEN TEKNIK KOMPUTER  
UNIVERSITAS ANDALAS**

**PROPOSAL TUGAS AKHIR DEPARTEMEN KOMPUTER**

**JUNI DIO KASANDRA**

**1811512030**



**DEPARTEMEN TEKNIK KOMPUTER**

**FAKULTAS TEKNOLOGI INFORMASI**

**UNIVERSITAS ANDALAS**

**PADANG**

**2023**

**TRANSPARANSI TANDA TANGAN MENGGUNAKAN JARINGAN *ETHEREUM* PRIBADI BERBASIS *SINGLE BOARD COMPUTER***

**STUDI KASUS DI DEPARTEMEN TEKNIK KOMPUTER  
UNIVERSITAS ANDALAS**

**PROPOSAL TUGAS AKHIR DEPARTEMEN KOMPUTER**

*Sebagai Salah Satu Syarat Untuk Menyelesaikan Program Sarjana*

*Pada Departemen Teknik Komputer Universitas Andalas*

**JUNI DIO KASANDRA**

**1811512030**



**DEPARTEMEN TEKNIK KOMPUTER**

**FAKULTAS TEKNOLOGI INFORMASI**

**UNIVERSITAS ANDALAS**

**PADANG**

**2023**

# BAB I

## PENDAHULUAN

### 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 tanganan 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 hadirlah *Ethereum* yaitu salah satu platform jaringan *Blockchain* hasil dari pengembangan *Bitcoin* yang dapat melakukan banyak proses selain bertukar uang kripto yang mendukung *Proof of Authorithy 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 *web3.js. web3.js* adalah kumpulan library yang digunakan untuk berinteraksi dengan *node*, melalui HTTP, WebSocket, atau IPC.

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.**

### Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah:

1. Bagaimana membuat jaringan *Blockchain* pribadi dengan *Ethereum Platform*
2. Bagaimana membuat *Node Blockchain* dengan menggunakan *Raspberry Pi*
3. Bagaimana menggunakan *Proof of Authorithy* untuk mengesahkan blok
4. Bagaimana merekam transaksi tanda tangan di jaringan *Blockchain* pribadi
5. Bagaimana merancang data dan aturan-aturanuntuk transaksi tanda tangan menggunakan *Smart Contract*
6. Bagaimana membuat *end user application* yang terintegrasi dengan jaringan *Blockchain* menggunakan *web3.js*

### 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 adalah *Raspberry Pi* 3 keatas

### 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 Authorithy* untuk mengesahkanblok
4. Terekamnya transaksi tanda tangan di jaringan *Blockchain* pribadi
5. Terciptanya rancangan data dan aturan-aturan untuk transaksi tanda tangan
6. Terciptanya aplikasi end user dan block explorer yang terintegrasi dengan sistem menggunakan *web3.js*

### 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 penandatangan
4. Mencegah pemalsuan dan manipulasi tanda tangan
5. Mempermudah penanda tanganan dokumen di Departemen Teknik Komputer, Universitas Andalas

### 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.

# BAB II

## LANDASAN TEORI

### Tanda Tangan

Tanda tangan adalah hasil dari proses menulis seseorang yang bersifat khusus sebagai substansi simbolik. Tanda tangan merupakan bentuk yang paling banyak digunakan untuk identifikasi seseorang. Fungsi tanda tangan sendiri adalah untuk pembuktikan. Dalam kehidupan sehari-hari, tanda tangan digunakan sebagai identifikasi dari pemilik tanda tangan. Keberadaan tanda tangan dalam sebuah dokumen menyatakan bahwa pihak yang menandatangani, mengetahui, dan menyetujui seluruh isi dari suatu dokumen[7].

### *Blockchain*

Blockchain adalah teknologi yang didistribusikan dan terdesentralisasi di mana data disimpan dalam bentuk blok dan setiap blok diikat dengan blok sebelumnya. Penggabungan blok dilakukan dengan hashing. Blockchain dikelola oleh sejumlah node. Setiap node menjaga salinan blockchain yang terdiri dari blok yang dimulai dari awal blockchain sampai sekarang. Node-node ini membentuk jaringan peer-to-peer untuk berbagi informasi dan meneruskan atau menerima blok. Setiap node saling bertukar informasi dengan node-node peer-nya dan node-node peer tersebut terus meneruskan informasi kepada peer-nya, proses ini terus berlanjut sampai setiap node dalam jaringan telah memperoleh informasi. Sebuah node menggabungkan transaksi masuk dalam bentuk blok dan memancarkannya ke jaringan. Node lain yang menerima blok memeriksa kevalidannya dan menambahkannya ke salinan blockchain lokal jika valid[1][2][3].

