# 

**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.

# 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.*