Komponen-komponen pada sebuah *blockchain,*

* + - 1. Buku Besar Terdistribusi (Basis Data Terdistribusi)

Basis Data yang dimana data disimpan dalam bentuk blok dan setiap blok memiliki identitas(kriptografi) dari blok sebelumnya.

* + - 1. Peer-to-peer network – P2P / *Node*

Jaringan P2P adalah model komunikasi dimana setiap pelaku (*peer node)* bertindak sebagai *client* dan *server.*

* + - 1. *Consensus Mechanism*

*Consensus Mechanism* adalah aturan-aturan dalam sebuah jaringan *blockchain* untuk mengesahkan sebuah blok dan memasukkannya kedalam basis data. *Consensus Mechanism* juga menentukan *state* dari sebuah jaringan *blockchain*.

* + - 1. Kriptografi

Digunakan untuk enkripsi data-data demi keamanan dan integritas.

* + - 1. *Wallet*

*Wallet* adalah akun atau sebagai bank untuk pengguna dalam sebuah jaringan *Blockchain.* *Wallet* digunakan untuk bertransaksi.

### Pengaplikasian Blockchain

Blockchain sudah diimplementasikan di berbagai bidang seperti di bidang supply chain, transportasi, logistik, kesehatan, dan pemilihan elektronik. Alasan penggunaan blockchain adalah karena blockchain meningkatkan kepercayaan atas suatu sistem karena tidak adanya pelaku pusat yang menengahi atau mengatur setiap proses, keamanan sistem karena setiap data akan dienkripsi, dan kecepatan sistem karena transaksi dapat dilakukan secara langsung tanpa memerlukan penengah seperti sistem sentral pada ummumnya[4][5][6].

### *Ethereum Platform*

*Bitcoin* adalah *Blockchain* pertama yang ada. *Bitcoin* diciptakan untuk transaksi uang digital dimana pengguna dapat mengirim dan menerima uang digital. *Bitcoin* hanya dapat melakukan proses mengirim uang dan menerima uang yang artinya tidak dapat melakukan proses yang lebih kompleks.

*Ethereum* adalah sebuah platform *blockchain* yang dapat ditanamkan aturan-aturan untuk sebuah transaksi (*smart contract)* sehingga mendukung transaksi yang kompleks. *Ethereum* mendukung *proof of authority(POA) consensus mechanism* untuk mengesahkan blokdan *Ethereum* juga mendukung *dapp* sehingga pengguna dapat membuat dan menguji sebuah aplikasi yang terdesantralisasi[1][3][11].

#### **2.4.1 Geth (Go Ethereum)**

**Geth, singkatan dari Go Ethereum, adalah perangkat lunak klien yang ditulis dalam Golang yang memudahkan implementasi protokol Ethereum. Di console Geth, pengguna dapat menghubungkan host ke jaringan Ethereum untuk mining, manajemen akun, publikasi kontrak dan serangkaian fungsi lainnya. Klien Geth dapat menyinkronkan semua data blockchain publik Ethereum ke host lokal.**

#### **2.4.2 Smart Contract**

**Smart Contract adalah baris kode yang diimplementasikan di blockchain yang menentukan serangkaian aturan untuk sebuah aplikasi. Sebuah Smart contract memelihara state aplikasi. Setiap transaksi yang valid di blockchain yang sesuai dengan smart contract akan memperbarui state smart contract. Ketika sebuah smart contract diimplementasikan di blockchain, semua orang dapat melihat smart contract tersebut. Smart contract tidak dapat diubah, yang berarti setelah diimplementasikan aturan di dalam kontrak tidak dapat diubah. Ini menjamin tidak adanya penyangkalan dari pihak yang tidak bertanggung jawab yang terlibat dalam kontrak.[3]**

#### **2.4.3 Proof of Authority**

**Proof of Authority (PoA) adalah algoritma konsensus Byzantine Fault Tolerant (BFT) untuk blockchain pribadi. Algoritma ini tergantung pada himpunan entitas terpercaya yang dikenal sebagai validator. Validator bertanggung jawab untuk mengumpulkan transaksi dari klien, menciptakan dan menambahkannya ke blockchain. Algoritma berjalan dalam putaran di mana dalam setiap putaran seorang validator diizinkan mengusulkan sebuah blok. Seorang validator mengusulkan blok di putaran masing-masing. Validator lain memverifikasi blok yang diusulkan dan menambahkan blok ke salinan blockchain lokal jika ditemukan valid. Setelah sebuah blok ditambahkan, tercapai konsensus global. Suatu validator dapat dikeluarkan melalui voting oleh validator-validator lainnya yang ada dalam jaringan, jika 51% setuju, maka validator tersebut akan dihapus, oleh karena itu, ia tidak lagi diakui untuk mengusulkan blok kedepannya. PoA adalah algoritma konsensus yang ideal untuk blockchain pribadi di mana peserta terautentikasi dan terbatas jumlahnya. Biasanya dianggap sebagai kompromi antara sistem terdesentralisasi sebenarnya dan sistem terpusat yang efisien. POA ringan dan memiliki kecepatan yang lebih tinggi; oleh karena itu, mekanisme konsensus yang ideal untuk implementasi blockchain IoT terlokalisasi seperti smart homes di mana konsumsi daya menjadi kritikal dan perangkat memiliki batas pada kapasitas komputasi dan penyimpanannya*.*[3][13]**

#### **2.4.4 Solidity**

**Solidity adalah bahasa pemrograman berorientasi objek yang sering digunakan untuk mengembangkan smart contract di Ethereum. Solidity adalah bahasa utama di Ethereum dan dirancang berdasarkan sintaks ECMAScript. Solidity adalah bahasa yang static type, mendukung inheritance, library, dan tipe yang didefinisikan oleh pengguna yang kompleks. *Solidity* terinspirasi dari bahasa pemrograman *C++, Python,* dan *Javascript.*[14][15]**

### Truffle

Truffle adalah development environment, testing framework, dan assets pipeline untuk Ethereum. Truffle memiliki banyak fungsi seperti kompilasi dan implementasi smart contract terintegrasi, pengujian smart contract otomatis, build pipeline yang dapat dikonfigurasi, migrasi dan implementasi yang dapat diatur dengan skrip, dan lain-lain. Truffle juga memiliki konsol interaktif untuk komunikasi dengan smart contract secara langsung, yang sangat berguna selama pengembangan[14].

### *Dapp*

*Decentralized Application* adalah aplikasi *peer to peer* yang menjadikan *blockchain* sebagai basis data dan proses utama, inilah yang membuat *dapp* berbeda dengan aplikasi pada umumnya yang hanya memiliki satu server sebagai basis data dan proses utama[1][11].

Manfaat menggunakan *dapp* adalah sebagai berikut.

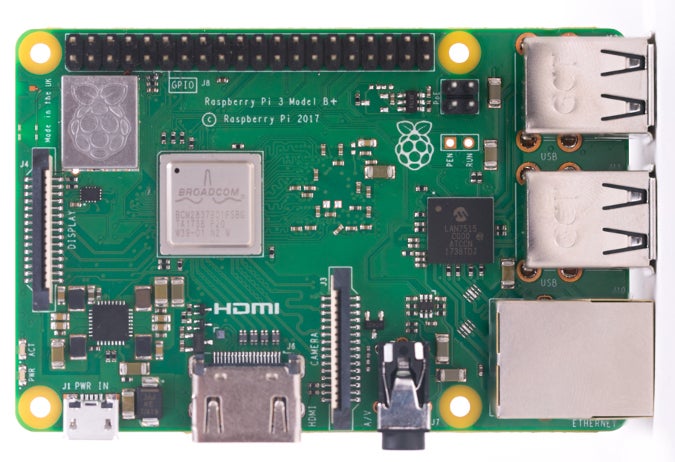
Pengguna dapat mengetahui apa yang akan terjadi sebelum menjalankan suatu fungsi atau mengirim data

Setelah pengguna melakukan transaksi, transaksi tidak dapat dibatalkan.

Tata Kelola dapat didesentralisasikan, sehingga pengguna aplikasi berpartisipasi langsung dalam pengelolaannya.

### Raspberry Pi

Raspberry Pi adalah serangkaian komputer miniatur yang bekerja pada satu papan tapi mampu melakukan hampir semua fungsi komputer normal. Semua model Raspberry Pi menampilkan sistem Broadcom pada chip (SoC) dengan unit pemrosesan sentral (CPU) yang kompatibel dengan ARM yang terintegrasi dan unit pemrosesan grafis (GPU) pada chip[2][14].



**Gambar 2. 1 Raspberry Pi**

### LevelDB

LevelDB adalah sebuah basis data dengan format key-value yang dibuat di Google yang menyediakan urutan pemetaan dari string key hingga string value[17].

Fitur-fitur pada LevelDB,

* + - 1. Key dan Value adalah array byte yang tidak terbatas.
      2. Data tersimpan dengan berdasarkan urutan key.
      3. Dapat dipanggil dengan fungsi buatan untuk menimpa urutan data.
      4. Operasi dasar adalah put, get, delete.
      5. Beberapa proses dapat dijalankan dalam satu batch.
      6. Mendukung iterasi maju dan mundur.

### Android

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan platform yang bersifat open source bagi para pengembang untuk menciptakan sebuah aplikasi. Awalnya, Google Inc. mengakuisi Android Inc. Yang mengembangkan software untuk ponsel yang berada di Palo Alto, California Amerika Serikat. Kemudian untuk mengembangkan Android, dibentuklah Open Handset Alliance, yaitu konsorsium dari 34 perusahaan hardware, software, dan telekomunikasi, termasuk Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nvidia. HTC Dream yang pertama memakai sistem operasi Android.

Dari segi arsitektur sistem, Android merupakan sekumpulan framework dan virtual machine yang berjalan di atas kernel linux. Virtual machine Android bernama Dalvik Virtual Machine (DVM), engine ini berfungsi untuk menginterpretasikan dan menghubungkan seluruh kode mesin yang digunakan oleh setiap aplikasi dengan kernel linux. Sementara untuk framework aplikasi sebagian besar dikembangkan oleh google dan sebagian yang lain dikembangkan oleh pihak ketiga (developer). (Andrey David, 2015)

### React Native

React Native adalah sebuah framework berbasis JavaScript yang digunakan untuk mengembangkan aplikasi mobile di dua sistem operasi secara bersamaan, yaitu Android dan iOS. React Native sendiri pertama kali diluncurkan pada tahun 2015 oleh Facebook dan bersifat open source[18].

Kelebihan React Native

Menghemat Biaya

Penggunaan React Native dapat mengurangi biaya pengembangan. Hal itu karena pengembang tidak perlu mencari dua orang developer untuk mengembangkan aplikasi pada sistem operasi iOS dan Android. Dengan begitu anggaran untuk dua orang developer dapat dialokasikan ke keperluan yang lain.

Menghemat Waktu

Kelebihan selanjutnya adalah penggunaan React Native ini dapat menghemat banyak waktu pengembangan aplikasi. Hal tersebut karena kode dari React ini dapat digunakan kembali tanpa harus merubah banyak komponen dari kodenya.

Memiliki Komunitas yang Besar

React Native adalah framework JavaScript yang bersifat open source sehingga para pengembang dapat saling berkontribusi selama mengikuti aturan dari komunitas. Komunitas ini dapat menjadi sebuah keuntungan untuk pengembang pemula untuk berbagi pengalaman, belajar, dan meningkatkan kemampuannya. Selain itu, komunitas ini dapat menjadi sumber jawaban untuk memecahkan suatu masalah yang dihadapi saat menggunakan React Native.

Kekurangan React Native

Debugging dan kompabilitas

React Native dapat disebut sebagai framework yang masih muda karena baru berumur sekitar 6 tahun. Karena itu, masih cukup banyak masalah dengan kompatibilitas dan kesulitan dalam melakukan debugging yang dapat ditemukan oleh pengembang. Hal ini dapat menjadi kesulitan untuk pengembang pemula.

Kinerja

Karena React Native ini digunakan dalam mengembangkan aplikasi untuk beberapa sistem operasi itu sebabnya kinerja dan hasil dari aplikasinya cukup rendah. Hal tersebut berbeda dengan aplikasi yang dikembangkan oleh bahasa pemrograman khusus yang sesuai dengan sistem operasinya.

### Web3.js

web3.js adalah kumpulan library-library yang memungkinkan pengguna untuk berinteraksi dengan node Ethereum lokal atau remote, menggunakan koneksi HTTP atau IPC. Web3.js dapat digunakan untuk menciptakan aplikasi frontend yang berfungsi sebagai antarmuka untuk berkomunikasi dengan blockchain dan membuat fungsi-fungsi lebih interaktif[14].

### Visual Studio Code

Visual Code Studio adalah sebuah code editor gratis yang bisa dijalankan di perangkat desktop berbasis Windows, Linux, dan MacOS. Code editor ini dikembangkan oleh salah satu raksasa teknologi dunia, Microsoft[19].

### Git dan Github

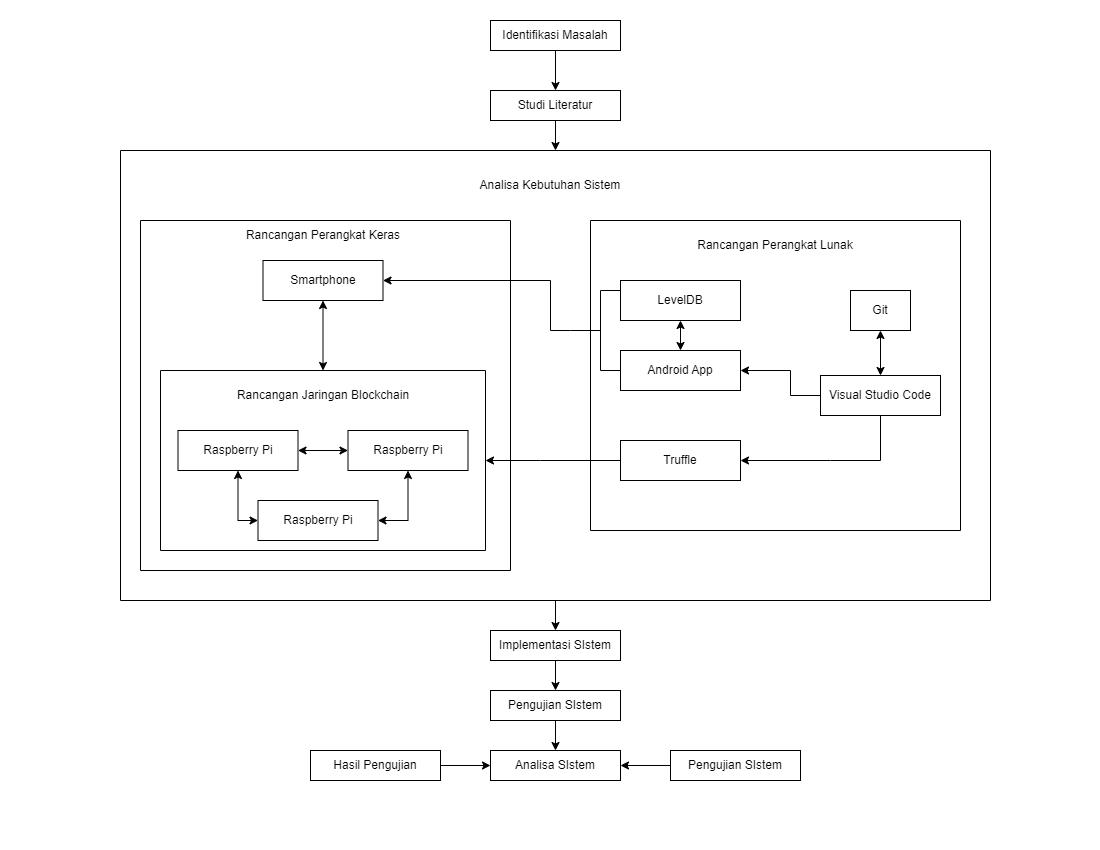
Git merupakan software berbasis Version Control System (VCS) yang bertugas untuk mencatat perubahan seluruh file atau repository suatu project. Developer software biasa menggunakan Git untuk distributed revision (VCS terdistribusi), hal ini bertujuan untuk menyimpan database tidak hanya ke satu tempat. Namun semua orang yang terlibat dalam penyusunan kode dapat menyimpan database ini. GitHub merupakan layanan cloud yang berguna untuk menyimpan dan mengelola sebuah project yang dinamakan repository (repo git). Cara kerja pada GitHub harus terkoneksi pada internet sehingga tidak perlu meng-install sebuah software ke dalam perangkat keras. Hal ini memberikan keringanan penyimpanan komputer yang kita gunakan karena file project tersimpan oleh cloud GitHub. Konsep kerja GitHub pada dasarnya sama dengan Git yaitu dapat menulis source code secara individu atau tim. User interface yang tersedia pada GitHub lebih menarik dan mudah dipahami oleh pengguna awal. Pekerjaan secara tim, pengguna juga bisa melihat siapa penulis kode dan tanggal berapa kode tersebut dibuat[20].

# BAB III

## PERANCANGAN SISTEM

### 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, Jaringan Ethereum Pribadi, dan aplikasi android.



Gambar 3. 1 Diagram Rancangan Penelitian

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

1. 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 tanganan dokumen. Kemudian, dari permasalahan tersebut dirancang sebuah sistem untuk mengatasi permasalahannya.

1. 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.

1. 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.

1. Perancangan Jaringan Blockchain

Pada tahap perancangan jaringan blockchain ini inisialisasi dan pengaturan jaringan dilakukan, dimulai dari pembuatan genesis blok, pemilihan konsensus, pembuatan akun dan pendefinisian validator, jumlah node, dan bootnode.

1. Perancangan Perangkat Lunak

Pada tahap perancangan perangkat lunak, dilakukan pembuatan aplikasi android 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.

1. 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.

1. Pengujian Sistem

Pada tahap pengujian sistem, akan dilakukan serangkaian pengujian untuk menguji kinerja sistem termasuk komponen-komponen yang digunakan dan dapat berjalan dengan lancar serta pengujian pada perangkat lunak agar dapat berjalan sesuai fungsinya.

1. 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. Aturan-aturan untuk transaksi tanda tangan dapat diimplementasikan dengan smart contract
      3. Transaksi penanda tanganan dokumen menjadi transparan dan dapat ditelusuri menggunakan dapp

1. 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

1. 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.

### Analisa Kebutuhan Sistem

Dalam melakukan rancangan terhadap sistem yang akan dibuat maka dilakukan analisa terhadap kebutuhan sistem yang akan dibutuhkan agar mendapatkan gambaran bagaimana sistem dapat bekerja sepenuhnya. Ada empat kategori diantaranya : kebutuhan perangkat keras, kebutuhan jaringan, kebutuhan perangkat lunak, kebutuhan fungsionalitas dan kebutuhan non-fungsionalitas

#### Kebutuhan Perangkat Keras

Dalam membangun sistem ini, ada beberapa komponen perangkat keras yang dibutuhkan agar dapat mencapai tujuan sesuai dengan yang telah ditentukan yaitu:

1. Raspberry Pi, merupakan single board computer untuk menjadi host node

#### Kebutuhan Jaringan

* + - 1. Tiga buah node, sebagai peer
      2. Proof of authority, sebagai consensus mechanism
      3. Satu validator di setiap node
      4. Genesis blok, sebagai blok pertama dalam jaringan blockchain
      5. Smart contract, sebagai program yang mengontrol transaksi tanda tangan
      6. Alamat IP di setiap host node, sebagai alamat node di jaringan internet

#### Kebutuhan Perangkat Lunak

1. Visual Studio Code

Sebagai code editor untuk membuat aplikasi android dan smart contract.

1. Aplikasi Android dan LevelDB

Aplikasi android digunakan sebagai antarmuka pengguna untuk mengakses jaringan blockchain yang dibuat sedangkan levelDB digunakan sebagai local storage untuk menyimpan data yang sering digunakan oleh pengguna (chacing) di aplikasi.

#### Kebutuhan Fungsional

Kebutuhan fungsional adalah kebutuhan yang sangat berfungsi dalam terlaksananya sistem dengan baik, agar proses yang dirancang dapat berjalan seperti :

1. Sistem dapat mendistribusikan basis data
2. Basis data bersifat immutable
3. Smart contract dapat mengontrol transaksi tanda tangan sesuai dengan aturan yang telah diberikan.
4. Aplikasi android dapat digunakan untuk berinteraksi dengan jaringan blockchain yang telah dibuat.

#### Kebutuhan Non-Fungsional

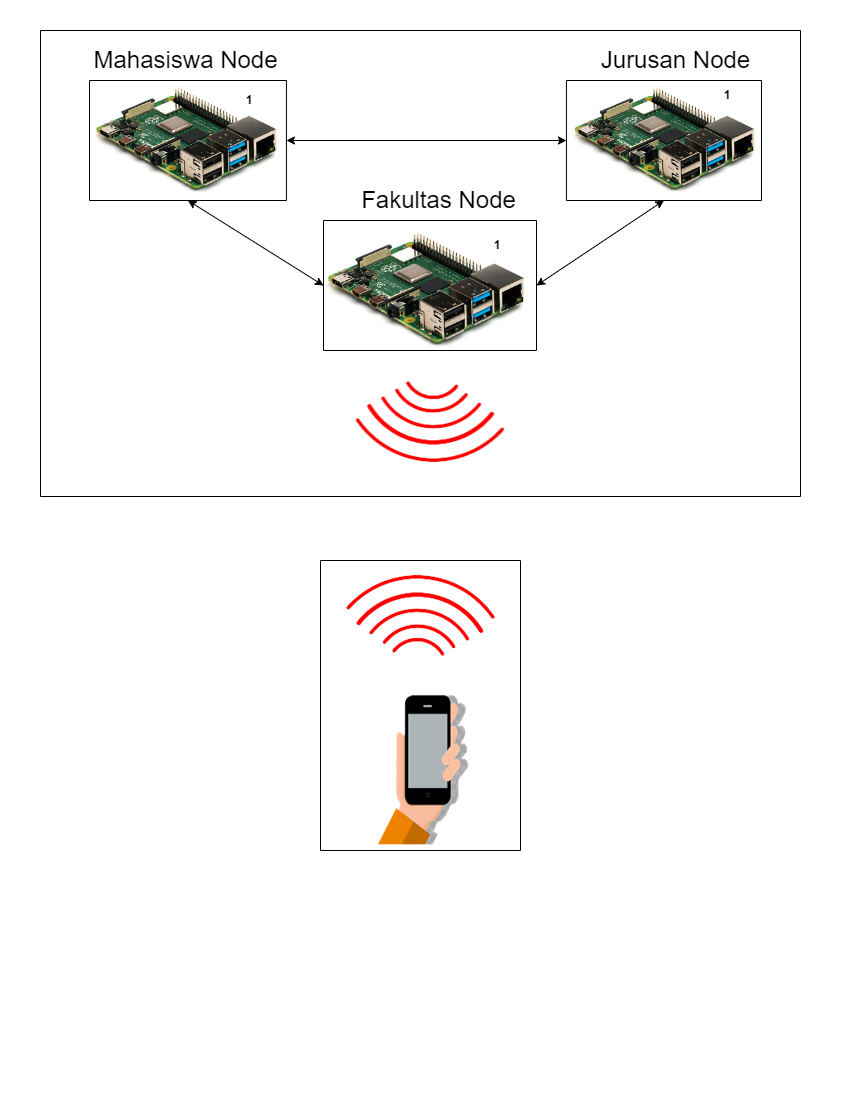
Kebutuhan Non-Fungsional adalah kebutuhan sistem di luar kebutuhan fungsional tetapi masih mempengaruhi bagaimana kerja sistem tersebut. Pada sistem ini, pengguna dapat berinteraksi dengan jaringan melalui aplikasi android.

Adapun kebutuhan non-fungsional yang harus dipenuhi agar sistem dapat berjalan sesuai dengan tujuan penelitian yaitu:

1. Tampilan antarmuka aplikasi mudah dipahami (user friendly)

### Rancangan Umum Sistem

Untuk memenuhi tujuan penelitian, perancangan sistem harus sesuai dengan kebutuhan fungsional maupun non-fungsional. Sistem digambarkan dari beberapa komponen yang saling terhubung seperti berikut :



Gambar 3. 2 Rancangan Umum Sistem

Keterangan :

1. Raspberry Pi 3

Berdasarkan Gambar 3.2, sistem tercipta dari node-node yang membentuk jaringan blokchain. Node-node akan dipegang oleh tiga pihak, yaitu mahasiswa Teknik Komputer, Departemen Teknik Komputer, dan Fakultas Teknologi Informasi. Node dapat ditempatkan dimana saja selama tersedia jaringan internet. Pengguna dapat berinteraksi dengan jaringan blockchain menggunakan aplikasi android di smartphone.

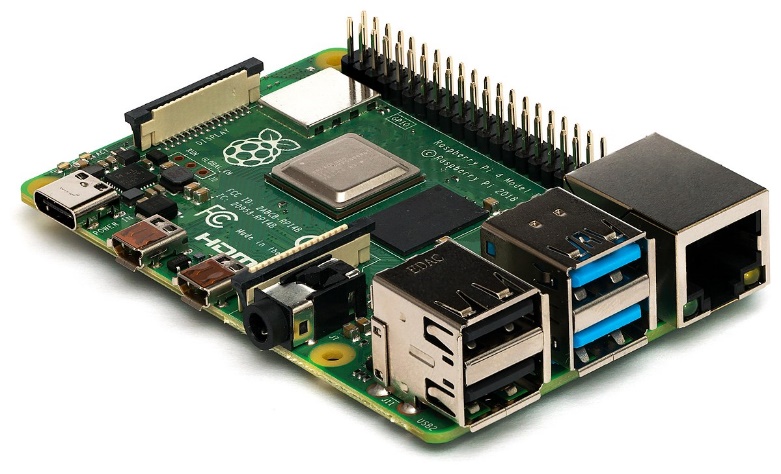
### Rancangan Proses

Pada perancangan umum proses dijelaskan bagaimana hubungan seluruh sistem mampu bekerja dengan baik sehingga tercipta jaringan blockchain.

#### Rancangan Perangkat Keras

Berikut merupakan bentuk rancangan perangkat keras yang akan dibutuhkan pada sistem.

Raspberry Pi



Gambar 3. 3 Rancangan Perangkat Keras

Berdasarkan Gambar 3.3, fungsi dari komponen yang digunakan pada rancangan perangkat keras adalah sebagai berikut.

1. Raspberry Pi 3, merupakan sebuah single board computer yang memliki fungsi yang sama dengan komputer normal.

# DAFTAR PUSTAKA

[1] Dannen, Chris. 2017. *Introducing Ethereum and Solidity.* New York: Brooklyn

[2] Erick Fernando, Meyliana, Surjandy. (2019). *Blockchain Technology Implementation In Raspberry Pi For Private Network.* Jakarta | Bina Nusantara University

[3] Singh dkk. (2019). *Managing Smart Home Appliances with Proof of Authority and Blockchain*. Department of CSE | Indian Institute of Technology Guwahati

[4] Koh dkk. (2019). *Blockchain applications in supply chains, transport, and logistics: a systematic review of the literature.* International Journal of Production Research

[5] Harb dkk. (2018). *Decentralized Voting Platform Based on Ethereum Blockchain*. Department of Computer Science | American University of Science and Technology

[6] Yavuz dkk. (2018). *Towards Secure E-Voting Using Ethereum Blockchain*. Computer Engineering Dept. | Dokuz Eylul University

[7] Octariadi, Barry Caesar. (2020). *PENGENALAN POLA TANDA TANGAN MENGGUNAKAN METODE SYARAF TIRUAN BACKPROPAGATION.* Jurnal Teknoinfo, 14(1)

[8] *Move your business forward with easy-to-use signNow features*.(2020). Diakses pada 19 Mei 2022, dari <https://www.signnow.com/features>

[9] *Yuk mengenal tentang layanan Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia*.(2019). Diakses pada 19 Mei 2022, dari <https://tte.kominfo.go.id/apaitu>

[10] Baiq, Furqan, Wang Fusheng.(2019). *Blockchain Enabled Distributed Data Management - A Vision*. Dept. of Computer Science | Stony Brook University

[11] Yano, Makoto dkk. 2020. *Blockchain and Crypt Currency.* Tokyo: Research Institute of Economy, Trade and Industry (RIETI)

[12] Nakamoto, Satoshi.(2002). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. Diakses dari <https://bitcoin.org/bitcoin.pdf>

[13] Asad dkk.(2020). *Permission-Based Blockchain with Proof of Authorithy for Secured Healthcare Data Sharing.* 2ndICAICT Bangladesh.

[14] Pathari dkk. (2021). *A private Ethereum blockchain implementation for secure data handling in internet of Medical Things.*

[15] Ethereum. (2022). *Solidity*. Diakses pada 9 januari, dari <https://docs.soliditylang.org/en/latest/>

[16] Huang dkk. (2020). *MResearch on Ethereum Private Blockchain Multi-nodes Platform.* International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)

[17] Google. (2023). *LevelDB*. Diakses pada 9 januari, dari <https://github.com/google/leveldb>

[18] Roni Setiawan. (2021). *Apa Itu React Native? Apa Kelebihan dan Kekurangannya*. Diakses pada 9 januari, dari <https://www.dicoding.com/blog/apa-itu-react-native/>

[19] Muhammad Ariffudin. (2022). *Mengenal Visual Code Studio dan Fitur-Fitur Pentingnya*. Diakses pada 9 januari, dari <https://www.niagahoster.co.id/blog/visual-code-studio/>

[20] Dicoding Intern. (2020). *Apa Perbedaan Git dan GitHub? Berikut Penjelasannya*. Diakses pada 9 januari, dari <https://www.dicoding.com/blog/perbedaan-git-dan-github/>